SÉCURITÉ DE L'INFORMATION ET POLITIQUE-CADRE DE PROTECTION DES DONNÉES PERSONNELLES

Numéro de document	KVKK_P1 VERSION 1.00
Date de révision	-
Date de publication	27/05/2024
Page	13

KARDELEN PAINT AND CHEMICAL INDUSTRY TRADE LIMITED COMPANY

CADRE DE SÉCURITÉ DE L'INFORMATION ET DE PROTECTION DES DONNÉES PERSONNELLES

POLITIQUE

1. INTRODUCTION ET OBJECTIF

1.1. Ce document a été préparé pour définir la politique-cadre de sécurité de l'information et des données personnelles de Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi (ci-après dénommée la politique-cadre), dont les détails sont donnés ci-dessous.

Responsable du traitement des données	Kardelen Paint and Chemical Industry Trade Limited Company: Alcı OSB
Adresse	Mah. 2036 Cad. No:7 Sincan/Ankara, Turquie
Téléphone	+90 312 398 11 33
Mail	kvkk@kardelenboya.com.tr
Site web	: http://www.kardelenboya.com.tr/ Production
Domaine d'activité	de peinture

Cette politique-cadre donne un aperçu général des politiques, réglementations, déclarations de divulgation et directives applicables de notre société en matière de sécurité de l'information et de protection des données personnelles, et vise également à démontrer l'engagement de la société en matière de formation et de sensibilisation dans ces domaines.

1.2. La présente politique-cadre vise à réunir les conditions nécessaires et valides pour un traitement licite, sécurisé, efficace et efficient de toutes les informations et données recueillies par notre société. Le traitement des informations et des données est essentiel au bon fonctionnement et à la gestion des opérations quotidiennes de notre société. La qualité, la planification, l'évaluation des performances, la sécurité au travail, l'assurance et la gestion financière des services offerts par la société dépendent largement de processus de collecte et de traitement des informations précis et fiables. Une gouvernance de l'information saine et fiable exige une gestion et une responsabilisation ouvertes et efficaces, des processus de gouvernance, des politiques et procédures documentées, un personnel formé et des ressources suffisantes. En conséquence, la présente politique-cadre définit les conditions, les normes et les bonnes pratiques applicables en matière de gestion des ressources informationnelles et de traitement licite des données personnelles.

1.3. La sécurité des informations et la protection des données personnelles constituent une responsabilité importante pour chaque employé de notre entreprise. Chaque employé est responsable de la mise en œuvre des pratiques de travail de l'entreprise et de l'intégration de ses politiques et règles de travail.
Il est donc essentiel que chacun de nos employés prenne connaissance des points énoncés dans le présent document-cadre. Les tiers utilisant les données de l'entreprise sont également tenus de respecter les principes qui y sont définis.

1.4. La présente politique-cadre a pour but d'aider notre entreprise à s'acquitter des responsabilités suivantes :

• Respect des obligations légales, administratives et contractuelles ;
• Garantir une saine gouvernance d'entreprise ; • Fournir des services de haute qualité ; • Protéger les ressources financières de l'entreprise ; • Planifier des processus de continuité des activités appropriés ; • Assurer la sécurité continue des transactions de données sous le contrôle de l'entreprise.
approvisionnement et développement.

1.5. L'entreprise effectue quotidiennement un large éventail d'activités standard et spécialisées de collecte et de traitement de données personnelles nécessaires à la fourniture de services, assurant la continuité des relations et engagements commerciaux et garantissant la sécurité d'emploi de ses employés.

2. CHAMP D'APPLICATION

2.1. La présente politique-cadre s'applique à toutes les données détenues par notre société et traitées par des tiers traitant des données pour le compte de la société, y compris les données énumérées ci-dessous à titre d'exemples, qu'elles soient sous forme électronique ou physique :

• Stocké par des ordinateurs de bureau ou portables et des périphériques de stockage
• Données électroniques traitées ; •
Données transmises sur des réseaux ;
• Informations transmises par télécopie et autres méthodes de transfert de données similaires ; •
Documents conservés sur tous types de supports papier ; •
Documents visuels et photographiques, y compris les microfiches, les diapositives et les enregistrements de systèmes de caméras en circuit fermé ;
• Données de communication verbale, y compris la communication en face à face, les messages vocaux et les conversations enregistrées.

