					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P17S					Titre du document : **Politique de protection des données et de la vie privée**							
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	Clauses 5.1, 6.1.3, 8	
ISO/IEC 27002:2022	Mesures 5.34, 8.10–8.12	
NIST SP 800-53 Rev.5	AR-2, PL-5, AC-6, IR-4	
RGPD de l'UE	Articles 5, 6, 12-23, 30, 32-34	
NIS2 de l'UE	Article 21(2)(e), 21(2)(f)	
DORA de l'UE	Articles 6, 15, 17	
COBIT 2019	APO12, DSS05, MEA03	

1. Objet

1.1. La présente politique définit la manière dont l'organisation protège les données à caractère personnel conformément aux obligations légales, aux exigences réglementaires et aux normes internationales de sécurité.

1.2. Elle établit que les données à caractère personnel, qu'elles concernent les clients, le personnel ou les partenaires, sont collectées, utilisées, stockées et supprimées de manière licite, loyale et sécurisée.

1.3. La présente politique vise également à assurer la conformité à l'ISO/IEC 27001:2022 et à soutenir la préparation aux audits en imposant une approche cohérente, fondée sur les risques, de la protection de la vie privée.

1.4. Par cette politique, l'organisation démontre sa responsabilité et renforce la confiance des clients en accordant la priorité à la transparence, à la minimisation des données et à une gouvernance robuste de la protection des données.

2. Champ d'application

2.1. La présente politique s'applique à :

2.1.1. Tous les employés, prestataires et fournisseurs de services qui accèdent à des données à caractère personnel, les traitent ou les gèrent

2.1.2. Tout système, toute application ou tout emplacement dans lequel des données à caractère personnel sont stockées ou transmises

2.1.3. Toutes les données à caractère personnel, qu'elles soient conservées sous forme électronique, sur support papier, dans des systèmes hébergés dans le cloud ou sur des appareils mobiles

2.2. La présente politique s'applique aux données relatives aux clients, au personnel, aux fournisseurs et à toute autre personne identifiable.

2.3. La politique demeure applicable que les données soient traitées en interne ou par des prestataires tiers.

3. Objectifs

3.1. Veiller à ce que les données à caractère personnel soient traitées conformément aux lois relatives à la protection de la vie privée et aux normes de sécurité, y compris le RGPD, NIS2 et l'ISO/IEC 27001.

3.2. Protéger les données à caractère personnel contre tout accès non autorisé, toute utilisation abusive, toute altération ou toute perte au moyen de contrôles techniques et organisationnels clairement définis.

3.3. Garantir le respect des droits des personnes concernées, y compris le droit d'accès, de rectification et d'effacement de leurs données.

3.4. Définir clairement les rôles et responsabilités relatifs à la protection des données au sein de l'organisation.

3.5. Imposer la minimisation des données, une conservation sécurisée et une suppression en temps utile dans l'ensemble des systèmes et processus.

3.6. Réduire le risque de non-conformité, de sanctions juridiques, d'atteinte à la réputation ou de perte de confiance des clients.

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. Approuve la présente politique et veille à sa mise en application

4.1.2. Fournit les ressources nécessaires pour gérer les risques relatifs à la vie privée et répondre aux incidents

4.1.3. Assume la responsabilité globale de la conformité aux lois et normes applicables en matière de protection de la vie privée

4.2. Coordinateur à la protection des données (interne ou externalisé)

4.2.1. Tient à jour les registres des activités de traitement

4.2.2. Traite les demandes des personnes concernées et les sollicitations des autorités de contrôle

4.2.3. Appuie les évaluations des risques, la formation et la mise en œuvre de la politique

4.2.4. Documente les violations de données et notifie les autorités lorsque cela est requis

[... 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. Revues planifiées

9.1.1. La présente politique doit faire l'objet d'une revue au moins une fois tous les 12 mois par le Coordinateur à la protection des données et être approuvée par le Directeur général

9.1.2. La revue doit évaluer la pertinence de la politique, l'alignement réglementaire et l'efficacité opérationnelle

9.2. Déclencheurs de revue intermédiaire

9.2.1. Les mises à jour de la politique doivent également être engagées en réponse aux éléments suivants :

9.2.1.1. Nouvelles lois sur la protection des données ou textes révisés (par exemple : RGPD, DORA)

9.2.1.2. Incidents de sécurité ou atteintes à la vie privée impliquant des données à caractère personnel

9.2.1.3. Mise en service de nouveaux systèmes, outils ou services traitant des données à caractère personnel

9.2.1.4. Constats d'audit significatifs ou recommandations d'une autorité de contrôle

9.3. Contrôle des changements et communication

9.3.1. Toutes les modifications apportées à la politique doivent être formellement documentées dans un journal des modifications

9.3.2. Les versions révisées doivent être diffusées à l'ensemble du personnel et aux prestataires concernés

9.3.3. Les versions archivées doivent être conservées pour les besoins de la piste d'audit de conformité

10. Politiques associées et articulations

10.1. La présente politique s'applique conjointement avec d'autres politiques PME afin d'établir un cadre complet et applicable de protection de la vie privée :

10.1.1. P13S – Politique de classification et d'étiquetage des données : garantit que les données à caractère personnel sont classifiées de manière appropriée afin que des mesures de protection adaptées à la vie privée puissent être appliquées selon le niveau de risque.

