GDPR – Politique de Confidentialité

Juillet 2019

SOMMAIRE

POLITIQUE DE CONFIDENTIALITÉ

La présente politique de confidentialité (la « **politique de confidentialité** ») fournit des détails sur la manière dont Marlux/STRADUS (« la **société** ») traite les données personnelles lorsque vous travaillez pour la société ou lorsque vous faites affaire avec la société.

Les données personnelles sont traitées conformément au Règlement relatif à la protection des données (Règlement (UE) 2016/679) et aux autres lois et règlements relatifs à la confidentialité applicable aux niveaux national et européen (qui forment ensemble la « **loi sur la protection des données** »).

Les termes qui apparaissent en caractères gras dans la présente politique de confidentialité sont définis dans le glossaire en Annexe 1.

1. CHAMP D'APPLICATION

La présente politique de confidentialité s'applique à toutes les données personnelles que nous traitons en tant que contrôleur des données.

Dans la mesure où la société décide pourquoi et comment les données personnelles sont traitées, la société est contrôleur des dites données personnelles.

Par exemple, la société peut traiter les données personnelles d'employés, d'anciens employés, des membres de leur famille, des travailleurs intérimaires, des travailleurs indépendants, des candidats à un poste, des sous-traitants, des contacts fournisseurs, des clients et des visiteurs.

2. OBJECTIF

Le but de cette politique de confidentialité est d'expliquer quelles données personnelles nous traitons, et comment et pourquoi nous les traitons. La présente politique de confidentialité a pour objectif d'expliquer quelles sont les données personnelles que nous traitons, et comment et pourquoi nous les traitons. Par ailleurs, cette politique de confidentialité décrit nos devoirs et responsabilités à l'égard de leur protection.

La présente politique de confidentialité ne représente pas une déclaration exhaustive de nos pratiques en matière de protection des données. Nous vous ferons part de toute modification dans la mesure du possible.

*[Dans la mesure où la législation nationale en matière de protection des données (la « **législation nationale** ») concerne la présente politique de confidentialité, et/ou que [insérer le nom de la société] (la « société ») traite les données personnelles d'une manière différente à ce qui est établi dans la présente politique de confidentialité (p. ex. en ce qui concerne les catégories de données personnelles traitées, la finalité du traitement, etc.), les précisions relatives à ces traitements spécifiques sont présentées dans l'Annexe 2.]*

1. TYPES DE DONNÉES PERSONNELLES

1.1 Employés, candidats et sous-traitants

La société recueille et traite les données personnelles en lien avec nos employés, les candidats à un poste et les sous-traitants, ainsi que nos anciens employés et nos anciens sous-traitants. Ces données personnelles incluent ce qui suit : les informations personnelles, telles que le nom, la date de naissance, le numéro de sécurité sociale, les coordonnées bancaires, les proches parents, les informations relatives aux comptes de médias sociaux, les données de visa/passeport ; les coordonnées, telles que l'adresse et le ou les numéros de téléphone ; les informations relatives au dossier personnel, notamment les conditions de travail et le poste, la formation, les évaluations de performance, les promotions, les plans de développement personnel, la conduite et les données disciplinaires, le lieu de travail, les informations liées aux salaires, les coordonnées bancaires et fiscales et le numéro de sécurité sociale, les habilitations de sécurité ; les informations relatives à l'historique professionnel et aux candidatures (de lettres de motivation, CV, formulaires de postulation), telles que l'historique des études poursuivies et l'historique des postes occupés ; le contenu éditorial ou journalistique, tel que les liens vers des travaux (par exemple, des liens vers des fichiers vidéo ou audio) ; les informations médicales, telles que les certificats médicaux et les arrêts de travail ; les informations relatives à la famille, telles que les noms et les dates de naissance des enfants (ces données sont pertinentes lorsqu'un individu demande un congé parental, par exemple) ; les informations requises pour la retraite ; les informations relatives à l'appartenance à un syndicat ; et les données relatives aux performances, telles que la notation de la gestion des performances pour les cadres et les revues annuelles de progression des salaires des employés, les tests psychométriques, etc. Cette liste n'est pas exhaustive, mais décrit les données personnelles les plus souvent recueillies, utilisées et autrement traitées.

