					Insérez ici la dénomination de l'entité juridique enregistrée							
Numéro du document : P16					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	Article 6.1	Exigences générales de gestion des risques et de contrôles opérationnels applicables au masquage et à la pseudonymisation
ISO/IEC 27002:2022	Mesures 8.11, 8	Recommandations de contrôle relatives à la mise en œuvre du masquage et de la pseudonymisation
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Mesures de protection des données et de la vie privée relatives à la minimisation des données, à leur transformation et à la limitation des accès
RGPD de l'UE	Articles 4(5), 5(1)(c,f), 32	Base juridique et exigences relatives à la pseudonymisation et aux mesures de protection des données
NIS2 de l'UE	Article 21(2)(c)	Obligation de mettre en œuvre des mesures techniques et organisationnelles, y compris des technologies renforçant la protection de la vie privée (PET)
DORA de l'UE	Articles 10(1), 10(2)(e)	Gestion des risques liés aux TIC et contrôles de confidentialité applicables au masquage des données et à la pseudonymisation
COBIT 2019	DSS05.01, DSS06.06, MEA	Contrôles de gouvernance pour la protection des données au moyen du masquage et l'évaluation de la conformité

1. Objet

1.1 La présente politique définit l'approche de l'organisation en matière de mise en œuvre du masquage des données et de la pseudonymisation en tant que technologies renforçant la protection de la vie privée (PET), afin de réduire l'identifiabilité et l'exposition des données à caractère personnel ou des données sensibles.

1.2 Elle encadre l'utilisation sécurisée de l'information dans les activités de test, d'analyse et d'exploitation, tout en assurant la conformité aux exigences légales et réglementaires, en réduisant l'impact d'une violation de données et en imposant les principes de minimisation des données et de confidentialité.

1.3 La présente politique est alignée sur l'ISO/IEC 27001:2022, prend en compte l'article 4(5) du RGPD relatif à la pseudonymisation et intègre une mise en œuvre fondée sur les risques, cohérente avec les référentiels NIST, NIS2, DORA et COBIT 2019.

2. Champ d’application

2.1 La présente politique s’applique à :

2.1.1 tous les employés, prestataires, tiers ou fournisseurs ayant accès à des systèmes traitant des informations à caractère personnel, confidentielles ou sensibles ;

2.1.2 tous les environnements de données, y compris les environnements de production, de développement, de test et de préproduction ;

2.1.3 toutes les formes de masquage des données (par exemple statique, dynamique, déterministe, tokenisation) et les techniques de pseudonymisation utilisées pour réduire les risques d’atteinte à la vie privée ;

2.1.4 tous les types de données (structurées ou non structurées), de systèmes (sur site ou hébergés dans le cloud) et d’applications impliquant des données à caractère personnel ou des données réglementées.

2.2 Le champ d’application couvre les usages suivants :

2.2.1 le développement applicatif et les environnements d’assurance qualité et de test ;

2.2.2 les plateformes d’analyse ou de reporting ;

2.2.3 les échanges de données avec des tiers ou des prestataires de services ;

2.2.4 les systèmes de sauvegarde, d’archivage ou de reprise.

3. Objectifs

3.1 Assurer une application cohérente et efficace du masquage et de la pseudonymisation afin de réduire les risques d’exposition ou d’usage abusif des données.

3.2 Garantir que des données réelles ne soient jamais utilisées dans des environnements hors production, sauf si elles ont été transformées au moyen de techniques PET approuvées.

3.3 Maintenir l’intégrité référentielle, l’exploitabilité et les transformations préservant le format lorsque cela est nécessaire pour garantir la cohérence opérationnelle.

3.4 Imposer des contrôles d’accès robustes aux données d’origine, aux données masquées et aux clés de réidentification.

3.5 Traiter les jeux de données masqués ou pseudonymisés comme des données sensibles, soumis à la journalisation des accès, aux contrôles de conservation et aux procédures de réponse aux incidents.

3.6 Valider l’efficacité de ces contrôles au moyen de tests continus, de la surveillance et de procédures d’audit.

4. Rôles et responsabilités

4.1 Haute direction

4.1.1 Approuve la présente politique et veille à sa mise en œuvre dans le cadre global de la gouvernance informatique et des initiatives de protection des données.

4.2 Responsable de la sécurité des systèmes d’information (RSSI) / responsable du SMSI

4.2.1 Supervise la mise en œuvre et le maintien de la conformité.

4.2.2 Veille à l’alignement avec l’article 6.1.3 de l’ISO/IEC 27001 (traitement des risques) et l’article 8.1 (contrôle opérationnel).