2.2. Les parties énumérées ci-dessous doivent se conformer aux procédures et principes énoncés dans le présent document-cadre. Il est nécessaire de :

• Tous les employés de l'entreprise ;
• Toutes les tierces parties autorisées à accéder aux données de l'entreprise, y compris les consultants, les prestataires de services et les sous-traitants, ainsi que les visiteurs.

2.3. La présente politique-cadre se compose de deux parties. La première décrit la stratégie de notre entreprise en matière de sécurité de l'information et de protection des données personnelles, tandis que la seconde…

Cette section décrit les rôles et les responsabilités des parties prenantes concernées à cet égard, ainsi que les politiques et les programmes de formation à mettre en œuvre dans ce domaine.

2.4. Vous trouverez ci-dessous des informations sur la manière dont les données sous le contrôle de la Société seront classées. est fourni :

(1) Les « Données personnelles » désignent toute information se rapportant à une personne physique identifiée ou identifiable (« personne concernée »). Une personne physique identifiée est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Les procédures et principes énoncés dans la Politique de traitement et de protection des données personnelles de l'entreprise doivent être respectés lors de la collecte, de l'utilisation et du stockage des données personnelles.

(2) Les données relatives à l'origine raciale ou 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, ainsi qu'aux données biométriques et génétiques, constituent des catégories particulières de données à caractère personnel. Les conditions supplémentaires et les mesures de protection visant à renforcer la sécurité du traitement de ces catégories particulières de données sont précisées dans la Politique de traitement et de protection des données personnelles et la Politique de sécurité des données de l'entreprise.

(3) Les données suivantes, à l'exclusion des données personnelles, sont des données d'entreprise de la société : seront désignées par le terme « données » :

(a) Données de planification/administratives ou de recherche, informations juridiquement privilégiées protégées par des accords et clauses de confidentialité, etc., qui sont commercialement protégées.
Données d'entreprise sensibles. Ces données doivent être protégées par les mesures de sécurité les plus avancées ;

(b) Données non privées relatives à l'entreprise qui n'ont pas été divulguées publiquement et qui peuvent être divulguées en vertu d'obligations légales telles que la loi sur la liberté d'information.

3. OBJECTIF

3.1. La stratégie de notre entreprise vise à garantir à nos clients, partenaires et fournisseurs que les données sont traitées et stockées dans le respect de leur valeur et des risques encourus, et à assurer le respect de nos obligations légales en matière de gestion et de sécurité de l'information, ainsi que de protection des données personnelles. Toutes les parties concernées doivent comprendre l'importance d'une utilisation appropriée des données, de leur collecte et de leur traitement licites, et de leur protection contre toute utilisation abusive.

3.2. L'objectif de cette stratégie est de garantir que notre société agisse conformément aux responsabilités légales et éthiques applicables dans les domaines suivants :

• Traitement licite des données relatives à des personnes identifiées ou identifiables
son utilisation et la protection de sa sécurité ;
• L'accès aux données ne doit se faire que dans le respect de la loi.
• Transfert de données
personnelles aux personnes physiques ; • Mise en place d'un cadre réglementaire applicable à la gestion
de l'information ; • Dispositions relatives à l'enregistrement, au partage et à l'utilisation des données personnelles.
Code de conduite relatif à l'obtention d'un consentement explicite ;
• Code de déontologie et pratiques professionnelles acceptés par l'entreprise
Les directives
comprennent : • Le partage mutuel d'informations et de données avec des tiers.

3.3. La stratégie vise à maintenir des normes de sécurité appropriées dans le domaine de la gestion de l'information, en plus des normes élevées attendues de l'identité de l'entreprise, et à établir pleinement une culture de sécurité des données personnelles dans toute l'entreprise.