1.2 Fournisseurs et clients

La société recueille et traite des données personnelles en lien avec nos fournisseurs et nos clients, et/ou ceux qui travaillent avec eux. Ces données personnelles peuvent inclure ce qui suit : les informations personnelles, telles que le nom, le titre, le poste, les numéros d'identification professionnels, le département, l'unité commerciale (y compris les données recueillies dans le cadre d'une formation ou d'une vérification) ; les coordonnées, telles que l'adresse électronique, le(s) numéro(s) de téléphone et le lieu de travail ; et les informations fiscales, telles que les numéros de TVA et autres numéros d'identification fiscale.

1.3 Catégories spéciales de données personnelles

Les types de catégories spéciales de données personnelles que la société peut traiter incluent, sans limitation, les données sur la santé, les informations sur les condamnations pénales et les données biométriques. La société traite toutes les données personnelles en conformité avec la loi de protection des données, en particulier toutes les catégories spéciales de données personnelles. [*Vous trouverez plus de détails sur les types de données personnelles et les* ***catégories spéciales de données personnelles*** *que nous traitons dans l'Annexe 2.*]

2. FINALITÉS DU TRAITEMENT

La société traite les données personnelles selon le ou les objectifs pour lesquels les données personnelles ont été obtenues.Parmi des exemples courants de raisons pour lesquelles la société traite les données personnelles figurent : l'administration de la paie et des avantages ; les RH, la gestion des talents et des performances ; le marketing et les RP ; l'amélioration des produits et services commerciaux ; la recherche et les analyses statistiques ; la stratégie commerciale ; les audits ou enquêtes internes ; la prévention et la détection des comportements illégaux et/ou criminels à notre égard ou à l'égard de nos clients et employés ; et/ou l'exécution d'obligations juridiques. Il est possible que de temps en temps, nous traitions des données personnelles pour d'autres raisons. La société essaie de s'assurer que les individus sont informés sur la ou les finalités du traitement de leurs données personnelles au moment où la société recueille leur consentement. Lorsque cela n'est pas possible, la société essaie de vous informer au plus vite après le traitement des données personnelles. Les individus ont le droit de retirer leur consentement à tout moment.

3. PROFILAGE

La société peut traiter les données personnelles de différents individus (par exemple, d'employés, de prestataires et de candidats à un poste) pour la gestion des talents et l'évaluation du personnel (afin de potentiellement inclure des analyses de présence et de performance).

La société procède aux dits traitements lorsque : (a) cela est expressément autorisé par la loi nationale (notamment pour le contrôle de la fraude et de l'évasion fiscale) ; (b) cela est nécessaire à la conclusion ou à l'exécution d'un contrat ; ou (c) l'individu a donné un consentement approprié. [*Vous trouverez plus de détails sur les types de profilage que nous réalisons dans l'Annexe 2.*]

4. DROITS DES PERSONNES

Les individus ont certains droits en vertu de la loi de protection des données.

4.1 **Vérification et accès** : vous pouvez nous demander un résumé et une copie de vos données personnelles que nous traitons ou que nous avons traitées en notre nom ;

4.2 **Correction/Ajout/Suppression** : si vous pensez que vos données personnelles sont inexactes ou incomplètes, vous avez le droit de nous demander de corriger, modifier ou supprimer vos données personnelles ;

4.3 **Objection :** vous pouvez vous opposer au traitement de vos données personnelles par nous en vous appuyant sur nos raisons légitimes de traitement (voir la section **Finalités Du Traitement** ci-dessus) ;

4.4 **Restriction : vous pouvez demander que nous limitions le traitement de vos données personnelles si la précision de vos données personnelles est contestée, si notre traitement est illégal, si vous pensez que nous n'avons plus besoin de ces données personnelles ou si vous vous êtes opposé au traitement ; et**

4.5 **Prise de décision automatisée :** si la société entreprend de procéder à des prises de décision automatiques (notamment le profilage), qui ont un impact significatif sur vous, vous avez le droit de vous opposer à une telle prise de décision.

La Procédure relative aux droits des personnes de la société explique comment les demandes précédemment mentionnées peuvent être effectuées et comment la société gère ces demandes.

5. SÉCURITÉ

5.1 Mesures de sécurité

La société a mis en place des mesures techniques et organisationnelles afin de protéger les données personnelles de toute destruction, perte, modification, divulgation, acquisition ou accès illicite ou non autorisé.

Les données personnelles sont conservées en toute sécurité grâce à plusieurs mesures de sécurité, notamment, le cas échéant, des mesures physiques telles que des armoires d'archives verrouillées et plusieurs mesures informatiques.

