Machine Translated by Google

INTERVENTION EN CAS DE FUITE DE DONNÉES

RÉGLEMENTATION DE L'AMÉNAGEMENT

KVKK_Y2 VERSION 1.00

Machine Translated by Google

1. OBJET ET PORTÉE

1.1. Kardelen Paint and Chemical Industry Trade Limited Company (ci-après dénommée « la Société »)

Le présent Plan de réponse aux violations de données personnelles (ci-après dénommé « le Plan ») a été adopté par notre société dans le cadre de sa planification stratégique afin de garantir sa capacité à réagir immédiatement en cas de violation de la sécurité des données, conformément aux dispositions de la décision n° 2019/10 de l'Autorité de protection des données personnelles du 24 janvier 2019 relative aux procédures et principes de notification des violations de données personnelles. Cette décision stipule qu'« en cas de violation de données, le responsable du traitement doit élaborer un plan de réponse précisant notamment à qui signaler la violation au sein de son organisation, qui est responsable des notifications à effectuer conformément à la loi et comment évaluer les conséquences potentielles de la violation. Ce plan doit être révisé à intervalles réguliers. » L'objectif principal du plan de réponse mis en œuvre en cas de violation est d'agir rapidement pour protéger les personnes et leurs données personnelles. Notre société prévoit de mener les actions suivantes en cas de violation de données :

(a) Notifier sans délai indu et au plus tard 72 heures après avoir pris connaissance de la violation de données à l'Autorité de protection des données personnelles (l'Autorité) (la Société a le pouvoir discrétionnaire de décider de notifier ou non la violation de données à caractère personnel si celle-ci est peu susceptible de constituer un risque pour les droits et libertés fondamentaux).

(b) Notifier sans délai indu les personnes concernées, sauf si la probabilité d'une violation de données à caractère personnel susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques est faible.

1.2. Le présent règlement :

a) Ce document sera communiqué à tous les sous-traitants concernés. Ces derniers sont tenus de nous informer immédiatement de toute violation de la sécurité des données personnelles qu'ils traitent pour le compte de notre société dès qu'ils en ont connaissance.

(b) Les dispositions du plan d'intervention seront communiquées à nos employés dès leur entrée en fonction et seront discutées lors de réunions périodiques du personnel et de séances de formation afin de garantir que le personnel soit informé du plan.

1.3. Étapes à suivre dans l'organigramme, qui fait partie intégrante du présent règlement.
Cela a été résumé.

1.4. Définitions : Les définitions applicables aux dispositions du présent règlement sont données ci-dessous.

Ils sont énumérés comme suit :

1.4.1. Connaissance de la violation : Un responsable du traitement des données est réputé « avoir connaissance de la violation » lorsqu'il a un degré raisonnable de certitude qu'une violation de sécurité s'est produite et compromet la sécurité des données personnelles.

1.4.2. Dommages : données personnelles altérées, corrompues ou incomplètes.

Machine Translated by Google

1.4.3. Destruction : Données qui ne sont plus disponibles ou que le responsable du traitement des données a perdues de quelque manière que ce soit.
non disponible sous une forme utilisable par lui/elle.

1.4.4. Perte : Les données peuvent encore être disponibles, mais le responsable du traitement a perdu le contrôle des données.
Ils ont perdu le contrôle ou l'accès aux données, ou ne les possèdent plus.

1.4.5. Une violation de données personnelles est une violation de sécurité qui entraîne la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé, accidentels ou illégaux, à des données personnelles transmises, stockées ou traitées ;

1.4.6. « Perte temporaire de données » : rendre les données personnelles inutilisables pendant une période donnée.
l'événement qui l'a provoqué.

1.4.7. « Traitement non autorisé ou illicite » désigne la divulgation (ou l'accès) de données personnelles à des destinataires qui ne sont pas autorisés à recevoir (ou à accéder) aux données, ou toute autre forme de traitement qui viole les dispositions de la loi n° 6698.

1.5. Une violation de la sécurité des données peut survenir pour diverses raisons, notamment les suivantes :

• Erreur humaine

• Perte ou vol de documents ou d'appareils contenant des données personnelles

• Entrée non autorisée, vol, cambriolage

• Mise en œuvre de contrôles d'accès inadéquats permettant une utilisation/un accès non autorisé

• Pannes d'équipement et systèmes de sauvegarde inadéquats

• Les situations de catastrophe telles que les inondations ou les incendies.

