					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P16S					Titre du document : **Politique de masquage des données et de pseudonymisation**							
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 6.1.3, 8	Risques de sécurité de l'information et contrôles nécessaires, y compris le masquage et la pseudonymisation
ISO/IEC 27002:2022	Mesures 8.11, 8.12	Recommandations relatives au masquage et à la prévention des fuites de données
NIST SP 800-53 Rev.5	SC-12, SC-28, PT-2, PT-3	Obfuscation des données, technologies de protection de la vie privée
NIS2 de l'UE	Article 21(2)(c)	Mesures techniques proportionnées, pseudonymisation en tant que mesure de sécurité
DORA de l'UE	Article 10(1)	Contrôles des risques liés aux TIC, y compris les garanties de transformation des données
COBIT 2019	DSS05.01, DSS06	Protection des données, techniques d'obfuscation et de pseudonymisation
RGPD de l'UE	Articles 4(5), 5(1)(c), 32	Minimisation des données, pseudonymisation en tant que mesure technique

1. Objet

1.1. La présente politique définit des exigences contraignantes relatives à l'utilisation du masquage des données et de la pseudonymisation afin de protéger les données sensibles, les données à caractère personnel et les données confidentielles au sein des petites et moyennes entreprises (PME).

1.2. Ces techniques sont obligatoires lorsque l'utilisation de données réelles n'est pas nécessaire, notamment dans les contextes de développement, d'analyse ou d'intervention de prestataires tiers, afin de réduire les risques d'exposition, d'utilisation abusive ou de violation de données.

1.3. La présente politique contribue directement à la conformité dans le cadre de la certification ISO/IEC 27001:2022, ainsi qu'au respect d'exigences réglementaires européennes telles que le RGPD, la directive NIS2 et le règlement DORA.

1.4. En transformant les données avant toute utilisation en dehors de leur contexte métier d'origine, l'organisation limite son exposition aux risques et renforce sa capacité à démontrer le respect de ses obligations de diligence en matière de protection de la vie privée et de sécurité.

2. Champ d'application

2.1. La présente politique s'applique à toutes les données structurées ou non structurées classées comme données à caractère personnel, confidentielles ou sensibles, qu'elles soient stockées ou traitées :

2.1.1. Dans des environnements de production, de test ou de développement

2.1.2. Sur des équipements locaux, des serveurs ou des plateformes cloud

2.1.3. Par le personnel interne, des prestataires ou des fournisseurs tiers

2.2. Elle couvre également tous les outils de transformation des données (masquage, tokenisation, pseudonymisation), qu'ils soient open source, commerciaux ou développés en interne.

2.3. Les cas d'usage couverts par la présente politique incluent :

2.3.1. La préparation d'ensembles de données de test ou de développement

2.3.2. L'exportation de données vers des systèmes analytiques

2.3.3. L'accès de fournisseurs ou de consultants à des systèmes opérationnels

2.3.4. La minimisation des données relatives aux personnes concernées afin de réduire le risque lié au traitement

3. Objectifs

3.1. Garantir que des données réelles à caractère personnel ou sensibles ne soient jamais exposées dans des environnements présentant un niveau de sécurité inférieur lorsqu'elles ne sont pas indispensables.

3.2. Imposer des techniques de masquage ou de pseudonymisation lorsque les identifiants réels ne sont pas strictement nécessaires à l'exécution de la tâche.

3.3. Prévenir tout accès non autorisé ou toute utilisation abusive des données en imposant des contrôles de transformation avant tout transfert ou traitement de données.

3.4. Garantir que tous les processus de masquage et de pseudonymisation soient traçables, auditables et mis en œuvre au moyen d'outils approuvés.

3.5. Respecter les exigences légales et réglementaires applicables imposant la minimisation des données, la confidentialité et des garanties de transformation.

4. Rôles et responsabilités

4.1. Directeur général (DG)

4.1.1. Est responsable de la présente politique et l'approuve

4.1.2. Veille à ce que tous les départements et prestataires respectent les exigences de transformation

4.1.3. Examine les dérogations, les évaluations des risques et les journaux de transformation

4.1.4. Coordonne les actions juridiques, opérationnelles ou fournisseurs en cas de manquement

4.2. Prestataire informatique / service informatique interne

4.2.1. Sélectionne et administre les outils de masquage ou de pseudonymisation

4.2.2. Veille à l'application de méthodes de transformation appropriées selon le type de données

4.2.3. Tient à jour les journaux des ensembles de données transformés et les procédures de gestion des clés

4.2.4. Veille à ce que le masquage soit appliqué avant toute utilisation à des fins de test, par un fournisseur ou à des fins analytiques

[... 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

9.1.1. La présente politique doit faire l'objet d'une revue au moins une fois par an par le directeur général afin de garantir qu'elle reflète :

