TRANSFERT DE DONNÉES
PROCÉDURES DE SÉCURITÉ ET
À PROPOS DE SES PRINCIPES
RÈGLEMENTS

KVKK_Y8 VERSION 1.00

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

PROCÉDURES ET PRINCIPES DE SÉCURITÉ DES TRANSFERTS DE DONNÉES RÉGLEMENTATIONS CONCERNANT

1. OBJET ET PORTÉE

Dans le cadre de ses activités économiques, notre entreprise stocke une grande quantité de données, sous format électronique et papier. Le présent Règlement relatif aux procédures et principes de sécurité des transferts de données (ci-après dénommé le « Règlement ») vise à encadrer les procédures applicables à la protection des données stockées et à garantir la sécurité des transferts de données personnelles, tant au sein de l'entreprise qu'à l'extérieur.

Le présent règlement s'applique à tous les groupes de personnes suivants au sein de notre société qui traitent des données personnelles et des données personnelles sensibles et qui sont tenus de transférer ces données aux parties prenantes de la société dans le cadre de leurs fonctions :

• Employés •
Fournisseurs et sous-traitants avec lesquels notre entreprise collabore • Stagiaires

Nos employés doivent prendre en compte ce règlement ainsi que le règlement relatif aux procédures et principes concernant l'utilisation des technologies de l'information et de la communication et la politique de sécurité de l'information.
Ils devraient l'acheter.

2. LÉGISLATION PERTINENTE

Loi n° 6698 relative à la protection des données personnelles et réglementations administratives connexes.

3. DONNÉES DE CATÉGORIE SPÉCIALE

Aux fins du présent règlement, les catégories particulières de données comprennent les catégories de données suivantes :

• Les 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 d'une personne, à son appartenance à des associations, des fondations ou des syndicats, à sa santé, à sa vie sexuelle, à ses condamnations pénales et à ses mesures de sécurité, ainsi que les données biométriques et génétiques.

• Les données confidentielles que notre entreprise considère comme des secrets commerciaux. • Les données confidentielles figurant dans les contrats relatifs aux biens, aux services et aux produits.
Toutes les données définies.

• Données confidentielles relatives aux clients et fournisseurs de notre entreprise.

Tout employé ayant le moindre doute quant à la nature des données traitées (données de catégorie spéciale) doit le signaler à son chef de service et agir conformément à ses instructions.

4. CONSIDÉRATIONS À PRENDRE LORS DES TRANSFERTS DE DONNÉES POINTS ESSENTIELS

4.1. Lors du transfert de données personnelles et de données personnelles sensibles, chaque employé doit consulter le chef de département concerné pour obtenir l'autorisation du transfert de données et fournir des instructions.

4.2. Les catégories particulières de données personnelles et les autres données personnelles ne doivent être transférées que dans la mesure absolument nécessaire au bon déroulement des activités légales de notre société. Par conséquent, avant chaque transfert de données, il convient de déterminer au préalable si ce transfert est nécessaire.

4.3. Lors de communications avec des tiers, il convient de vérifier si des accords de partage de données et des protocoles complémentaires relatifs à la protection des données personnelles ont été signés avec les parties concernées. Il convient également de s'assurer de l'existence de dispositions concernant les modalités de transfert de données envisagées et, le cas échéant, de veiller à leur application.

4.4. Il convient de toujours vérifier si les informations fournies ne dépassent pas celles nécessaires à la finalité déclarée. Par exemple, si seule une section ou une partie spécifique d'un document est demandée, le document ou le graphique dans son intégralité ne doit pas être transmis.

4.5. Dans tous les cas où des données personnelles et des informations contenant des catégories particulières de données personnelles sont transférées, l'identité du destinataire et son autorisation d'accès aux données doivent être clairement définies.