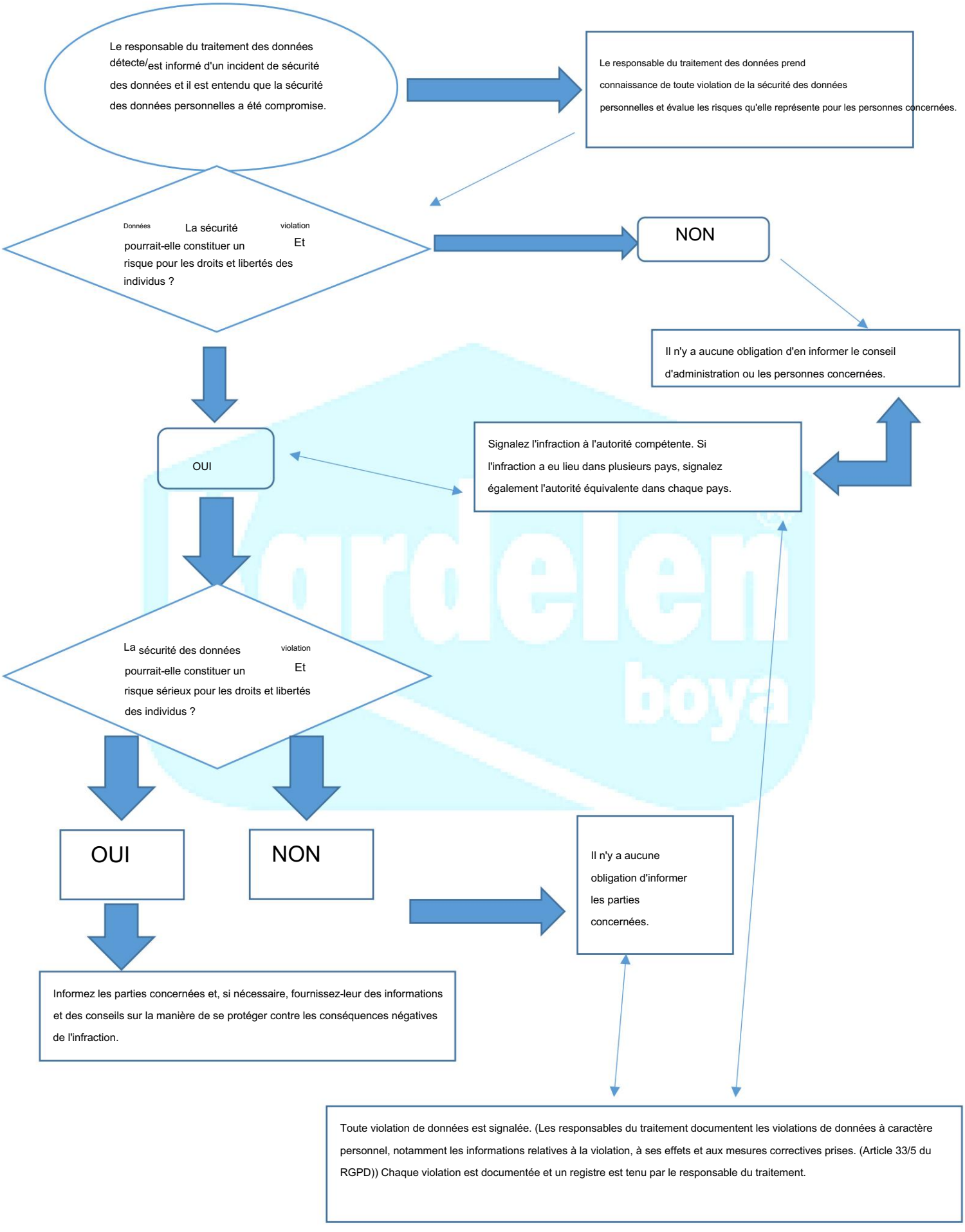
• L'hameçonnage (obtention illégale du mot de passe ou des informations de carte de crédit d'une personne par l'envoi de messages), la fraude électronique ou le vol d'informations, où des informations personnelles sont obtenues par tromperie ou fraude.

• Les cyberattaques malveillantes telles que le piratage, les logiciels malveillants, les attaques par déni de service (DoS-DDoS) ou les attaques par rançongiciel.

1.6. Les violations de données personnelles peuvent avoir des conséquences négatives pour les personnes concernées, pouvant entraîner des préjudices physiques, matériels ou moraux. Ces situations peuvent causer de la gêne, de la détresse ou de l'humiliation à la personne concernée. Parmi les autres conséquences négatives possibles figurent : la perte de contrôle sur les données personnelles, la restriction des droits individuels, la discrimination, l'usurpation d'identité ou la fraude, les pertes financières, l'atteinte à la réputation, la levée du secret professionnel et d'importants désavantages économiques ou sociaux pour les personnes affectées.

Machine Translated by Google

A. Organigramme relatif à l'obligation de signaler les infractions



Machine Translated by Google

1.7. Les violations de données personnelles peuvent conduire aux situations suivantes, par exemple :
Cela pourrait également nuire à notre entreprise :

• Atteinte à la relation de confiance que nous avons établie avec notre personnel et nos clients,

• Perte, suppression ou altération des données personnelles nécessaires à la gestion de notre entreprise vision,

• Atteinte à la réputation de notre entreprise,

• Faire l'objet de sanctions administratives en vertu de la législation sur la protection des données, ou engager des poursuites et des enquêtes à notre encontre en vue d'obtenir des dommages matériels ou moraux.