9.1.1.1. Les mises à jour de la réglementation applicable (par exemple, RGPD, DORA)

9.1.1.2. Les nouveaux systèmes métier ou les échanges de données avec des tiers

9.1.1.3. Les retours issus des audits ou des incidents impliquant l'utilisation de données non masquées

9.2. Revues intermédiaires

9.2.1. Des revues doivent également avoir lieu lorsque :

9.2.1.1. De nouvelles applications ou plateformes traitant des données sensibles sont introduites

9.2.1.2. Un incident majeur met en évidence des lacunes dans les contrôles de transformation en place

9.2.1.3. Des modifications des niveaux de classification affectent les procédures de traitement des données

9.3. Gestion des versions et des changements

9.3.1. Toute modification de la politique doit :

9.3.1.1. Être approuvée par le DG et documentée dans un journal des modifications

9.3.1.2. Être clairement communiquée aux employés et prestataires concernés

9.3.1.3. Être archivée de manière sécurisée, avec un accès restreint aux versions obsolètes

10. Politiques associées et articulations

10.1. La présente politique doit être appliquée conjointement avec les politiques PME suivantes afin de garantir une protection cohérente et contraignante des données sensibles :

10.1.1. P13S – Politique de classification et d'étiquetage des données : définit les niveaux de classification (par exemple, « Confidentiel – Données à caractère personnel ») qui déterminent les cas dans lesquels le masquage ou la pseudonymisation doivent être appliqués. Cette politique impose les règles de transformation selon le niveau de sensibilité des données.

10.1.2. P14S – Politique de conservation et d'élimination des données : garantit que les ensembles de données transformés, y compris les sauvegardes contenant des données masquées ou pseudonymisées, sont conservés et éliminés conformément aux règles applicables, y compris la suppression des clés de correspondance lorsqu'elles ne sont plus nécessaires.

10.1.3. P17S – Politique de protection des données et de la vie privée : aligne les pratiques de transformation sur les obligations plus larges en matière de vie privée, y compris les exigences du RGPD relatives à la minimisation des données et à l'utilisation de la pseudonymisation comme mesure de protection pour le traitement des données à caractère personnel.

10.1.4. P30S – Politique de réponse aux incidents : couvre les procédures de signalement et d'escalade en cas de divulgation non autorisée de données, y compris l'utilisation inappropriée ou l'inversion de données masquées ou pseudonymisées.

10.1.5. P2S – Politique relative aux rôles et responsabilités de gouvernance : attribue la responsabilité globale de la mise en œuvre de la politique, de l'acceptation du risque et de l'approbation des dérogations, principalement au directeur général.

10.2. Ces politiques constituent un cadre intégré de protection des données, garantissant que les mesures de masquage et de pseudonymisation contribuent à la certification ISO/IEC 27001 et à la conformité réglementaire transversale.

11. Normes et référentiels de référence

11.1. ISO/IEC 27001

11.1.1. Clause 6.1.3 : exige le traitement des risques liés à la sécurité de l'information, ce qui inclut la réduction de l'exposition au moyen de techniques de transformation des données.

11.1.2. Clause 8.1 : impose la mise en œuvre des contrôles nécessaires pour atteindre les objectifs de sécurité, y compris la pseudonymisation et le masquage.

11.2. ISO/IEC 27002

11.2.1. Mesure 8.11 : fournit des recommandations sur le masquage des données sensibles dans les environnements de test et de développement.

11.2.2. Mesure 8.12 : propose des approches visant à prévenir les fuites de données au moyen de pratiques contrôlées de transformation et d'accès.

11.3. NIST SP 800-53 Rev.5

11.3.1. SC-12 : garantit la confidentialité de l'information au moyen de l'obfuscation des données.

11.3.2. SC-28 : protège l'information au repos et en cours d'utilisation.

11.3.3. PT-2/PT-3 : encouragent l'utilisation de technologies de protection de la vie privée, y compris la pseudonymisation, lors du traitement des informations personnellement identifiables.

11.4. RGPD de l'UE

11.4.1. Article 4(5) : définit juridiquement la pseudonymisation et impose des contrôles sur les clés de correspondance et les identifiants.

11.4.2. Article 5(1)(c) : soutient les principes de minimisation des données par le recours au masquage.

11.4.3. Article 32 : reconnaît la pseudonymisation comme une mesure technique réduisant les risques pour la vie privée.

11.5. Directive NIS2 de l'UE

11.5.1. Article 21(2)(c) : exige des mesures techniques proportionnées afin de réduire le risque de sécurité pesant sur les données, y compris la pseudonymisation dans le cadre de la maîtrise des risques.

11.6. Règlement DORA de l'UE

11.6.1. Article 10(1) : impose des contrôles des risques liés aux TIC incluant des garanties de transformation des données afin d'assurer la continuité et la confidentialité dans le cadre de l'externalisation et du développement des systèmes.

11.7. COBIT 2019

11.7.1. DSS05.01 : exige la protection des actifs informationnels, y compris leur transformation lorsque cela est possible.

11.7.2. DSS06.06 : requiert des techniques appropriées d'obfuscation et de pseudonymisation afin de limiter l'exposition des données dans des environnements à faible niveau de confiance.