3.4. Les objectifs stratégiques de l'entreprise en matière de sécurité de l'information et de protection des données personnelles sont énumérés ci-dessous :

• La gestion de l'information doit soutenir la stratégie globale de l'entreprise, ses sous-stratégies et ses programmes de transformation. La sécurité de l'information doit être un élément essentiel de l'élaboration et de la mise en œuvre de ces stratégies et programmes. • L'infrastructure et les processus nécessaires doivent être mis en place pour garantir que la bonne information
parvienne à la bonne personne, au bon moment et pour le bon usage. Il convient également d'identifier l'infrastructure et les processus nécessaires pour assurer une diffusion éthique, légale, efficace et appropriée de cette information.

• Développer des solutions innovantes en matière de gouvernance de l'information, en tenant compte de la transformation des processus métier ; • Intégrer la gouvernance de
l'information dans les opérations administratives de l'entreprise en mettant en œuvre des changements comportementaux globaux afin de reconnaître l'information comme un atout fondamental ;

• Aspects spécifiques de la gouvernance de l'information liés aux qualifications des employés et aux descriptions de poste.
établir les conditions;
• Encourager les employés à travailler ensemble pour éviter les efforts inutiles et assurer une utilisation plus efficace des ressources ; • Veiller à ce que les normes applicables soient en place pour se
conformer aux obligations et politiques légales, administratives et contractuelles ;

• Identifier et gérer les ressources informationnelles au sein de l'entreprise et établir un régime de gestion des risques liés à l'information qui équilibre les risques et les opportunités applicables à ces ressources informationnelles ;
• Garantir la confiance de toutes les parties concernées en mettant en œuvre les mesures nécessaires et proportionnées pour appliquer les meilleures pratiques en matière de protection des ressources informationnelles ;
• Assurer une formation adéquate à tous nos employés et principaux partenaires, sensibiliser leurs niveaux de compétence et veiller à ce que toutes les données et informations traitées au sein de l'entreprise soient correctement comprises.

Créer un environnement culturel propice à l'examen des problèmes avec un sens des responsabilités et du devoir.

4. L'APPROCHE DE NOTRE ENTREPRISE

4.1. La sécurité des informations et la confidentialité des données personnelles sont pleinement intégrées aux activités de notre entreprise. À cet égard, quatre éléments principaux de son fonctionnement sont pris en compte :

- Élément humain
- Processus
- Informatique

4.2. Dans les activités de gouvernance, de développement et de protection de l'information, les facteurs énumérés ci-dessus sont évalués en fonction de leur contribution à la réalisation de nos objectifs stratégiques.

4.3. Nos objectifs stratégiques en matière de gouvernance de l'information seront atteints grâce aux politiques qui seront mises en place. Lors de l'élaboration de nouveaux programmes et processus d'entreprise, chaque projet de gestion de l'information sera défini, mis en œuvre et suivi conformément aux approches et aux réglementations administratives décrites dans la présente politique-cadre.

4.4. La mise en œuvre de la stratégie susmentionnée devrait produire les avantages suivants :

- Les informations et les données traitées au sein de l'entreprise le sont de manière cohérente et efficace. gestion;
- Une meilleure compréhension de la législation pertinente et du niveau de conformité à ses dispositions croissant;
- Événements survenant et affectant la sécurité de l'information et la confidentialité des données personnelles réduisant considérablement sa fréquence ;
- Le temps et les efforts que les employés doivent consacrer à cette question
  - Réduire ; •

Améliorer la qualité des données ; •

Définir clairement les responsabilités à assumer en matière de gestion et de sécurité de l'information.

être présenté d'une manière ou d'une autre ;

- Gérer efficacement les risques qui menacent la sécurité des informations et des données ;

4.5. Le directeur général de l'entreprise est responsable de la mise en œuvre de cette stratégie. Le Comité de protection des données personnelles, présidé par le directeur général, est chargé de suivre l'application de la présente politique-cadre et des politiques et directives connexes tout au long de l'année et de rendre compte des progrès accomplis. La stratégie de sécurité de l'information et de protection des données personnelles sera mise en œuvre au moyen de politiques, de programmes de développement et de projets convenus. Le Comité de protection des données personnelles procédera à un examen de la stratégie à la fin de chaque année.