Pour en savoir plus sur les mesures de sécurité de la société, veuillez consulter la Politique relative à la sécurité des informations [*et l'Annexe 2*].

5.2 Violation des données personnelles

La société gère les violations des données personnelles conformément à la procédure de signalement des violations des données personnelles. Pour en savoir plus sur la façon d'identifier et de signaler une violation des données, veuillez consulter notre Procédure en cas de violation des données personnelles.

6. DIVULGATION DE DONNÉES PERSONNELLES

De temps à autre, il est possible que la société divulgue des données personnelles à des tiers, ou autorise des tiers à accéder aux données personnelles que nous traitons (par exemple, si un organisme chargé de faire appliquer la loi ou une autorité réglementaire soumet une demande d'accès aux données personnelles valide).

La société peut également partager des données personnelles : (a) avec un autre membre du CRH Group (y compris nos filiales, notre société mère et ses filiales) ; (b) avec certains tiers, notamment des partenaires commerciaux, des fournisseurs et des sous-traitants ; (c) avec des tiers lorsque nous vendons ou achetons des entreprises ou des actifs ; ou (d) si la société est juridiquement tenue de divulguer des données personnelles. Ceci inclut l'échange d'informations avec d'autres sociétés et organisations à des fins de prévention de la fraude.

Lorsque la société conclut des accords avec des tiers pour le traitement de données personnelles en son nom, elle s'assurera que les protections contractuelles appropriées sont en place afin de les protéger. Parmi ces tiers figurent les fournisseurs de services de communications, les prestataires de services de paie, les prestataires de médecine du travail, les agences de marketing ou de recrutement, les opérateurs de centres de données utilisés par la société, etc. [*Vous trouverez plus de détails sur les catégories de tiers auxquelles la société divulgue les données personnelles des individus dans l'Annexe 2.*]

7. CONSERVATION DES DONNÉES

La société ne conserve les données personnelles qu'aussi longtemps que la conservation des dites données personnelles est jugée nécessaire pour les finalités pour lesquelles ces données personnelles sont traitées. Les données personnelles sont conservées conformément aux lois pertinentes et aux directives de la société. [***Vous trouverez plus de détails sur la** période de conservation des données personnelles appliquée par la société (ou les critères utilisés pour déterminer cette période de conservation**) dans l'Annexe 2.***]**

8. TRANSFERTS DE DONNÉES EN DEHORS DE L'EEE

Il peut arriver que la société soit dans l'obligation de transférer les données personnelles en dehors de l'EEE. Ledit transfert s'effectuera alors en conformité avec la loi de protection des données applicable. La société prend des mesures raisonnables pour s'assurer que les données personnelles sont traitées en toute sécurité et conformément à la présente politique de confidentialité lorsqu'elles sont transférées en dehors de l'EEE. [***Vous trouverez plus de détails sur la nature des transferts de données engagés par la société dans l'Annexe 2.***]

9. RÔLES ET RESPONSABILITÉS

La société est responsable du traitement des données personnelles. Le directeur général de la société est entièrement responsable de la conformité de la société avec la présente politique de confidentialité et doit désigner un point de contact principal en ce qui concerne (i) le traitement des données personnelles des anciens et actuels employés et prestataires de la société ; (ii) le traitement des données personnelles des contacts professionnels ; et (iii) le maintien de la sécurité et de l'intégrité des données personnelles traitées par la société.

Les services juridiques et de la conformité doivent soutenir la société en fournissant des conseils juridiques et en interprétant la loi de protection des données et la présente politique de confidentialité à un niveau local.

Tous les employés de la société doivent respecter la dernière version en date de la présente politique de confidentialité, tel qu'elle est publiée de temps à autre. S'il s'avère que des employés ont sciemment enfreint la présente politique de confidentialité, ils peuvent faire l'objet de mesures disciplinaires allant jusqu'au licenciement.

10. PROCÉDURE DE PLAINTE

Vous pouvez poser une question ou faire une réclamation à propos de la présente politique de confidentialité et/ou du traitement de vos données personnelles en contactant le [responsable des ressources humaines/RPC] au numéro +32 13 679100. Vous pouvez déposer une réclamation au sujet de notre conformité avec la loi de protection des données auprès du régulateur de la protection des données concerné [*comme spécifié dans l'Annexe 2*], mais nous vous demandons de contacter le DRH (Directeur de Ressources humaines) en premier lieu afin de nous donner l'opportunité de répondre à toutes les préoccupations que vous pouvez avoir.