2. PLAN D'INTERVENTION

En cas de violation potentielle de la sécurité des données personnelles, la Société agira conformément au plan d'intervention décrit ci-dessous :

2.1. Détecter une violation de la sécurité des données et informer les autorités compétentes de la situation.

2.1.1. Le responsable ou le gestionnaire de la protection des données[1] doit être informé dès que possible. sera fait.

2.1.2. Le responsable ou le gestionnaire de la protection des données doit immédiatement en informer le directeur général. Il fournira des informations.

2.1.3. Le délégué à la protection des données (DPO) constitue une petite équipe, appelée Équipe d'intervention en cas d'incident de cybersécurité (EIIC), afin d'évaluer les dommages potentiels, les pertes, les accès non autorisés et les pertes de données temporaires, et de prendre les mesures appropriées pour contenir la violation, remédier à la situation et rétablir l'état antérieur à l'incident. L'ensemble du personnel, les sous-traitants et/ou les responsables conjoints du traitement des données sont tenus d'apporter toute l'assistance nécessaire au DPO et aux membres de l'équipe constituée.

2.1.4. Le responsable/gestionnaire de la protection des données établit une chronologie écrite des événements, consignant tous les aspects de la violation, y compris les éléments suivants :

(a) Date et heure du signalement de l'infraction (au format JJ/MM/AAAA et 24 heures).

(b) Si la notification concerne une violation potentielle, les détails de l'enquête préliminaire (le cas échéant) à mener pour déterminer si une violation a effectivement eu lieu.

(c) Détails concernant la personne qui a signalé l'incident.
(d) Ce qui est connu / ce qui est soupçonné à ce stade initial.
(e) des détails concernant le système/ensemble de données auquel la violation de données est associée.
(f) Évaluation du risque pour les droits et libertés des personnes physiques.

---

1. Le délégué à la protection des données est la personne désignée par notre société comme notre interlocuteur auprès du conseil d'administration et peut être un cadre supérieur affecté à la structure administrative de la société, un spécialiste de la protection des données employé par la société à cette fin, ou un avocat que nous avons engagé à cette fin.

Machine Translated by Google

(g) Actions qui doivent être entreprises d'urgence (enquête, confinement des dommages, remédiation de la situation, récupération des données, etc.).
h) Détails de l'équipe constituée pour aider.
(i) Détails des tâches assignées à chaque membre de l'équipe.
j) De la même manière qu'au point g), dans les 72 heures suivant la prise de connaissance de l'infraction, au Conseil notification à faire.
k) (si nécessaire) notification aux personnes concernées sans délai indu.

2.1.5. Qu'une décision ait été prise ou non d'informer le Conseil, les informations concernant chaque violation potentielle, signalée ou suspectée de données personnelles, y compris ses effets et les mesures correctives prises, doivent être documentées.

2.2. Limiter la violation de sécurité, atténuer ses effets et
Mesures visant à éliminer

2.2.1. La société prendra des mesures immédiates pour contenir la violation et mettre en œuvre les mesures nécessaires pour empêcher l'accès non autorisé aux données personnelles conservées et pour limiter tout dommage qui en résulterait.

2.2.2. En cas de violation de la sécurité des données impliquant des systèmes informatiques et/ou des données électroniques, le personnel de support informatique de la Société sera immédiatement contacté pour obtenir ses conseils et son soutien technique concernant les mesures appropriées à prendre, telles que la limitation des dommages, la mise en quarantaine des zones de stockage de données affectées et la préservation des données et des journaux.

2.2.3. Selon la nature de la violation/menace à l'égard des données personnelles, les mesures à prendre peuvent comprendre les étapes suivantes :

(a) Mise en quarantaine de tout ou partie des ordinateurs personnels, réseaux, etc.

(b) Le personnel doit être averti de ne pas accéder aux ordinateurs, réseaux, appareils, etc.

(c) Suspension des comptes d'utilisateurs,

d) Vérifier les enregistrements conservés sur les serveurs de sauvegarde,

(e) Identifier les types de données personnelles qui pourraient avoir été divulgués et comment l'incident d'accès non autorisé s'est produit.

2.2.4. Si cela est jugé nécessaire, la mise en quarantaine des zones d'enregistrement de données maintenues manuellement ou d'autres manières peut également être envisagée.

2.2.5. Le cas échéant, l'équipe d'enquête sur la criminalité informatique peut être utilisée et des conseils juridiques peuvent être sollicités.

Machine Translated by Google

2.3. Analyse des risques

2.3.1. En cas de violation de données personnelles, la société est tenue de procéder à une analyse de risques complète afin de déterminer si cette violation de données personnelles représente un risque pour les droits et libertés des personnes.