En fonction des priorités convenues et des ressources disponibles, le directeur général validera les programmes de développement prévus pour l'année suivante. Le directeur général approuvera ensuite les programmes de développement validés par le Comité de protection des données personnelles.

4.6. Définitions

4.6.1 SMSI : Système de gestion de la sécurité de l'information.

4.6.2 Inventaire : Tous les actifs informationnels importants pour l'entreprise.

4.6.3 Direction générale : Ceci fait référence à la haute direction de l'entreprise.

4.6.4 Savoir-faire : La capacité de faire quelque chose.

4.6.5 Informations confidentielles : Les informations, comme tous les autres actifs de l'entreprise, constituent un atout précieux qui doit être protégé de manière appropriée. Au sein d'une entreprise, le savoir-faire, les procédés, les formules, les techniques et les méthodes, les données clients, les informations marketing et commerciales, les informations relatives au personnel, les informations commerciales, industrielles et technologiques ainsi que les secrets sont considérés comme des INFORMATIONS CONFIDENTIELLES.

4.6.6 Confidentialité : Il s'agit de limiter l'accès au contenu des informations aux seules personnes autorisées à les consulter. (Exemple : L'envoi de courriels chiffrés empêche les personnes non autorisées de lire les courriels, même en cas d'interception – Courrier électronique recommandé – KEP)

4.6.7 Intégrité : Il s'agit de garantir que toute modification, suppression ou ajout non autorisé ou accidentel d'informations puisse être détecté et que la traçabilité soit assurée. (Exemple : Stockage des données dans la base de données avec des informations récapitulatives – signature électronique – signature mobile)

4.6.8 Disponibilité : Ce terme désigne la capacité du matériel à être prêt à l'emploi à tout moment. Autrement dit, les systèmes doivent être disponibles en permanence, les données qu'ils contiennent ne doivent pas être perdues et ils doivent être accessibles en permanence. (Exemple : Utilisation d'onduleurs et d'alimentations redondantes dans le châssis des serveurs pour les protéger des fluctuations et des coupures de courant).

4.6.9 Actifs informationnels : Il s'agit des actifs appartenant à la Société et indispensables au bon déroulement de ses activités. Dans le cadre des processus couverts par la présente politique, les actifs informationnels comprennent notamment :

- Tous les types d'informations présentées sur support papier, électronique, visuel ou auditif, et données,
- Tout logiciel utilisé pour accéder aux informations et les modifier, et matériel,
- Les réseaux qui permettent le transfert d'informations,

• Installations et espaces privés,

• Départements, unités, équipes et employés,

• Partenaires de solutions,

• Il s'agit de services, de produits ou d'offres fournis par des tiers.

4.7. L'organigramme figurant en annexe à la présente politique-cadre précise les acteurs et leurs rôles dans la gouvernance de l'information au sein de la Société.

4.7.1 Responsabilité de la direction

- La direction s'engage à respecter le système de sécurité de l'information et de protection des données personnelles défini, mis en œuvre et applicable, à allouer les ressources nécessaires à son bon fonctionnement et à veiller à ce qu'il soit compris par tous les employés. Le directeur général est responsable de l'évaluation et de la réduction des risques liés à la sécurité de l'information et s'assure que les politiques et les actions de sensibilisation pertinentes sont diffusées auprès de tous les employés concernés. Les risques liés à la sécurité de l'information et des données sont traités au même titre que les autres risques financiers, juridiques et de réputation.

- Lors de la mise en place du système de sécurité de l'information et de protection des données personnelles, un délégué à la protection des données est désigné par un document de mission écrit. Ce document peut être révisé par la direction et la désignation reconduite si nécessaire.

- Les cadres supérieurs aident les employés de niveau inférieur en leur confiant des responsabilités et en montrant l'exemple en matière de sécurité. Cette approche, initiée par la direction et mise en œuvre jusqu'aux employés les plus bas de l'échelle, est essentielle.
Par conséquent, tous les responsables encouragent leurs employés, par écrit et verbalement, à suivre les consignes de sécurité et à participer aux activités liées à la sécurité.