5. MÉTHODES DE TRANSFERT DE DONNÉES

Avant de déterminer les méthodes de transfert de données, les points suivants doivent être pris en compte :

• La nature des informations à transmettre, leur sensibilité, leur niveau de confidentialité ou leur potentiel valeur

• La taille des données à transférer •

Les pertes susceptibles d'être subies par les personnes concernées du fait du transfert de données des pertes ou difficultés potentielles qui pourraient subsister

• Les conséquences d'une perte de données pour notre entreprise. • Les

informations et documents non nécessaires à la finalité indiquée ne doivent pas être transférés. Toutes les données inutiles doivent être masquées ou, si nécessaire, supprimées intégralement avant transfert.

5.1. Transferts de données par courrier électronique

• La communication par courriel ne doit pas servir au transfert de données sensibles non chiffrées susceptibles de contenir des renseignements personnels. Nos employés doivent être conscients que le courriel n'est pas conçu pour l'envoi et le transfert de volumes importants de données.

Nos employés doivent privilégier, dans la mesure du possible, l'utilisation de méthodes de transmission sécurisées alternatives pour les données sensibles. À défaut, des mesures de sécurité supplémentaires doivent être mises en œuvre.

Par exemple, le chiffrement doit être utilisé, ou des mots de passe et des identifiants doivent être exigés pour accéder aux données sensibles à transmettre. Lors du transfert de ces identifiants, il convient d'utiliser des méthodes alternatives telles que le courrier postal, les appels téléphoniques à des numéros spécifiques ou les SMS.
• Dans les courriels, des instructions
claires doivent être fournies concernant les responsabilités légales du destinataire ayant reçu les données par erreur, ainsi que la marche à suivre si ce dernier n'est pas la personne autorisée. • Le cas échéant, les informations transmises doivent être jointes dans des fichiers scellés.

Il devrait être envoyé.
• Il convient de veiller à l'exactitude des informations figurant dans l'objet ou le corps du courriel. Le contenu intégral des pièces jointes et les données personnelles sensibles ne doivent pas être divulgués dans le nom du fichier ni dans l'objet. • Les courriels doivent être adressés à l'entreprise afin d'afficher les informations appropriées
relatives à la confidentialité et à la sécurité.
Le transfert doit être effectué à l'aide de l'adresse électronique fournie.

5.2. Portail interne de l'entreprise

• Les utilisateurs qui doivent copier ou transférer des données sur un support amovible, ou qui ont une très grande quantité de données à envoyer, doivent demander l'aide de l'équipe de support informatique de l'entreprise.

• L'accès au portail via un explorateur de fichiers est interdit sans autorisation préalable de l'équipe de support informatique. • Lors du
chargement de données sur le portail, veillez à nommer correctement les fichiers et à les stocker aux emplacements appropriés. Les données sensibles destinées au portail ne doivent pas être stockées dans des emplacements accessibles au public.
• Lors du chargement de données sur le réseau de l'entreprise, il convient d'utiliser un portail sécurisé en suivant les procédures appropriées.
• Chaque donnée à transférer vers des ressources pédagogiques en ligne doit être chiffrée à l'aide d'un document protégé par mot de passe ou d'un fichier zip chiffré.

5.3. Dispositifs de stockage de données amovibles (carte mémoire, clé USB, etc.)

Toutes les données transférées via des supports amovibles, tels que les clés USB, doivent être chiffrées. Les supports de stockage portables chiffrés doivent être protégés par des mots de passe robustes. Si le mot de passe doit être communiqué à un tiers, cette information doit être transmise par d'autres moyens, comme le courrier, le téléphone ou les SMS.

• Les utilisateurs qui doivent copier ou transférer des données sur un support amovible, ou qui ont une très grande quantité de données à envoyer, doivent demander l'aide de l'équipe de support informatique de l'entreprise.

• La propriété des supports amovibles utilisés doit être clairement définie. Ces supports doivent être restitués à leur propriétaire après le transfert de données, et les données transférées doivent être effacées du support après utilisation.
• Dans les cas où le destinataire n'est pas la bonne personne et que des données ont été transférées par erreur, des instructions claires doivent être fournies concernant les responsabilités légales du destinataire et la marche à suivre concernant le courriel entrant.