2.3.2. Les catégories de risques qui serviront de base à l'évaluation sont les suivantes :

- Aucun risque : La mise en œuvre de garanties techniques et administratives appropriées et la protection des données personnelles par des mesures telles que le chiffrement qui rend les données illisibles pour les personnes non autorisées à y accéder, ainsi que des précautions supplémentaires, garantissent qu'un risque élevé pour les droits et libertés des personnes concernées n'est plus possible.

- Faible risque : Les personnes concernées peuvent surmonter les inconvénients mineurs.
  Ils peuvent rencontrer (un temps excessif passé, des inconvénients, etc.)
- Risque modéré : Les individus peuvent rencontrer des difficultés qu'ils sont capables de surmonter.
  (efforts supplémentaires, coûts additionnels, stress, léger inconfort physique, etc.)
- Risque élevé : Les individus peuvent être confrontés à de graves conséquences qu'ils devront surmonter (préjudice financier, perte d'emploi, enquête judiciaire, détérioration de la santé, etc.).
- Risque très élevé : Les personnes concernées peuvent se trouver confrontées à des difficultés insurmontables et à des conséquences irréversibles (arrêt de travail, détresse psychologique et physique à long terme, décès, etc.).

S'il est établi qu'aucun risque ne court pour les droits et libertés des personnes physiques, les motifs ayant conduit à cette évaluation seront consignés.

2.3.3. Lors de la réalisation d'une analyse des risques, la Société tiendra compte du niveau de sensibilité des données et des catégories de personnes concernées (par exemple, les enfants, les personnes vulnérables) afin de déterminer si elles seraient exposées à un risque plus élevé en raison de la violation.

2.3.4. Le fait que les données personnelles soient chiffrées de manière sécurisée à l'aide des méthodes de chiffrement les plus récentes et que les clés n'aient pas été compromises en cas de violation de la sécurité peut servir de base pour conclure que la violation de données ne présente pas de risque pour les droits et libertés des personnes et qu'il n'est pas nécessaire d'en informer le Conseil et les propriétaires des données.

2.3.5. Dans son évaluation des risques, la société tiendra compte des recommandations du Conseil d'administration, du Centre national de réponse aux incidents cybernétiques (USOM) et de l'Agence de l'Union européenne pour la cybersécurité (ENISA).

2.3.6. S'il est déterminé qu'il n'est pas nécessaire d'informer le Conseil et les propriétaires des données, les raisons de cette décision seront documentées et cette documentation sera conservée dans les dossiers pour être présentée lors de tout audit qui pourrait être mené par le Conseil.

---

2 www.enisa.europa.eu/publications/dbn-severity

Machine Translated by Google

2.4. Notification de la violation aux institutions et personnes concernées

2.4.1. Signalement des incidents de violation de la sécurité des données à l'autorité de protection des données personnelles : Tous les incidents dans lesquels des données personnelles et des données personnelles sensibles peuvent être menacées (les situations qui ne présentent pas de risque pour les droits et libertés des personnes concernées ne sont pas incluses dans ce champ d'application). L'incident sera signalé au Conseil sans délai indu et dans un délai maximum de 72 heures après notification de l'infraction.

2.4.2. REMPLISSAGE DU FORMULAIRE DE SIGNALEMENT DE VIOLATION DE DONNÉES PERSONNELLES DE LA KVKK : Après avoir accédé au site Web de l'Autorité de protection des données personnelles à l'adresse www.kvkk.gov.tr, cliquez sur l'icône de signalement de violation de données personnelles située dans les menus sur le côté droit de la page d'accueil pour accéder à la zone de signalement des violations de données personnelles.

2.4.3. La page de connexion contient l'« AVIS CONCERNANT LA DÉCISION DU COMITÉ DE PROTECTION DES DONNÉES PERSONNELLES DU 24.01.2019 ET N° 2019/10 RELATIVE AUX PROCÉDURES ET PRINCIPES DE NOTIFICATION DES VIOLATIONS DE DONNÉES PERSONNELLES ». Vous pouvez accéder à la page de notification en cliquant sur le Formulaire de notification de violation de données personnelles (Internet) situé en bas de cette page. Si vous souhaitez remplir le formulaire manuellement, cliquez sur le Formulaire de notification de violation de données personnelles (PDF).

2.4.2. La notification au Conseil doit comprendre au moins les points suivants :

- Informations concernant l'origine de l'infraction et les circonstances de son déroulement.
- Les groupes individuels touchés par la violation (par exemple, les enfants, les autres groupes vulnérables, les personnes handicapées,
  - Nombre de personnes et

d'enregistrements affectés par la fuite de données (au moins une estimation).
- Catégories de données personnelles concernées par la violation (par exemple, informations d'identité, dossiers scolaires, données de sécurité sociale, informations financières, numéros de compte bancaire, numéros de passeport et données de santé, ainsi que des catégories particulières de données telles que l'origine raciale et ethnique).
- Nom et coordonnées du délégué à la protection des données (coordonnées de la personne auprès de laquelle des informations détaillées peuvent être obtenues)
- Une description de l'impact potentiel de la violation sur les personnes concernées (par exemple, perte de contrôle sur les données personnelles, vol d'identité, discrimination, restriction des droits, fraude, perte financière, atteinte à la réputation, risque de divulgation d'informations professionnelles confidentielles, etc.).
- Une description des mesures administratives et techniques prises par l'entreprise avant la violation de données, ainsi que des mesures prises ou prévues pour y remédier (par exemple, suppression des données transmises par erreur, sécurisation des mots de passe, planification de formations à la sécurité des données, etc.). Si possible, les mesures prises pour atténuer les conséquences négatives de la violation seront également incluses dans cette section.