- La haute direction a alloué le budget nécessaire aux efforts globaux en matière de sécurité de l'information. Cela crée.

Le responsable de la liaison avec les données est chargé, auprès de la direction générale désignée, de signer les accords de partage et de traitement des données ainsi que les protocoles complémentaires avec les parties prenantes concernées, et de préparer les autres accords et protocoles applicables à l'accès aux données et au transfert de données requis dans le cadre des activités de l'entreprise.

4.7.2. Personne de contact pour les données

Le responsable de la liaison avec les données est chargé de préparer et de mettre en œuvre la vision, les stratégies et les programmes d'entreprise nécessaires à la protection des actifs et des systèmes d'information de l'entreprise. Ses fonctions à cet égard sont énumérées ci-dessous :

- La planification du système de sécurité de l'information et de protection des données personnelles est acceptable. déterminer le niveau de risque, déterminer la méthodologie d'évaluation des risques,

- Fournir les ressources nécessaires aux activités de soutien et de complémentarité pour la mise en place du système de sécurité de l'information et de protection des données personnelles, garantir/améliorer les capacités des utilisateurs et sensibiliser, organiser des formations, assurer la communication et fournir la documentation requise.

- Mise en œuvre et gestion des applications des systèmes de sécurité de l'information et de protection des données personnelles, en assurant la continuité des évaluations, des améliorations et des analyses de risques,

- Audits internes, réunions d'examen des objectifs et de la direction, et sécurité de l'information et l'évaluation du système et des contrôles de protection des données personnelles,

- Maintenir la structure actuelle et assurer des améliorations continues du système de sécurité de l'information et de protection des données personnelles.

4.7.3 Chefs de département

- Réaliser des inventaires d'actifs et des études d'analyse des risques liés aux départements,

- Le responsable de la protection des données est tenu de procéder à une évaluation des risques chaque fois qu'un changement survient dans les actifs informationnels sous sa responsabilité et susceptible d'affecter les risques liés à la sécurité de l'information. information,

- Les employés placés sous sa supervision doivent se conformer aux politiques et règlements de l'entreprise. veiller à ce qu'il fonctionne conformément aux procédures,

- Sensibiliser et assurer la communication dans le cadre du SMSI concernant les départements, Fournir les exigences en matière de documentation,

- Dans le cadre du SMSI, il s'agit de maintenir la structure actuelle et d'assurer des améliorations continues. est responsable.

- Les chefs de service sont responsables de l'évaluation des aspects liés à la gestion de l'information dans les processus de travail de leurs services et dans les activités menées en collaboration avec les parties prenantes. Veuillez consulter la politique de sécurité de l'information pour connaître les responsabilités spécifiques en matière de sécurité de l'information.

4.7.4 Responsabilité de tous les employés

- Ils sont responsables de mener leur travail conformément aux objectifs, aux politiques et aux documents du système de gestion de la sécurité de l'information.

- Assurer le suivi des objectifs de sécurité de l'information liés à sa propre unité et contribuer à la réalisation de ces objectifs.

- Tout problème de sécurité de l'information observé ou suspecté dans les systèmes ou les services.
en prêtant attention et en signalant toute faille ou violation,

- Outre les contrats de service (conseil, etc.) conclus avec des tiers qui ne relèvent pas de la responsabilité de l'acheteur, ce dernier est responsable de l'établissement d'accords de confidentialité et du respect des exigences en matière de sécurité de l'information.

- Tous les employés de l'entreprise et les tiers autorisés à accéder à ses ressources informationnelles doivent se conformer aux lois et réglementations en vigueur et être conscients de leurs responsabilités personnelles en matière de gestion de l'information. Tous les employés doivent respecter les politiques, procédures et directives établies par l'entreprise et participer aux formations et événements relatifs à la gestion de l'information.

5. PRINCIPES GÉNÉRAUX DE LA SÉCURITÉ DE L'INFORMATION

5.1. Les employés de la société et les tiers sont tenus de connaître les détails et les procédures concernant les exigences et les règles de sécurité de l'information énoncées dans la présente politique-cadre et de mener leur travail conformément à ces règles.

