| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insérez ici la dénomination de l'entité juridique enregistrée | | | | | | | |
| Numéro du document :<br>P17 | | | | | Titre du document :<br>**Politique de protection des données et de la vie privée** | | | | | | | |
| Version :<br>1.0 | | Date d'entrée en vigueur :<br>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, 6.1.3, 8.1, 10 | Contrôles généraux, techniques, d'amélioration continue et de protection des données pertinents |
| ISO/IEC 27002:2022 | Mesures 5.34, 8.10, 8.11, 8.12 | Contrôles relatifs au traitement des données à caractère personnel, à la conservation, à la suppression, à l'anonymisation et aux droits des personnes concernées |
| NIST SP 800-53 Rev.5 | AR-1, AR-2, AR-4, AR-5; PL-2, PL-8; AC-2, AC-6; AU-2, AU-6, AU-9; IR-4, IR-5, IR-6; PM-1, PM-21, PM-23 | Exigences relatives à la gouvernance, aux risques, à la gestion des accès, à la journalisation, à la réponse aux violations de données et au programme de protection de la vie privée |
| RGPD de l'UE | Articles 5, 6, 12–23, 25, 28, 30, 32–34; Considérant 78 | Exigences fondamentales en matière de protection de la vie privée, de responsabilité, de droits des personnes concernées, de traitement des demandes des personnes concernées, de notification des violations, de protection des données dès la conception et de protection des données par défaut |
| NIS2 de l'UE | Article 21(2)(e), (f) | Contrôles de sécurité fondés sur les risques pour les entités essentielles et importantes |
| DORA de l'UE | Articles 6(2)(d), 11(1)(c), 15(1), 17 | Exigences relatives à la gouvernance, aux risques liés aux tiers et aux délais de traitement sécurisé |
| COBIT 2019 | APO12, DSS01, DSS05, MEA | Gestion des risques, exploitation sécurisée, surveillance de la conformité |

## 1. Objet

1.1 La présente politique établit les principes organisationnels obligatoires et les exigences techniques applicables à la protection des données à caractère personnel et à la mise en œuvre de la protection des données dès la conception dans tous les environnements.

1.2 Elle formalise les responsabilités de l'entreprise au regard des normes internationales et des cadres réglementaires, afin de garantir que les données à caractère personnel sont collectées, traitées, conservées, partagées et supprimées de manière licite, sécurisée et transparente.

1.3 La présente politique renforce également la conformité aux lois et référentiels applicables en matière de protection de la vie privée, notamment le règlement général sur la protection des données (RGPD) de l'Union européenne, la directive NIS2 de l'Union européenne, le règlement DORA de l'Union européenne, l'ISO/IEC 27001:2022 et COBIT 2019.

## 2. Champ d'application

**2.1 La présente politique s'applique à l'ensemble des unités organisationnelles, du personnel et des systèmes intervenant dans le traitement des données à caractère personnel, notamment :**

2.1.1 les employés, prestataires, consultants et fournisseurs de services tiers ;

2.1.2 les données collectées à partir de sources internes et externes dans l'ensemble des fonctions métier ;

2.1.3 les supports physiques et numériques, y compris les services cloud, les plateformes SaaS, les appareils mobiles et les enregistrements papier ;

2.1.4 tous les environnements, y compris les systèmes de production, de développement, de test et de sauvegarde, dans lesquels des données à caractère personnel peuvent être présentes.

**2.2 Elle couvre l'ensemble des activités de traitement régies par les lois et normes applicables en matière de protection de la vie privée, y compris, sans s'y limiter :**

2.2.1 la collecte, le stockage, l'utilisation, la transmission et la suppression des données à caractère personnel ;

2.2.2 la mise en œuvre des droits des personnes concernées, la documentation de la base légale et la gestion du consentement ;

2.2.3 les transferts transfrontaliers, la notification des violations et le partage de données avec des tiers ;

2.2.4 la conception sécurisée et la mise en œuvre de la protection des données par défaut dans les systèmes et les processus.

## 3. Objectifs

3.1 Garantir un traitement licite, transparent et responsable des données à caractère personnel, en alignement avec l'ISO/IEC 27001:2022 et les obligations juridiques associées.

3.2 Intégrer les principes de protection des données dès la conception et de protection des données par défaut dans tous les systèmes d'information, services et processus métier.