- Remarque importante : L'absence d'informations définitives concernant les points mentionnés ci-dessus ne doit pas retarder la notification du Conseil dans les meilleurs délais. Il convient de préciser que les informations actuelles seront communiquées et que l'établissement sera informé dès que des informations plus détaillées seront disponibles.

2.4.3. Dans les cas où la violation de données relève de la compétence des autorités judiciaires, des forces de l'ordre ou d'autres institutions publiques situées à l'étranger, et concernant cette violation...

Machine Translated by Google

Les organisations ou institutions situées à l'étranger peuvent devoir être informées. Le cas échéant, les documents attestant de cette notification doivent être consignés et soumis au Conseil.
Elle doit être jointe à la notification.

2.4.4 Motifs de la notification de la société :

(a) Éviter les amendes administratives : Article 18 de la loi n° 6698 relative à la protection des données personnelles.
Le défaut d'aviser le Conseil conformément à l'article pertinent peut entraîner une amende administrative.

(b) Demande de conseils : La société peut demander conseil au Conseil d'administration concernant les mesures à prendre en réponse à la violation, et la coopération avec le Conseil d'administration est importante pour justifier ses décisions concernant l'information ou non des propriétaires de données concernés.

2.4.5. Information des personnes concernées par la violation

2.4.5.1. Après avoir effectué l'analyse des risques mentionnée à la section 2.3.1 ci-dessus, si une violation de données à caractère personnel est susceptible de présenter un « risque élevé » pour les droits et libertés des personnes physiques, la Société doit :

(a) Les parties concernées seront contactées par téléphone, courriel, etc., sans délai indu.

(b) Elle informera les personnes concernées qu'une violation de données s'est produite.

(c) Elle fournira aux personnes concernées des informations détaillées sur les points décrits ci-dessus au point 2.4.2.

d) Le cas échéant, elle fournira des conseils spécifiques aux personnes concernées sur la manière de se protéger contre les conséquences négatives potentielles de la violation (telles que la réinitialisation du mot de passe).

2.4.5.2. La notification à la personne concernée expliquera clairement et simplement la nature de la violation de données personnelles et comprendra, au minimum, le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations complémentaires peuvent être obtenues, les conséquences possibles de la violation de données personnelles et, le cas échéant, des explications des mesures prises ou recommandées par notre société pour remédier à la violation de données personnelles, y compris des mesures visant à atténuer les effets négatifs possibles de la violation de données personnelles.

2.4.6. La notification à la personne concernée n'est pas obligatoire si l'une des conditions suivantes est remplie :

(a) L'entreprise doit avoir mis en œuvre des mesures de protection techniques et administratives appropriées, notamment des mesures telles que le chiffrement qui rend les données personnelles illisibles pour toute personne non autorisée à y accéder, et ces mesures doivent avoir été appliquées aux données personnelles concernées par la violation ;

(b) L'entreprise doit prendre des mesures supplémentaires pour s'assurer que le risque élevé pour les droits et libertés des personnes concernées n'est plus possible ;

Machine Translated by Google

c) Si la notification exige un effort excessif. Dans ce cas, une notification publique ou une mesure similaire, permettant d'informer les personnes concernées avec la même efficacité, est appliquée.

2.4.7. Notification aux autorités chargées de l'application de la loi

(a) En cas d'accès non autorisé à des données personnelles, l'affaire doit être immédiatement signalée à l'autorité chargée de l'application de la loi.

(b) En fonction de la nature des données personnelles à risque, et notamment lorsque des données personnelles sensibles peuvent être menacées, une assistance supplémentaire devrait être demandée aux forces de l'ordre.

c) En cas de perte ou d'altération de données, les autorités compétentes doivent être informées. À défaut, l'entreprise s'expose à des sanctions et à des mesures de sécurité.

2.4.8. Autres institutions et organisations : Si nécessaire, le ministère de la Santé, le ministère de la Famille et des Politiques sociales, les institutions financières et d'autres ministères et organisations concernés peuvent être informés.

2.4.9. La société notifiera la compagnie d'assurance avec laquelle le contrat d'assurance a été conclu et l'informera d'une violation de la sécurité des données personnelles.

2.5. Utilisation de services de conseil juridique et d'avocat : La société peut informer les parties prenantes auprès desquelles elle reçoit des services de conseil juridique et d'avocat et peut les informer d'une violation de la sécurité des données personnelles afin de solliciter des conseils juridiques, une défense dans d'éventuels procès, un règlement ou d'autres solutions à l'amiable.

