IMPACT SUR LA PROTECTION DES DONNÉES

PROCÉDURE D'ÉVALUATION ET À PROPOS DE SES PRINCIPES RÈGLEMENTS

KVKK_Y3 VERSION 1.00

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

ANALYSE D'IMPACT SUR LA PROTECTION DES DONNÉES (AIPD) RÉGLEMENTATION DES PROCÉDURES ET DES PRINCIPES

1. INTRODUCTION ET PORTÉE

1.1. Le présent Règlement sur les procédures et les principes de l'analyse d'impact relative à la protection des données (AIPD) (ci-après dénommé le Règlement) doit être évalué conjointement avec la politique de sécurité de l'information, la politique de protection des données personnelles et la politique-cadre de notre société.

1.2. Le présent règlement régit les procédures et les principes à suivre lorsque notre société, en tant que responsable du traitement des données, est tenue de procéder à une évaluation de l'impact des activités de traitement prévues sur la protection des données à caractère personnel avant le traitement (article 35 du RGPD), ou lorsque les propriétaires d'actifs informationnels effectuent des analyses d'impact relatives à la protection des données au cours de leurs processus d'examen annuel des actifs informationnels qu'ils contrôlent, notamment lorsque de nouvelles technologies sont utilisées en termes de méthodologie des technologies de l'information et de la communication ou d'utilisation commerciale générale, et lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques, compte tenu de la nature, de la portée, du contexte et des finalités de l'activité de traitement des données.

1.3. Définitions : Aux fins du présent règlement, les actifs informationnels sont des actifs appartenant à Kardelen Boya qui sont nécessaires au bon déroulement de ses opérations et qu'elle est donc tenue de protéger.

1.4. Propriétaire de l'actif informationnel : Le responsable du secteur d'activité où l'actif concerné est utilisé.

2. ÉVALUATION D'IMPACT SUR LA PROTECTION DES DONNÉES

2.1. Les employés désignés comme propriétaires d'actifs informationnels sont responsables de la gestion des actifs informationnels sous leur contrôle conformément aux responsabilités décrites dans la politique-cadre.

2.2. Les propriétaires d'actifs informationnels doivent effectuer une évaluation d'impact au moins une fois par an, et en particulier lorsqu'il y a des changements importants dans l'actif informationnel, ses méthodes de stockage et de traitement, ou des changements dans les réglementations ou politiques juridiques qui prévoient des changements dans les données personnelles stockées dans les actifs informationnels, ils doivent effectuer une évaluation d'impact avant que tout changement ne soit mis en œuvre.

2.3. Les propriétaires d'actifs informationnels doivent s'assurer que la sécurité des actifs qu'ils contrôlent répond aux conditions suivantes énoncées dans la politique de sécurité de l'information de l'entreprise :

- Tous les utilisateurs doivent s'assurer qu'ils ont bien accès à l'information avant de l'utiliser. Ils doivent être autorisés.
- Une contrepartie raisonnable compatible avec la valeur et/ou la sensibilité de l'actif informationnel. Un certain niveau de sécurité doit être assuré.

Tout incident entraînant ou susceptible d'entraîner une violation de données doit être signalé au délégué à la protection des données et au responsable informatique. Les utilisateurs concernés doivent également informer sans délai l'équipe de support informatique, leur chef de service ou la direction de l'entreprise.

- Les utilisateurs sont tenus de réaliser une analyse d'impact relative à la protection des données (AIP) sur leurs actifs dans le cadre de l'examen annuel de leur inventaire des actifs informationnels.

2.3.1. Chaque propriétaire d'un actif informationnel est tenu de déployer des efforts raisonnables pour s'assurer que tous les documents en sa possession répondent en tout temps aux exigences suivantes :

- Les données collectées doivent être licites.
- Le respect des conditions d'utilisation des ressources informatiques, telles que décrites à la section 11 de la politique de sécurité de l'information de l'entreprise, est requis.
- Les données collectées ne doivent pas contenir de liens menant à des contenus illégaux ni de contenu non conforme aux conditions d'utilisation des outils d'information et de communication de la société.
- Sauf autorisation du chef de département concerné, aucune promotion ni aucun commentaire sur les biens, produits ou services de la société ne peut être publié au nom de celle-ci.
- Sauf autorisation du chef de département concerné, du propriétaire des actifs informationnels ou de toute autre société, partenariat, consortium ou cabinet de conseil, les informations et/ou données contenant des éléments promotionnels ou des commentaires sur leurs activités « privées » ne doivent pas être incluses.

2.3.2. Les informations appartenant à toute personne physique qui sont incluses dans les actifs informationnels de la société et données:

- Il ne doit pas contenir la marque de commerce, le logo, l'en-tête, etc. de l'entreprise.