5.2. Sauf indication contraire, ces règles et politiques doivent être respectées pour toutes les informations stockées et traitées sous forme imprimée ou électronique, et pour l'utilisation de tous les systèmes d'information.

5.3. Le système de sécurité de l'information et de protection des données personnelles est structuré et exploité conformément à la loi turque sur la protection des données personnelles (KVKK), au RGPD et à la norme TS ISO/IEC 27001 « Techniques de sécurité des technologies de l'information et exigences relatives aux systèmes de gestion de la sécurité de l'information ».

5.4. La mise en œuvre, l'exploitation et l'amélioration du système de sécurité de l'information et de protection des données personnelles sont réalisées avec la contribution des parties prenantes. Le délégué à la protection des données est responsable de la mise à jour des documents pertinents.
C'est leur responsabilité.

5.5. Sauf disposition contraire de la loi ou du contrat, les systèmes d'information et l'infrastructure fournis par la société aux employés ou aux tiers, ainsi que toutes les informations, documents et produits produits à l'aide de ces systèmes, appartiennent à Kardelen Boya ve Kimya Sanayi Ticaret Limited Şirketi.

5.6. Des accords de confidentialité sont signés avec les employés, les consultants, les prestataires de services (sécurité, transport, restauration, entreprises de nettoyage, etc.), les fournisseurs et les stagiaires.

5.7. Informations à appliquer dans les processus de recrutement, de changement d'emploi et de cessation d'emploi. Des contrôles de sécurité sont définis et mis en œuvre.

5.8. Des sessions de formation visant à sensibiliser les employés à la sécurité de l'information et à leur permettre de contribuer au fonctionnement du système sont régulièrement proposées aux employés actuels et aux nouveaux employés.

5.9. Toutes les violations réelles ou suspectées de la sécurité de l'information sont signalées ; les irrégularités qui ont causé les violations sont identifiées, leurs causes profondes sont déterminées et des mesures sont prises pour empêcher leur récurrence.

5.10. Un inventaire des actifs informationnels est créé et la propriété des actifs est attribuée conformément aux besoins de gestion de la sécurité de l'information.

5.11. Les données personnelles et professionnelles sont classées et la sécurité des données dans chaque classe est assurée. Les besoins et les règles d'utilisation sont déterminés.

5.12. Sécurité physique conforme aux besoins des biens stockés dans des zones sécurisées.
Des contrôles sont appliqués.

5.13. Exposition des actifs informationnels de l'entreprise, tant à l'intérieur qu'à l'extérieur de l'organisation.
Des contrôles et des politiques nécessaires sont élaborés et mis en œuvre pour contrer les menaces physiques.

5.14. Des procédures et des instructions sont élaborées et mises en œuvre concernant la gestion des capacités, les relations avec les tiers, la sauvegarde, l'acceptation du système et d'autres processus de sécurité.

5.15. Les configurations de génération des journaux d'audit pour les périphériques réseau, les systèmes d'exploitation, les serveurs et les applications sont ajustées en fonction des besoins de sécurité des systèmes respectifs.
Les enregistrements d'audit sont protégés contre tout accès non autorisé.

5.16. Les droits d'accès sont attribués selon les besoins. Les technologies et techniques les plus sécurisées possibles sont utilisées pour le contrôle d'accès.

5.17. Les exigences de sécurité sont déterminées lors de l'acquisition et du développement du système.
Lors de la réception ou des essais, on vérifie si les exigences de sécurité sont respectées.

5.18. Des plans de continuité sont préparés, maintenus et mis en pratique pour les infrastructures critiques.

5.19. Les processus sont conçus pour assurer la conformité aux lois, aux politiques et procédures nationales et aux normes techniques de sécurité ; la conformité est assurée par des activités de surveillance et d'audit continues et périodiques.