10.1.2. P14S – Politique de conservation et d'élimination des données : définit des règles claires concernant la durée de conservation des données à caractère personnel et les méthodes sécurisées de leur élimination à expiration.

10.1.3. P16S – Politique de masquage des données et de pseudonymisation : précise la manière dont les identifiants personnels doivent être transformés avant l'utilisation des données dans des environnements hors production ou leur partage externe.

10.1.4. P30S – Politique de réponse aux incidents : couvre les étapes requises pour répondre aux violations de données, y compris la notification des autorités de contrôle et des personnes concernées dans les délais requis.

10.1.5. P2S – Politique relative aux rôles et responsabilités de gouvernance : clarifie la structure de responsabilité et les rôles décisionnels applicables à l'application et à la supervision de la protection de la vie privée.

10.2. Ces politiques associées doivent faire l'objet d'une revue et être appliquées conjointement afin d'assurer une couverture de bout en bout de la protection de la vie privée sur les systèmes, le personnel et les fournisseurs.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 5.1 – Exige que la direction démontre son leadership et son engagement en matière de protection des données à caractère personnel.

11.1.2. Clause 6.1.3 – Implique le traitement des risques liés au traitement des données à caractère personnel.

11.1.3. Clause 8.1 – Exige la mise en œuvre de contrôles opérationnels pour protéger les données tout au long de leur cycle de vie.

11.2. ISO/IEC 27002

11.2.1. Mesure 5.34 – Fournit des orientations de mise en œuvre pour la protection de la vie privée et le traitement sécurisé des informations personnellement identifiables.

11.2.2. Mesure 8.10 – Traite de la suppression sécurisée des données à caractère personnel afin d'éviter toute divulgation résiduelle.

11.2.3. Mesure 8.11 – Soutient l'utilisation du masquage et de la pseudonymisation pour la minimisation des données.

11.2.4. Mesure 8.12 – Vise à prévenir toute fuite non autorisée de données au moyen de contrôles portant sur l'accès aux données et leur utilisation.

11.3. NIST SP 800-53 Rev.5

11.3.1. AR-2 – Attribue les rôles et responsabilités relatifs à la gestion du risque lié à la protection de la vie privée.

11.3.2. PL-5 – Exige une documentation du plan de protection de la vie privée couvrant l'utilisation et la protection des données.

11.3.3. AC-6 – Implique le principe du moindre privilège et des contrôles d'accès applicables aux données à caractère personnel.

11.3.4. IR-4 – Exige des processus de gestion des incidents pour les violations impliquant des données à caractère personnel.

11.4. RGPD de l'UE

11.4.1. Article 5 – Définit les principes fondamentaux du traitement licite, loyal et transparent des données.

11.4.2. Article 6 – Exige une base légale valide pour chaque activité de traitement de données à caractère personnel.

11.4.3. Articles 12–23 – Définissent les droits des personnes concernées, y compris l'accès, la rectification, l'effacement et l'opposition.

11.4.4. Article 30 – Exige la tenue d'un registre des activités de traitement.

11.4.5. Article 32 – Exige des mesures techniques et organisationnelles appropriées.

11.4.6. Articles 33–34 – Définissent les obligations de notification des violations auprès des autorités et des personnes concernées.

11.5. NIS2 de l'UE

11.5.1. Article 21(2)(e) – Exige des mesures garantissant une protection des données alignée sur les politiques de cybersécurité.

11.5.2. Article 21(2)(f) – Implique des mécanismes de gestion de la sécurité des données à caractère personnel et des données confidentielles dans les systèmes TIC.

11.6. DORA de l'UE

11.6.1. Article 6 – Exige des cadres de gouvernance interne permettant de gérer les risques et la protection des données.

11.6.2. Article 15 – Implique que les entités financières veillent à ce que les prestataires tiers protègent les données à caractère personnel et soutiennent la conformité réglementaire.

11.6.3. Article 17 – Exige que les entreprises veillent à ce que les systèmes TIC traitant des données à caractère personnel soient sécurisés, résilients et surveillés.

11.7. COBIT 2019

11.7.1. APO12 – Gérer les risques : exige l'identification et le traitement des risques liés à la protection de la vie privée et à la protection des données.

11.7.2. DSS05 – Gestion des services de sécurité : exige des mesures de protection afin d'empêcher tout accès non autorisé aux données à caractère personnel.

11.7.3. MEA03 – Surveiller la conformité : exige des organisations qu'elles assurent une conformité continue aux lois relatives à la protection de la vie privée et à la protection des données.