2.6. Mesures à prendre suite à une violation : Après la mise en œuvre des mesures d'urgence nécessaires dans un premier temps, une évaluation et un examen complets de la violation doivent être menés dans un délai raisonnable. Les points suivants seront pris en compte lors de ce processus :

2.6.1. Il sera confirmé que les violations de données personnelles sont documentées, y compris les informations concernant la violation de données personnelles, ses effets et les mesures correctives prises.

2.6.2 Il convient de déterminer les conclusions tirées de l'incident, les aspects à améliorer et les détails des mesures à prendre.

2.6.3 La Société demandera un compte rendu et un rapport d'enquête appropriés à son responsable de la protection des données/procureur (et/ou à d'autres experts externes dont l'expérience peut être utilisée pour l'aider), et une copie de la correspondance échangée avec le Conseil d'administration et/ou les parties concernées par la violation sera conservée.

2.6.4 L'entreprise examinera attentivement s'il convient ou non d'engager des procédures disciplinaires, le cas échéant.

2.6.5 Lorsque des mesures correctives sont jugées nécessaires, la responsabilité sera attribuée aux fonctionnaires concernés, et ils seront chargés de veiller à ce que les mesures nécessaires soient prises dans des délais précis en fonction de leurs domaines de responsabilité.

Machine Translated by Google

2.6.6 Le personnel doit être informé de toute modification apportée au présent plan d'intervention et de toute mise à jour des mesures de sécurité. Il doit également suivre une formation de recyclage au besoin.

Machine Translated by Google

ANNEXE – EXEMPLE DE RAPPORT DE VIOLATION

RAPPORT DE VIOLATION DE LA SÉCURITÉ DES DONNÉES

À UTILISER UNIQUEMENT AVEC LA PEINTURE KARDELEN.

Violation de données personnelles : il s'agit d'une violation de sécurité entraînant la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé, accidentels ou illégaux, à des données personnelles transmises, stockées ou traitées.

Numéro de suivi des infractions :	
Quand la violation de données a-t-elle eu lieu ?	
Où la faille de sécurité des données a-t-elle eu lieu ?	Lieu où l'infraction a eu lieu
Quand l'infraction a-t-elle été signalée ?	Veuillez préciser la date et l'heure.
Qui a signalé la faille de sécurité ?	
Quelles sont les coordonnées de la personne qui a signalé la violation de données ?	
Une notification a-t-elle été faite à l'Autorité de protection des données personnelles ?	Oui □ Non □
Si la réponse est « Oui », veuillez préciser le mode de notification (téléphone, courriel, etc.) ainsi que la date et l'heure de la notification.	
Si la réponse est « Non », un autre haut responsable, directeur, etc., a-t-il été contacté ? Si oui, par quels moyens (par exemple, téléphone, courriel, etc.) et à quelle date et heure le contact ?	
Y a-t-il des témoins de l'incident ? Si oui, veuillez indiquer leurs noms et leurs coordonnées téléphoniques.	

Machine Translated by Google

Veuillez fournir des informations sur la source de l'infraction.
Fournissez des informations détaillées sur la manière dont l'infraction a eu lieu.
Veuillez fournir des informations sur les catégories de parties concernées, affectées ou susceptibles d'être affectées par la violation de données (stagiaires, employés, candidats à l'emploi, clients, fournisseurs, sous-traitants, etc.).
Combien de personnes et d'enregistrements sont touchés ou susceptibles d'être touchés par la fuite de données ? (S'il s'agit d'une estimation, veuillez expliquer pourquoi les chiffres exacts ne peuvent être déterminés.)
Quelles catégories de données personnelles ont été affectées par la violation ? (Identité, coordonnées, localisation, informations personnelles, procédures judiciaires, transactions clients, sécurité physique, sécurité des transactions, gestion des risques, finances, expérience professionnelle, marketing, enregistrements audio et vidéo, origine raciale et ethnique, opinions politiques, convictions philosophiques, vêtements, appartenance à une association, informations de santé, condamnations pénales et mesures de sécurité, données biométriques, etc.)

Machine Translated by Google

Décrivez les conséquences potentielles de la violation sur les personnes concernées. (Perte de contrôle des données personnelles, usurpation d'identité, discrimination, restriction des droits, fraude, perte financière, atteinte à la réputation, perte de sécurité des données personnelles, etc.)
Veuillez décrire les mesures prises ou proposées par la Société pour remédier à la violation de données personnelles, y compris les mesures visant à atténuer les impacts négatifs potentiels de cette violation. Note importante : L'ignorance des détails relatifs aux mesures mentionnées ci-dessus ne justifie pas de s'abstenir d'en informer l'Autorité de protection des données personnelles. Les informations pourront être communiquées par étapes, sans délai supplémentaire injustifié. Le cas échéant, veuillez l'indiquer clairement.
Pensez-vous qu'une violation de données soit une situation temporaire ? Est-il possible de récupérer des données personnelles compromises et d'y accéder à nouveau ?