- Les documents conservés doivent être directement liés ou pertinents à l'autorisation donnée au propriétaire des actifs informationnels d'utiliser les actifs informatiques de l'entreprise.

- Quelle que soit la manière dont elles sont mentionnées, les politiques et réglementations pertinentes de l'entreprise et la façon dont les informations détenues individuellement sont présentées ne doivent en aucun cas être interprétées comme impliquant que l'entreprise assume une quelconque responsabilité ou approuve les informations détenues individuellement elles-mêmes ou tout document ou opinion qui y est contenu.

Pour toutes les informations détenues individuellement, une mention légale certifiée doit être affichée à l'écran indiquant que ces informations n'ont pas été officiellement publiées par la société.

2.4. L'ensemble du personnel est tenu de respecter les meilleures pratiques en matière de sécurité de l'information afin de garantir la protection adéquate des informations détenues par l'entreprise, quel que soit leur format. Les chefs de service sont responsables de la supervision des pratiques de sécurité de l'information au sein de leurs services respectifs, dans le cadre de leurs responsabilités managériales. À ce titre, ils examinent les actifs détenus par leurs services et sont tenus de mettre en œuvre les mesures et contrôles nécessaires pour garantir que l'inventaire des actifs informationnels de l'entreprise reflète fidèlement l'ensemble des actifs gérés.

2.5. L'inventaire des actifs informationnels aide les services concernés à déterminer le support informatique spécifique requis pour chaque actif informationnel, notamment en matière de sécurité des technologies de l'information et de la communication et de gestion des actifs informatiques, ainsi qu'à mettre en œuvre des contrôles de sécurité de l'information. Bien que cet inventaire soit géré par le responsable informatique, il convient de prendre les précautions nécessaires concernant la sécurité des documents et actifs conservés sur support papier.

2.6. Les ressources informationnelles doivent être identifiées à l'aide de liens logiques et de méthodes de collecte. Par exemple, les informations recueillies pour une étude HSE peuvent être stockées sur différents supports, notamment plusieurs ordinateurs portables, disques durs et clés USB. Dans ce cas, une entrée décrivant chaque support et les mesures de sécurité mises en place doit être consignée.

2.7. Chaque service concerné doit déclarer les actifs informationnels qu'il détient et s'assurer de leur inscription à l'inventaire. Tout système de stockage supplémentaire acquis localement à des fins d'archivage numérique doit être enregistré comme un « Système utilisé par le service ». En cas de doute quant à l'inscription d'actifs informationnels supplémentaires, il convient de contacter l'équipe de support informatique. Les systèmes de stockage en nuage et les systèmes de classement papier doivent également être considérés comme des actifs informationnels et inscrits à l'inventaire.

2.8. Lors de l'examen des actifs informationnels de leurs services, les chefs de service doivent tenir compte des éléments suivants :

• Existe-t-il des actifs informationnels à ajouter à l'inventaire ?

• Tous les actifs informationnels qui ne sont pas utilisés et qui doivent être retirés de l'inventaire
Est-ce possible ?

• Y a-t-il eu un changement dans l'utilisation des actifs informationnels qui nécessiterait une mise à jour des enregistrements dans l'inventaire des actifs informationnels ?

• Existe-t-il des changements de politique ou des réglementations juridiques qui prévoient une modification de la façon dont les ressources informationnelles utilisées par le ministère sont collectées et traitées ?

2.9. Il est admis que les chefs de département ne possèdent pas une connaissance exhaustive de toutes les informations utilisées par le personnel de leur département ni de tous les supports de stockage de ces informations. Il est recommandé aux départements, lors de la constitution de leur inventaire des actifs informationnels, de prendre en compte les risques fondamentaux liés aux informations détenues par le département et à leur lieu de stockage. Les départements pourraient juger utile de se concentrer sur le transfert de données, notamment lorsque celles-ci sont sensibles ou transférées hors de l'établissement. Veuillez contacter l'équipe de sécurité informatique pour obtenir des conseils supplémentaires.