• Divulgation d'informations sur le contenu du fichier chiffré dans le nom du fichier et les messages joints.
Il ne faut pas le faire.

• L'expéditeur doit confirmer sans délai si le transfert de données a réussi et délivrer un accusé de réception à cet effet.

Les courriels confirmant la réception du fichier peuvent convenir. • Tout problème doit être signalé à la hiérarchie immédiate, et le délégué à la protection des données/agent de liaison doit être informé sans délai de toute perte ou corruption de données.

5.4. Appels téléphoniques

Étant donné que les conversations téléphoniques peuvent être surveillées, entendues ou interrompues (intentionnellement ou accidentellement), les précautions suivantes doivent être prises :

• Les données personnelles ne doivent pas être transmises ni discutées par téléphone sans avoir préalablement vérifié l'identité et l'autorisation du destinataire.
• Lorsque vous utilisez un répondeur, ne laissez pas de messages sensibles ou confidentiels et n'incluez aucune donnée personnelle. Fournissez simplement un moyen de communication et attendez-vous à ce que le destinataire vous réponde personnellement.
• Pendant que vous écoutez les messages vocaux qui vous sont laissés, d'autres personnes pourraient vous écouter aux portes. Veillez à ne pas activer l'enregistrement audio dans les zones ouvertes où il existe un risque d'accidents.

5.5. Transferts de données par voie postale et par coursier

Pour les transferts de données sur supports physiques tels que cartes mémoire ou CD, il est recommandé d'utiliser des services postaux sécurisés. Les services de livraison spéciale et de courrier recommandé sont à privilégier par rapport aux services postaux de première ou deuxième classe. Si vous utilisez un service postal autre que PTT (Poste turque), choisissez une entreprise proposant des services de messagerie sécurisés avec signature à la livraison.

• Le destinataire doit être clairement indiqué sur le formulaire d'expédition postale, et l'emballage physique doit être conçu pour éviter toute casse ou tout dommage. • Les destinataires doivent être informés à l'avance de la date prévue de réception des données. Ils doivent confirmer la réception des données de manière sécurisée dès leur arrivée. L'expéditeur responsable de la transmission des données est tenu de confirmer la bonne réception des données.

5.6. Livraison en main propre

La remise en main propre des documents figure parmi les modes de transfert autorisés. Si une personne est désignée pour recevoir les données à transférer, son identité doit être vérifiée au préalable et des méthodes de vérification d'identité appropriées doivent être utilisées au moment de la remise afin de confirmer que le destinataire est bien la personne prévue.

6. Données manquantes

Lorsqu'un employé constate une perte de données, il doit immédiatement en informer son supérieur hiérarchique direct et le délégué à la protection des données/agent de liaison, et les procédures spécifiées dans le règlement relatif au plan de réponse aux violations de données personnelles doivent être mises en œuvre sans délai.

En cas de suspicion d'accès non autorisé à des données personnelles sensibles, les forces de l'ordre doivent être immédiatement averties.

7. Négligence dans les procédures de transfert de données

Tout employé ne respectant pas les dispositions du présent règlement pourra être considéré comme ayant commis une faute lourde dans l'exercice de ses fonctions et son contrat de travail pourra être résilié. Toute violation de données personnelles pourra entraîner la perte de contact de notre entreprise et de lourdes amendes.

Par conséquent, nos employés doivent faire preuve de la plus grande prudence lors du transfert de données personnelles sensibles. C'est essentiel. Les actions pouvant être considérées comme de la négligence et un comportement fautif incluent : le transfert de données sans autorisation, le défaut de chiffrement adéquat des données, l'absence de protection par compression et chiffrement, le défaut d'utilisation de services postaux recommandés ou assurés, etc.