4.2.3 Revoit les journaux d’audit et valide l’efficacité des contrôles.

[... 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 faire l’objet d’une revue au moins annuelle, ou plus tôt en cas de :

9.1.1 changements réglementaires affectant le masquage ou la pseudonymisation ;

9.1.2 adoption de nouveaux systèmes informatiques traitant des données sensibles ;

9.1.3 modification significative du schéma de classification des données de l'organisation ;

9.1.4 constats d'audit indiquant des défaillances de contrôle ;

9.1.5 émergence de nouvelles menaces ou de nouvelles technologies de masquage.

9.2 Le responsable du SMSI pilote la revue en concertation avec le DPD, les propriétaires de données, la sécurité informatique et les services juridiques. Les mises à jour doivent être soumises à une gestion des versions, approuvées par la haute direction et communiquées à l'ensemble des parties prenantes concernées.

10. Politiques associées et articulations

10.1 P13 - Politique de classification et d'étiquetage des données. Les décisions de masquage et de pseudonymisation dépendent directement de la classification des champs de données et des niveaux de sensibilité définis dans la P13.

10.2 P14 - Politique de conservation et d'élimination des données. Les jeux de données transformés doivent être conservés et éliminés conformément aux règles de cycle de vie définies dans la P14, en veillant à ce que les données masquées et pseudonymisées soient traitées comme des données sensibles.

10.3 P17 - Politique de protection des données et de la vie privée. Cette politique définit les principes de protection de la vie privée et les fondements réglementaires applicables à la pseudonymisation en tant qu'activité de traitement conforme au RGPD et à des législations similaires.

10.4 P22 - Politique de journalisation et de surveillance. Elle permet l'audit centralisé et l'alerte sur les événements de masquage et de pseudonymisation, conformément à des procédures structurées de surveillance de la sécurité.

11. Normes et référentiels de référence

11.1 ISO/IEC 27001

11.1.1 Article 6.1.3 - Plan de traitement des risques : établit le masquage et la pseudonymisation comme des mécanismes de traitement des risques visant à réduire l'identifiabilité des données sensibles dans des environnements de traitement non essentiels.

11.1.2 Article 8.1 - Planification et contrôle opérationnels : impose des contrôles techniques et procéduraux pour la transformation sécurisée des données pendant leur traitement, leur stockage ou leur transfert.

11.2 ISO/IEC 27002:2022

11.2.1 Mesures 8.11, 8 : recommandations relatives au masquage des données et à la pseudonymisation afin de minimiser les risques de réidentification et de fuite de données.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Protection des informations personnellement identifiables : mise en œuvre de technologies renforçant la protection de la vie privée, telles que le masquage et la pseudonymisation.

11.3.2 PT-2, PT-3 : minimisation et sécurité du traitement des informations personnellement identifiables - transformation visant à réduire l'identifiabilité et à appliquer le contrôle d'accès.

11.3.3 SC-12, SC-28, SC-30 : confidentialité et intégrité des données - contrôles de confidentialité et d'obfuscation pour le stockage, la transmission et l'utilisation.

11.4 RGPD de l'UE (2016/679)

11.4.1 Article 4(5) : définition formelle de la pseudonymisation.

11.4.2 Article 32 : sécurité du traitement - mesures organisationnelles et techniques applicables à la pseudonymisation.

11.4.3 Article 5(1)(c,f) : minimisation des données et confidentialité au moyen de la pseudonymisation et du masquage.

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

11.5.1 Article 21(2)(c) : exige des PET telles que le masquage et la pseudonymisation en tant que mesures de sécurité.

11.6 DORA de l'UE (2022/2554)

11.6.1 Article 10(1) : le cadre de gestion des risques liés aux TIC comprend des contrôles de masquage et de pseudonymisation.

11.6.2 Article 10(2)(e) : impose l'utilisation de technologies de transformation pour protéger les données à caractère personnel et les données financières.

11.7 COBIT 2019

11.7.1 DSS05.01 : protéger les actifs informationnels - exigences relatives au masquage et à la pseudonymisation.

11.7.2 DSS06.06 : sécurisation des tests et des analyses - masquage dans les environnements hors production.

11.7.3 MEA03 : surveillance de la conformité portant sur l'efficacité du masquage et de la pseudonymisation.