11. POLITIQUES ASSOCIÉES

La présente politique doit être lue conjointement avec les politiques et procédures suivantes :

- Procédure en cas de violation des données personnelles
- Procédure relative aux droits des personnes
- Politique de sécurité des informations
- Déclaration de confidentialité du site Web

Annexe 1

GLOSSAIRE

Les termes ci-dessous apparaissent dans la présente politique de confidentialité avec la définition suivante :

L'« **Agent de traitement des données** » désigne la partie qui traite les données personnelles pour le compte du contrôleur des données (par exemple, un fournisseur de services de paie).

Les « **catégories spéciales de données personnelles** » sont des types de données personnelles qui révèlent l'une des informations suivantes concernant un individu : origine raciale ou ethnique, opinions politiques, croyances religieuses ou philosophiques, ou appartenance à un syndicat. Les catégories spéciales de données personnelles comprennent également le traitement des données génétiques, des données biométriques (par exemple les empreintes digitales ou les images faciales), les données de santé, les données concernant la vie sexuelle ou l'orientation sexuelle et toutes données personnelles afférentes aux condamnations pénales ou délits.

Le « **Contrôleur des données** » désigne l'entité qui décide pourquoi et comment les données personnelles sont traitées.

Les « **Données personnelles** » désignent toute information relative à une personne vivante qui permet l'identification de cette personne. Une personne est identifiable si son identité peut raisonnablement être établie à partir des données sans effort démesuré. Les données personnelles peuvent inclure :

Employés et sous-traitants

1. Les informations personnelles, telles que le nom, la date de naissance, les coordonnées bancaires, les proches parents et les informations relatives aux comptes de médias sociaux ;

2. Les coordonnées, telles que l'adresse et le ou les numéros de téléphone ;

3. Les informations relatives au dossier personnel, notamment les conditions de travail, le poste, la formation, les évaluations de performance, les promotions, les plans de développement personnel, la conduite et les données disciplinaires, le lieu de travail, les informations liées aux salaires, les coordonnées bancaires et fiscales, ainsi que les numéros personnellement identifiables tels que le numéro de sécurité sociale ;

4. Les informations relatives à l'historique professionnel et aux candidatures, telles que l'historique des études poursuivies et l'historique des postes occupés (de lettres de motivation, curriculum vitae et formulaires de postulation) ;

5. Le contenu éditorial ou journalistique, tel que les liens vers des travaux (par exemple, des liens vers des fichiers vidéo ou audio) ;

6. Les informations médicales, telles que les certificats médicaux et les arrêts de travail ;

7. Les informations relatives à la famille, telles que les noms et les dates de naissance des enfants (ces données sont pertinentes lorsqu'un individu demande un congé parental, par exemple) ;

8. Les informations requises pour la retraite ;

9. Les informations relatives à l'appartenance à un syndicat ; et

10. Les données relatives aux performances, telles que la notation de la gestion des performances pour les cadres et les revues annuelles de progression des salaires des employés, les tests psychométriques, etc.

Fournisseurs et clients

1. les informations personnelles, telles que le nom, le titre, le poste, les numéros d'identification professionnels, le service, l'unité commerciale ;

2. les coordonnées, telles que l'adresse et le ou les numéros de téléphone ;

3. le lieu de travail ; et

4. les informations fiscales, telles que les numéros de TVA et les numéros d'identification fiscale.

L'« **Espace économique européen** » ou « **EEE** » désigne l'Autriche, la Belgique, la Bulgarie, la Croatie, la République de Chypre, la République tchèque, le Danemark, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Hongrie, l'Irlande, l'Italie, la Lettonie, la Lituanie, le Luxembourg, Malte, les Pays-Bas, la Pologne, le Portugal, la Roumanie, la Slovaquie, la Slovénie, l'Espagne, la Suède, le Royaume-Uni, l'Islande, le Liechtenstein et la Norvège.

Le « **profilage** » est le traitement automatisé des données personnelles en vue d'évaluer certains aspects liés à un individu, ce qui permet d'analyser ou de prévoir les performances, les décisions ou les comportements de cet individu.