3. STRUCTURE DE L'INVENTAIRE DES ACTIFS INFORMATIFS

Nom de domaine	Explications
Propriétaire des actifs informationnels	Qui est responsable des informations stockées dans cet ensemble de données, et qui est le point de contact/agent de liaison pour les demandes de renseignements concernant cet ensemble de données ?
Gestionnaire d'actifs informationnels	Le rôle du gestionnaire des actifs informationnels est défini dans le document de politique-cadre du SMSI et peut être décrit comme celui de la personne la plus autorisée qui utilise quotidiennement l'actif informationnel.
Nom de l'actif informationnel	Le nom spécifique attribué à l'actif informationnel
Définition d'un actif informationnel	Veuillez fournir une brève description de l'actif informationnel. Si possible, veuillez inclure une courte note d'information sur les données qui seront conservées dans cet actif.
L'état actuel de l'actif est indiqué uniquement dans l'inventaire des actifs informationnels : temporaire, approuvé ou inactif, etc.	
Classification	• Le bien informationnel contient-il des catégories particulières de données ? Quels sont les risques associés à ces données ? Quelles mesures sont prises pour éliminer ou atténuer ces risques ? Les données qui seront considérées comme des données de catégorie spéciale sont les suivantes : o Données relatives à l'administration ou à la recherche de l'entreprise qui sont considérées comme des données commercialement sensibles.

	données. Cela fait référence aux « données relatives à la race, à l'origine ethnique, aux opinions politiques, aux convictions philosophiques, à la religion, à l'appartenance à une secte ou à d'autres croyances, à l'apparence et à l'habillement, à l'appartenance à des associations, des fondations ou des syndicats, à la santé, à la vie sexuelle, aux condamnations pénales et aux mesures de sécurité des individus, ainsi qu'aux données biométriques et génétiques », comme spécifié à l'article 6 de la loi n° 6698. c'est-à-dire des données financières individuelles ; c'est-à-dire des données relatives à des études de Développement recherche commandées par l'entreprise. Les données personnelles non mentionnées ci-dessus, mais dont la divulgation pourrait causer un préjudice ou nuire à la réputation des personnes concernées, doivent également être prises en compte dans cette catégorie.
Lieu de stockage du bien Type d'environnement	Électronique, manuel ou les deux.
Base juridique	Quel est le fondement juridique du traitement et/ou de la conservation des données concernées ? Conformément à la loi n° 6698, les responsables du traitement doivent s'appuyer sur des fondements juridiques légitimes pour traiter les données à caractère personnel de manière licite.
Du point de vue du flux de travail Son importance	L'importance vitale de cet actif informationnel pour le flux de travail de l'entreprise et l'ampleur des conséquences négatives qui surviendraient en cas de perte de cet actif ou de violation de sa confidentialité.
Emplacement de la ressource informationnelle : Où est physiquement stockée la ressource informationnelle ? Par exemple, sur des ordinateurs locaux, dans le système central, sur le portail ou à un emplacement autre que le serveur ?	
Ajout de la ressource d'information Côté	La personne qui a saisi l'enregistrement pertinent dans l'inventaire des actifs informationnels Qui est-ce?
Stockage prévu Durée	Pendant combien de temps ces données seront-elles conservées dans l'inventaire ? Quel est le processus prévu pour déterminer que ces informations ne sont plus nécessaires aux activités de l'entreprise et pour assurer leur destruction sécurisée ? Veuillez consulter la politique de conservation et de destruction des données de l'entreprise concernant le délai après lequel les données doivent être détruites.
Entrée la plus ancienne	La date de l'enregistrement le plus ancien qui ne devrait pas se trouver dans la plage de dates de conservation actuelle.
Dernière entrée dans l'enregistrement	Date de la dernière saisie pour les actifs informationnels qui ne sont plus mis à jour.

Les responsables désignés comme propriétaires d'actifs informationnels doivent également tenir compte des éléments suivants :

- Unité responsable : Quelle unité est responsable de l'actif informationnel en question ? (Généralement l'unité responsable du « propriétaire de l'actif »)
- Quelles unités et/ou personnes auront accès à la ressource informationnelle ? Veuillez préciser les groupes de personnes qui devraient y avoir accès. Par exemple, les employés affectés à une équipe spécifique ou l'ensemble du personnel de l'entreprise. De plus, les tiers qui ne sont pas des employés de l'entreprise mais qui devraient avoir accès à la ressource informationnelle doivent également être clairement identifiés.
- Comment la sécurité des données sera-t-elle assurée ? Décrivez les mesures prises pour garantir leur sécurité. Par exemple, la protection par mot de passe. Les documents contenant des données personnelles sensibles, conservés sur support papier, sont-ils stockés dans un système de classement sécurisé ? Comment ces systèmes de verrouillage sont-ils entretenus ? Attention : Ne divulguez en aucun cas l'emplacement des mots de passe ou des systèmes de

verrouillage ! • Dispositifs de sauvegarde, de résilience et de reprise après sinistre : Quelles mesures sont prises pour récupérer les données et/ou maintenir leur fonctionnalité et leur accessibilité en cas de perte ou de violation de la sécurité des données/systèmes, ou en cas de catastrophe (séisme, etc.) ?