3.3 Imposer des mesures techniques et organisationnelles (MTO) protégeant la confidentialité, l'intégrité et la disponibilité des données à caractère personnel tout au long de leur cycle de vie.

3.4 Définir les rôles de gouvernance et les structures de responsabilité relatifs à la protection des données, y compris les responsabilités du délégué à la protection des données (DPD), de la sécurité de l'information, des affaires juridiques et des propriétaires de données.

3.5 Permettre une conformité complète aux articles 5, 6, 25, 30 et 32 du RGPD, ainsi qu'aux exigences de réduction des risques et de résilience prévues par NIS2 et DORA.

3.6 Garantir les droits des personnes concernées, y compris l'accès, la rectification, l'effacement, la limitation, la portabilité, l'opposition et la protection contre la prise de décision automatisée.

3.7 Atténuer les risques réglementaires, réputationnels, juridiques et opérationnels résultant d'un accès non autorisé, d'un usage abusif ou de la perte de données à caractère personnel.

## 4. Rôles et responsabilités

### 4.1 Haute direction

4.1.1 Assure la supervision stratégique et alloue des ressources suffisantes pour soutenir le programme de protection de la vie privée.

4.1.2 Approuve la présente politique et veille à son application dans l'ensemble de l'organisation.

**4.2 Délégué à la protection des données (DPD)**

4.2.1 Exerce sa mission en toute indépendance afin de superviser la conformité à la réglementation relative à la protection des données.

4.2.2 Tient le registre des activités de traitement conformément à l'article 30 du RGPD.

4.2.3 Pilote les échanges avec les autorités de contrôle, réalise les analyses d'impact relatives à la protection des données (AIPD) et gère les processus de notification des violations.

4.2.4 Examine les dérogations relatives à la protection de la vie privée et tient le registre correspondant.

[ ... 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 La présente politique doit être revue au moins une fois par an, ou plus tôt dans les cas suivants :**

9.1.1 mises à jour juridiques ou réglementaires significatives (par exemple : modifications du RGPD, échéances DORA) ;

9.1.2 nouveaux systèmes ou nouvelles activités de traitement impliquant des données à caractère personnel ;

9.1.3 constats d'audit interne révélant des lacunes de la politique ;

9.1.4 incidents de violation significatifs ou retours d'une autorité de contrôle.

**9.2 Responsabilités de revue**

9.2.1 Le DPD doit initier la revue de la politique, en coordination avec le juridique, les risques, la sécurité de l'information et la haute direction.

9.2.2 Toute mise à jour doit être enregistrée dans le registre de contrôle documentaire du SMSI et diffusée aux parties prenantes concernées.

**9.3 Contrôle des changements**

9.3.1 Toute révision de la présente politique doit être formellement approuvée par la haute direction.

9.3.2 Les versions obsolètes doivent être archivées de manière sécurisée, et la version mise à jour doit inclure un historique des modifications documenté.

**10. Politiques associées et articulations**

10.1 P1 – Politique de sécurité de l’information. Établit les principes généraux de gouvernance de la sécurité qui sous-tendent la présente politique de protection de la vie privée. P1 soutient la confidentialité, l'intégrité et la disponibilité des données à caractère personnel dans l'ensemble des systèmes et services.

10.2 P6 – Politique de gestion des risques. Définit la méthodologie de traitement des risques de l'organisation, essentielle pour l'évaluation des risques liés à la protection de la vie privée, les processus d'AIPD et les évaluations du risque résiduel exigés par l'article 6.1.3 de l'ISO/IEC 27001 et le RGPD.

10.3 P13 – Politique de classification et d'étiquetage des données. Oriente la catégorisation des données à caractère personnel et des données sensibles, et sert de base à l'application des contrôles appropriés de protection de la vie privée, notamment la mise en œuvre de la conservation, la limitation des accès et la suppression sécurisée.

10.4 P14 – Politique de conservation et d’élimination des données. Soutient directement les exigences de protection de la vie privée prévues aux articles 5(1)(e) et 17 du RGPD, en garantissant que les

données à caractère personnel ne sont conservées que pendant la durée nécessaire et sont supprimées de manière sécurisée conformément aux obligations légales.

10.5 P16 – Politique de masquage des données et de pseudonymisation. Établit des contrôles visant à réduire l'identifiabilité des données à caractère personnel au moyen de mesures techniques telles que la tokenisation, le masquage dynamique et la pseudonymisation, assurant ainsi la conformité à l'article 32 du RGPD et à la mesure 5.34 de l'ISO/IEC 27002.