Le « **RPC** » désigne le responsable pays de la conformité de l'entreprise ;

Le « **Traitement transfrontalier »** se produit : (a) quand nous sommes établis dans plusieurs États membres de l'UE et que notre traitement des données personnelles a lieu dans plusieurs États membres de l'UE ; ou (b) si notre traitement des données personnelles a lieu dans un seul État membre de l'UE, mais que ce traitement affecte sensiblement (ou est susceptible d'affecter sensiblement) des individus résidant dans plusieurs États membres de l'UE.

Le « **Traitement** » inclut la collecte, l'utilisation, l'enregistrement, l'organisation, la modification, la divulgation, la destruction ou la conservation de données personnelles d'une quelconque manière. Le traitement peut être réalisé manuellement ou avec des systèmes automatisés, tels que les systèmes de technologie de l'information, et les termes « **traiter** » et « **traitement** » doivent être interprétés en conséquence.

La « **Violation des données personnelles** » désigne une violation de la sécurité entraînant la destruction, la perte, la modification accidentelles ou illégales, la divulgation ou l'accès non autorisé à des données personnelles transmises, stockées ou autrement traitées.

Annexe 2

TRAITEMENT PROPRE À UNE SOCIÉTÉ [1]

Cette annexe comporte des informations supplémentaires concernant la manière dont la société traite les données personnelles.

1. Législation applicable et autorité de régulation en charge de la protection des données au niveau local

Dans la présente annexe, on entend par « **loi de protection des données** » le règlement général sur la protection des données (règlement (UE) 2016/679). Concernant la société, l'autorité de régulation en charge de la protection des données au niveau local est : l' autorité de protection des données.

2. Données personnelles traitées par la société

En plus des catégories de données personnelles détaillées à la section 1 de la politique de confidentialité; la société traite également les catégories de données personnelles suivantes **:** pas applicable.

3. Objectifs du traitement des données personnelles

En plus des finalités décrites à la section 2 de la politique de confidentialité, la société traite également les données personnelles aux fins suivantes : les voitures du société, assurance hospitalisation, assurance groupe, enregistrement du temps (GPS).

4. Profilage

La société réalise les types de profilage suivants : nécessaire pour le paiement des salaires, la gestion des talents, la planification des successions, la formation des employés, l'octroi des avantages extralégaux (gestion de la flotte, données de présence, enregistrement du temps, inscription du client et du fournisseur).

5. Mesures de sécurité

La société a mis en place les mesures de sécurité techniques et organisationnelles supplémentaires ci-après pour protéger les données personnelles face à une éventuelle destruction, perte, modification, divulgation, acquisition ou accès non autorisés : automatisation des dossiers,…

6. Divulgation de données personnelles à des tiers

La société divulgue aux catégories de tiers supplémentaires suivantes ou leur permet d'accéder aux données personnelles aux fins expliquées ci-dessous : secrétariat social, sécurité sociale, fiscalité, santé au travail, DKV, Vivium, Assurance Fédérale, sociétés de leasing, Total (cartes carburant), assurance accidents du travail, syndicats, fédération professionnelle, Edenred, enregistrement des temps, Centro, SuccessFactors, Benefits@work. Cette liste n'est pas exhaustive, mais la plus récente peut toujours consulter dans le registre de données. Cela peut être consulté sur demande.

7. Délais de conservation des données

La société conserve les données personnelles en fonction des critères suivants : conformément aux règles juridiques et sur la base de la nécessité. Les lettres de motivation, les curriculum vitae et les données des formulaires de candidature sont conservés pour la construction d'un pool de talents pendant une période de 3 ans.

8. Transferts de données

La société transfère les données personnelles aux endroits suivants en dehors de l'EEE, aux fins indiquées ci-dessous, avec les garanties légales indiquées (dont une copie peut être demandée chez le département RH (SuccessFactors).

PROCÉDURE EN CAS DE VIOLATION DES DONNÉES PERSONNELLES

1. INTRODUCTION

La procédure en cas de violation des données personnelles (la « **procédure** ») décrit le processus d'escalade, de notification et d'enregistrement des violations présumées ou réelles de données personnelles (comme défini ci-dessous). Elle s'applique à Remacle (la « **société** »). Cette procédure vise à garantir que la société gère et contrôle rapidement toute violation des données personnelles (telle que définie ci-dessous) de manière à ce que l'incidence de la violation des données puisse être minimisée et à ce que toute obligation légale de signaler cette dernière à une autorité de régulation et/ou aux personnes concernées par la violation des données (conformément au règlement général sur la protection des données [règlement (UE) 2016/679, le « **GDPR** »]) puisse être respectée en temps voulu.