Machine Translated by Google

Un système informatique a-t-il été affecté par l'incident ? (Par exemple : messagerie électronique, site web, applications cloud, systèmes de gestion électronique de documents, etc.) Si oui, veuillez les énumérer ci-dessous.
Existe-t-il des documents d'information supplémentaires disponibles, tels que des messages d'erreur, des captures d'écran, des fichiers journaux ou des enregistrements de vidéosurveillance ?
Avez-vous pris des mesures pour éliminer ou atténuer les risques pour les personnes concernées que vous pensez avoir été affectées, ou pour d'autres personnes concernées que vous pensez avoir été affectées ? Si votre réponse est « OUI », veuillez expliquer ci-dessous.
Avez-vous informé un membre de la direction, comme un membre du conseil d'administration, le PDG ou le responsable informatique, de cette situation ? Si oui, veuillez décrire brièvement votre interlocuteur et les conseils ou instructions reçus.
Avez-vous contacté des organismes externes (compagnies d'assurance, fournisseurs informatiques, forces de l'ordre, etc.) ? Si oui, veuillez indiquer ci-dessous les personnes contactées ainsi que leurs noms et coordonnées. .

Machine Translated by Google

Si vous souhaitez apporter des précisions supplémentaires, veuillez l'indiquer ci-dessous.

Édité par :	
Votre tâche :	
Officier Être Unité:	
Vos coordonnées : (Idéalement votre numéro de téléphone)	
Histoire:	
Délai d'achèvement du rapport :	

Merci d'avoir rempli ce formulaire. Cela permettra à Kardelen Boya de mieux enquêter sur cette affaire.

Veuillez vous assurer que ce rapport soit transmis directement au responsable/professeur chargé de la protection des données de l'entreprise :

Responsable de la protection des données : Nom et prénom :
Fonction :

Adresse : Téléphone :
E-mail:

*CE FORMULAIRE A ÉTÉ ÉLABORÉ EN TENANT COMPTE DES AFFAIRES CIVILES ET PÉNALES.

Machine Translated by Google

POUR VOTRE INFORMATION:

Les violations de la sécurité des données sont classées selon les principes de sécurité de l'information généralement acceptés suivants :

A) Protection des données : Il s'agit d'empêcher l'accès aux données par des personnes non autorisées. Une « violation de la confidentialité » désigne la divulgation ou l'accès non autorisé ou accidentel à des données personnelles.

B) Intégrité des données : Il s'agit de s'assurer que les données sont conservées et protégées comme il se doit. L'expression « atteinte à l'intégrité » désigne toute modification non autorisée ou accidentelle de données personnelles.

C) Accessibilité/Disponibilité des données : Cela signifie que les données doivent être accessibles et utilisables en permanence. Une « violation d'accès » désigne la perte accidentelle ou non autorisée d'accès à des données personnelles, ou la destruction accidentelle ou non autorisée de ces données.

Selon les circonstances, une violation de la sécurité des données peut résulter d'une atteinte à la confidentialité, à l'intégrité ou à la disponibilité des données personnelles, ou d'une combinaison de ces éléments. Les informations permettant de déterminer si une atteinte à la confidentialité ou à l'intégrité des données a eu lieu sont relativement faciles à identifier. En revanche, il peut être plus difficile de déterminer si la disponibilité des données a été compromise. La perte ou la destruction définitive de données personnelles constitue systématiquement une violation du principe de disponibilité des données.

PROCÉDURES À SUIVRE EN CAS DE FAUX DE SÉCURITÉ.

CHOSES À NE PAS FAIRE :

CHOSES À FAIRE :

- Davantage d'accès non autorisés, de divulgations de données, de dommages aux systèmes d'enregistrement, etc. Pour éviter d'autres incidents, isolez immédiatement le système concerné.
- Utilisez votre téléphone pour communiquer. Les pirates peuvent surveiller le trafic de courriels.
- Contactez immédiatement le responsable/directeur de la protection des données de l'entreprise.

Responsable/Gestionnaire de la protection des données :

Nom et prénom :

Titre d'emploi:

Adresse:

Téléphone:

E-mail:

- Conservez tous les enregistrements de journaux pertinents, par exemple, pare-feu, routeur et système de détection d'intrusion.
- Créez des copies de sauvegarde des fichiers endommagés ou modifiés et stockez ces sauvegardes. Conservez-le en lieu sûr.
- Déterminer où se situe le système concerné au sein de la topologie du réseau.
- Identifier tous les systèmes et unités connectés au système concerné.
- Programmes et processus exécutés sur le(s) système(s) affecté(s), impact de la panne et autorisations Spécifiez la durée maximale d'interruption autorisée.
- Si des preuves concernant le système affecté sont recueillies, prenez les dispositions nécessaires pour assurer la continuité du service, c'est-à-dire préparez un système redondant et créez des sauvegardes de données.