6. POLITIQUES À ÉTABLIR DANS LE CADRE DE LA POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION ET AUX DONNÉES PERSONNELLES

6.1. Les règlements définissant les politiques et les codes de conduite qu'il est prévu d'établir dans le cadre de la politique relative à la sécurité de l'information et aux données personnelles sont les suivants :

RÉFÉRENCE DU TYPE DE DOCUMENT	NOMBRE	TITRE
POLITIQUE	KVKK_P1	SÉCURITÉ DES INFORMATIONS ET PERSONNALITÉ POLITIQUE DU CADRE DE DONNÉES
POLITIQUE	KVKK_P2	PROTECTION DES DONNÉES PERSONNELLES ET SA POLITIQUE DE TRAITEMENT
POLITIQUE	KVKK_P3	POLITIQUE DE STOCKAGE ET DE DESTRUCTION DES DONNÉES PERSONNELLES

POLITIQUE	KVKK_P4	RENSEIGNEMENTS PERSONNELS CONCERNANT LE PERSONNEL DONNÉES PROTECTION POLITIQUE
POLITIQUE	KVKK_P5	POLITIQUE DE SÉCURITÉ DE L'INFORMATION
POLITIQUE	KVKK_P6	INFORMATION ET COMMUNICATION UTILISATION DES TECHNOLOGIES POLITIQUE
POLITIQUE	KVKK_P7	POLITIQUE DE CONTRÔLE D'ACCÈS
POLITIQUE	KVKK_P8	SYSTÈMES DE CAMÉRAS INTÉRIEURES POLITIQUE
POLITIQUE	KVKK_P9	ACCEPTATION D'INTERNET ET DES OUTILS DE COMMUNICATION ÉLECTRONIQUE peut être fait USAGE PROCÉDURES ET PRINCIPES CONCERNANT POLITIQUES LIÉES
POLITIQUE	KVKK_P10	POLITIQUE RELATIVE AUX CAMÉRAS EMBARQUÉES
RÈGLEMENTS	KVKK_Y1	SUJETS DE DONNÉES À LEURS DEMANDES À DONNER PRINCIPES ET PROCÉDURES POUR LES RÉPONSES RÉGLEMENTATIONS CONCERNANT
RÈGLEMENTS	KVKK_Y2	PLAN D'INTERVENTION EN CAS DE VIOLATION DE DONNÉES RÈGLEMENT
RÈGLEMENTS	KVKK_Y3	IMPACT SUR LA PROTECTION DES DONNÉES PROCÉDURE D'ÉVALUATION ET À PROPOS DE SES PRINCIPES RÈGLEMENTS
RÈGLEMENTS	KVKK_Y4	COMMUNICATIONS ÉLECTRONIQUES ET DONNÉES ÉLECTRONIQUES À PROPOS DE L'INSPECTION RÈGLEMENTS
RÈGLEMENTS	KVKK_Y5	MESSAGERIE ÉLECTRONIQUE PROCÉDURE D'UTILISATION ET RÉGLEMENTATION RELATIVE À SES PRINCIPES
RÈGLEMENTS	KVKK_Y6	CAMÉRA EN CIRCUIT FERMÉ PROCÉDURES D'UTILISATION DES SYSTÈMES ET SUR SES PRINCIPES RÈGLEMENTS
RÈGLEMENTS	KVKK_Y7	MOTS DE PASSE UTILISATEUR IDENTIFICATION, UTILISATION ET PROCÉDURES RELATIVES À SA PROTECTION À PROPOS DES PRINCIPES RÈGLEMENTS
RÈGLEMENTS	KVKK_Y8	PROCÉDURE DE SÉCURITÉ DES TRANSFERTS DE DONNÉES ET SUR SES PRINCIPES RÈGLEMENTS
TEXTE DE PROTECTION DES DONNÉES	KVKK_A1	VALABLE POUR LES CANDIDATURES À UN EMPLOI. Texte d'information sur le RGPD
TEXTE DE PROTECTION DES DONNÉES	KVKK_A2	INTERNET COOKIES DU SITE USAGE À PROPOS TEXTE D'INFORMATION