10.6 P30 – Politique de réponse aux incidents. Décrit les protocoles obligatoires de réponse aux violations, articulés avec le traitement des violations relatives à la protection de la vie privée et les délais de notification exigés par les articles 33 et 34 du RGPD.

10.7 P33 – Politique d'audit et de surveillance de la conformité. Impose des évaluations planifiées de l'efficacité du programme de protection de la vie privée, de l'application de la politique et du suivi des actions correctives dans les unités organisationnelles et chez les sous-traitants traitant des données.

## 11. Normes et référentiels de référence

### 11.1 ISO/IEC 27001

11.1.1 Article 5.1 – Leadership and Commitment : établit la responsabilité de la haute direction en matière de protection des données à caractère personnel et de mise en œuvre des principes de protection de la vie privée.

11.1.2 Article 6.1.3 – Information Security Risk Treatment : soutient l'identification, l'évaluation et le traitement des risques liés à la protection de la vie privée au moyen des AIPD et des exceptions.

11.1.3 Article 8.1 – Operational Planning and Control : exige des mesures de protection techniques et procédurales afin de garantir un traitement sécurisé des données à caractère personnel.

11.1.4 Article 10.1 – Continual Improvement : impose une évaluation périodique et l'adaptation du programme de protection de la vie privée.

11.2 Mesures 5.34, 8.10, 8.11 et 8.12 de l'ISO/IEC 27002:2022 : fournissent des orientations sur le traitement des données à caractère personnel, la mise en œuvre de la conservation, la suppression, l'anonymisation et la transparence à l'égard des droits des personnes concernées.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 AR-1, AR-2, AR-4, AR-5 : définissent les responsabilités en matière de gouvernance, de rôles, de responsabilité et de formation à la protection de la vie privée.

11.3.2 PL-2, PL-8 : imposent l'intégration de contrôles relatifs à la protection de la vie privée dans le cycle de vie des systèmes et l'architecture d'entreprise.

11.3.3 AC-2, AC-6 : imposent le principe du moindre privilège et la gestion des comptes pour la protection des données à caractère personnel.

11.3.4 AU-2, AU-6, AU-9 : imposent la journalisation, la traçabilité et l'intégrité d'audit pour les accès aux données à caractère personnel.

11.3.5 IR-4, IR-5, IR-6 : définissent des processus structurés de détection, d'analyse et de signalement des violations relatives à la protection de la vie privée.

11.3.6 PM-1, PM-21, PM-23 : établissent un programme complet de protection de la vie privée, aligné sur les objectifs stratégiques de risque et de gouvernance des données.

### 11.4 RGPD de l'Union européenne (2016/679)

11.4.1 Articles 5, 6, 12–23, 25, 28, 30, 32–34 : encadrent le traitement licite, la limitation des finalités, les droits des personnes concernées, la responsabilité, la protection des données dès la conception et par défaut, les obligations des tiers et la gestion des violations.

11.4.2 Considérant 78 : renforce les principes de protection des données dès la conception.

### 11.5 Directive NIS2 de l'Union européenne (2022/2555)

11.5.1 Article 21(2)(e) et (f) : impose la mise en œuvre de contrôles de sécurité fondés sur les risques et la protection des données à caractère personnel dans le périmètre des entités essentielles et importantes.

**11.6 DORA de l'Union européenne (2022/2554)**

11.6.1 Article 6(2)(d) : impose une gouvernance interne du risque lié aux TIC relatif au traitement des données.

11.6.2 Article 11(1)(c) : impose la supervision des risques liés aux tiers pour les services liés aux données.

11.6.3 Articles 15(1) et 17 : exigent un traitement sécurisé des données par les prestataires de services et des notifications rapides aux autorités de contrôle à la suite d'incidents liés aux TIC.

**11.7 COBIT 2019**

11.7.1 APO12 – Gestion des risques : intègre les risques liés à la protection de la vie privée dans la supervision globale des risques de l'organisation.

11.7.2 DSS01 – Managed Operations et DSS05 – Gestion des services de sécurité : garantissent une exploitation sécurisée, y compris le contrôle d'accès, la conservation et l'intégrité des systèmes.

11.7.3 MEA03 – Surveillance de la conformité : impose une revue continue de l'état de conformité au regard des obligations relatives à la protection de la vie privée d'origine réglementaire et documentaire.