Machine Translated by Google

CHOSES À NE PAS FAIRE :

- Ne supprimez, ne déplacez ni ne modifiez aucun fichier sur les systèmes affectés. • Ne contactez pas les auteurs présumés des attaques. •

N’effectuez aucune analyse de cybercriminalité sans autorisation.

Machine Translated by Google

CE FORMULAIRE DOIT ÊTRE REMPLI UNIQUEMENT PAR L'ÉQUIPE D'INTERVENTION EN CAS DE VIOLATION DE DONNÉES.

Responsable/Gestionnaire de la protection des données :	
Date et heure de soumission de ce formulaire à la société :	
Veuillez préciser l'impact de la violation de la sécurité des données. Confidentialité des données, intégrité des données, accès et disponibilité des données (voir explications ci-dessus)	
Nombre de personnes et d'enregistrements affectés par la fuite de données	Nombre estimé de personnes et de données affectées par la violation ? Quelles catégories de données sont concernées ?
Suite à la fuite de données, quelles catégories particulières de données personnelles (origine raciale et ethnique, opinions politiques, convictions religieuses et philosophiques, appartenance à une confession ou un syndicat, données biométriques et génétiques, données de santé, données à caractère sexuel) ont été affectées ? Veuillez indiquer les informations pertinentes ci-dessous. Par exemple, combien de personnes ont vu leurs données personnelles affectées par cette fuite ? La vie a-t-elle été affectée ?	Oui □ Non □

« La possibilité que les personnes concernées soient exposées à des effets indésirables. » La destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données personnelles transmises, stockées ou traitées, qu'ils soient accidentels ou illégaux, constituent une violation de la sécurité. L'étendue de la violation doit être déterminée en évaluant son impact potentiel sur les personnes concernées. Cette évaluation doit prendre en compte la nature et la cause de la violation, le type de données impliquées, les mesures prises pour en atténuer les effets et les catégories de personnes touchées. * Si aucun risque n'est évalué, veuillez en expliquer les raisons :		Risque très élevé : les personnes concernées peuvent se trouver confrontées à des difficultés insurmontables et à des conséquences irréversibles (arrêt de travail, détresse psychologique et physique à long terme, décès, etc.).
		Risque élevé : Les personnes concernées pourraient subir de graves conséquences qu'elles devront surmonter (dommages matériels, perte d'emploi, enquête judiciaire, détérioration de la santé, etc.).
		Modéré : Les personnes peuvent rencontrer des difficultés gérables (efforts excessifs, coûts supplémentaires, stress, inconfort physique mineur, etc.).
		Faible : Les individus peuvent rencontrer des obstacles mineurs qu'ils peuvent surmonter (par exemple, passer trop de temps, s'ennuyer).
		Absence de risque : La mise en œuvre de garanties techniques et administratives appropriées, ainsi que la protection des données personnelles par des mesures telles que le chiffrement qui les rend illisibles pour toute personne non autorisée, garantissent l'absence de risque élevé pour les droits et libertés des personnes concernées.

Machine Translated by Google

Les hauts dirigeants membres du conseil d'administration ont-ils été informés ?	Oui □ Non □
Le prestataire de services informatiques/l'équipe de support technique informatique a-t-il été informé ?	Oui □ Non □
La compagnie d'assurance a-t-elle été informée ?	Oui □ Non □
Un rapport/une plainte a-t-il été déposé auprès des forces de l'ordre ?	Oui □ Non □
Les conseillers juridiques ont-ils été informés ?	Oui □ Non □
Les personnes concernées ont-elles été informées ? Nombre de personnes impliquées ? Existe-t-il des listes de contacts qui nous permettraient de joindre les personnes concernées ? Ou est-il possible de récupérer leurs coordonnées ?	Oui □ Non □
Une notification a-t-elle été faite à l'Autorité de protection des données personnelles ? Autorité de protection des données personnelles Téléphone : 0312 216 50 00 Centre d'appels : Ligne d'assistance téléphonique ALO 198 sur la protection des données, Centre d'information et de conseil Courriel : veriguvenligi@kvkk.gov.tr Page web contenant le formulaire de notification d'infraction : https://www.kvkk.gov.tr/Icerik/5362/Ve notification de violation de données Adresse : Quartier Nasuh Akar, 1407e rue. N° 4, 06520 Çankaya/Ankara	Oui □ Non □ Si la réponse est « OUI », veuillez indiquer la date et l'heure de la notification (le cas échéant). Notez ci-dessous les conseils et instructions reçus de l'établissement :
Autres points à noter	
Signature du responsable/gestionnaire de la protection des données :	
PDG ou nommé Signature du représentant :	
Histoire:	

*CE FORMULAIRE EST DESTINÉ À ÊTRE UTILISÉ DANS LES AFFAIRES CIVILES ET PÉNALES.

PRÉPARÉ EN LE TENANT DISPONIBLE.