TEXTE DE PROTECTION DES DONNÉES	KVKK_A3	SYSTÈMES DE CAMÉRAS INTÉRIEURES TEXTE D'INFORMATION
TEXTE DE PROTECTION DES DONNÉES	KVKK_A4	Texte d'information sur la loi relative à la protection des données personnelles (KVKK)
TEXTE DE PROTECTION DES DONNÉES	KVKK_A5	ÉCLAIRAGE DU SITE WEB TEXTE
TEXTE DE PROTECTION DES DONNÉES	KVKK_A6	PROTECTION DES DONNÉES PERSONNELLES À PROPOS DE L'ENTREPRENEUR TEXTE D'INFORMATION
TEXTE DE PROTECTION DES DONNÉES	KVKK_A7	TEXTE D'INFORMATION POUR LES VISITEURS
FORMULAIRE	KVKK_F1	IMPACT SUR LA PROTECTION DES DONNÉES FORMULAIRE D'ÉVALUATION
ACCORD	KVKK_S1	DONNÉES PERSONNELLES ANNEXE RELATIVE À SA PROTECTION PROTOCOLE

6.2. Élaboration des politiques

6.2.1. Le Comité de protection des données personnelles examine toutes les politiques de gestion de la sécurité de l'information et, le cas échéant, soumet ses recommandations de modifications à la direction. Toutes les politiques établies et leurs mises à jour sont communiquées aux employés via le portail de l'entreprise ou Internet.

6.2.2. Les politiques sont revues annuellement et mises à jour au besoin. De nouvelles politiques peuvent être établies pour remédier aux lacunes. Le cas échéant, ces politiques sont examinées en lien avec le contrat de travail de l'employé.

6.2.3. Les politiques établies dans le cadre de la présente politique définiront le champ d'application et l'objectif de la sécurité de l'information et fourniront un cadre de gestion de cette sécurité, précisant les responsabilités du personnel et des autres parties prenantes. L'entreprise s'engage à prendre les mesures nécessaires pour informer ses employés et ses partenaires commerciaux de ses objectifs et des responsabilités attendues des parties prenantes concernées pour les atteindre. À cet égard, les politiques et règlements établis jouent un rôle essentiel pour informer les employés et les partenaires commerciaux de leurs obligations.

6.3. Formation et perfectionnement

6.3.1. Les programmes de formation et de développement en matière de gestion de la sécurité de l'information sont essentiels pour améliorer et renforcer les connaissances et les compétences du personnel de l'ensemble de l'entreprise en matière de gestion de la sécurité de l'information.

6.3.2. La formation en gestion de la sécurité de l'information devrait inclure des sujets allant au-delà de la sensibilisation de base à la confidentialité et à la sécurité afin de développer et de surveiller les meilleures pratiques.

Le personnel doit comprendre la valeur de l'information et ses responsabilités, notamment en matière de qualité des données, de sécurité de l'information, de gestion des dossiers, de confidentialité, etc.

7. SURVEILLANCE DU RESPECT DE LA POLITIQUE-CADRE

7.1. Le Comité des données personnelles est chargé de veiller au respect de la présente politique-cadre et de réviser et de mettre à jour chaque politique pertinente.

7.2. Les politiques et procédures doivent être revues au moins une fois par an. Elles doivent également être revues après toute modification affectant la structure du système ou l'évaluation des risques, et toute modification nécessaire doit être approuvée par la direction et consignée dans une nouvelle version. Chaque révision doit être publiée de manière à être accessible à tous les utilisateurs.

7.3. Les réunions d'examen de la direction sont organisées par le responsable de la liaison avec les données et se tiennent avec la participation de la direction générale et des chefs de service. Ces réunions, au cours desquelles la pertinence et l'efficacité du système de gestion de la sécurité de l'information sont évaluées, ont lieu au moins une fois par an.

8. VIOLATION DES POLITIQUES ET SANCTIONS

S’il est établi que la politique et les normes relatives au cadre de sécurité de l’information et aux données personnelles n’ont pas été respectées, les employés responsables de cette violation seront passibles des sanctions prévues dans les clauses pertinentes des contrats, lesquelles sont également applicables aux tiers, conformément à la directive et à la procédure disciplinaires.