2. QU'ENTEND-ON PAR « DONNÉES PERSONNELLES » ?

Le terme Données personnelles désigne toute information relative à une personne vivante (se trouvant dans l'Espace économique européen) qui permet l'identification de cette personne (les « **données personnelles** »). Une personne est identifiable si son identité peut raisonnablement être établie à partir des données sans effort démesuré. Les données personnelles peuvent inclure : le nom, l'adresse, la date de naissance, le numéro de téléphone, le numéro de compte, l'intitulé du poste, une photo, l'adresse IP, etc.

3. QU'ENTEND-ON PAR « VIOLATION DES DONNÉES PERSONNELLES » ?

Selon le GDPR, une violation des données personnelles est « *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* » (« **violation des données personnelles** »). Une violation des données personnelles se produit en cas de divulgation, de perte ou toute autre forme de collecte, utilisation, enregistrement ou diffusion non autorisées, accidentelles ou illicites des données personnelles. Exemples de violations des données personnelles : la perte ou le vol d'un ordinateur portable ou d'un téléphone mobile qui contient des données personnelles ; l'envoi d'un fichier Excel (non protégé) contenant des données personnelles à une personne non autorisée ; l'impression d'une feuille de salaire laissée ensuite sur l'imprimante ; le piratage d'un système contenant des données personnelles ; la perte ou le vol de fichiers, etc.

Un incident lié à une violation de la sécurité des données est appelé « **incident de données** ». Un incident de données ne concernant pas de données personnelles ne constitue pas une violation des données personnelles. Par ailleurs, tous les incidents de données concernant des données personnelles ne seront pas forcément considérés comme des violations des données personnelles. Par exemple, la perte ou la mise en péril de données personnelles peuvent ne pas être considérées comme une violation des données personnelles lorsque : (i) les données personnelles sont chiffrées ou anonymisées ; (ii) les données personnelles ont été sauvegardées récemment dans leur intégralité ; et (iii) l'accès aux données personnelles est surveillé. Par conséquent, la question de savoir si un incident de données constitue ou non une violation des données personnelles doit être tranchée au cas par cas.

4. QUAND CETTE PROCÉDURE S'APPLIQUE-T-ELLE ?

Si l'incident de données *ne concerne pas* des données personnelles, alors cette procédure ne s'applique pas. Si l'incident de données *concerne* des données personnelles, une violation des données personnelles peut s'être produite et cette procédure s'appliquera. En cas de doute sur la survenance ou non d'une violation des données personnelles, la société doit immédiatement demander conseil au service juridique et de la conformité afin d'évaluer rapidement la situation.

5. COMMENT SIGNALER UNE VIOLATION DES DONNÉES PERSONNELLES EN INTERNE ?

Il est important que toutes les violations des données personnelles réelles ou présumées soient immédiatement signalées au sein de CRH conformément aux étapes suivantes :

5.1 Notification initiale

Toute violation réelle ou présumée des données personnelles doit être signalée dès qu'elle est détectée au directeur général de la société (le « **MD de la société** ») ou directement au service juridique et de conformité. Le MD de la société devra rapidement signaler toute violation réelle ou présumée des données personnelles au service juridique et de la conformité.

5.2 Plan d'action

En cas de violation des données personnelles, le MD de la société ou son délégué devront collaborer avec le service juridique et de la conformité pour élaborer un plan d'action en réponse à la violation des données personnelles. L'annexe 1 présente un graphique illustrant la gestion d'un cas de violation des données personnelles.

Pour élaborer le plan d'action qui convient, l'équipe d'intervention examinera :

- les informations contenues dans la notification de violation des données personnelles ;
- les mesures devant être prises immédiatement pour contenir les effets de la violation des données personnelle
- s'il est obligatoire de signaler à l'autorité de protection des données concernée (« **APD** ») la

  violation des données personnelles et si oui, les éléments qui doivent être communiqués ;
- les conséquences potentielles de la violation des données personnelles pour la société et les individus concernés
- les mesures prises par la société au moment donné et les mesures qu'elle pourrait prendre pour atténuer les préjudices subis par les individus concernés ;
- la façon dont les individus concernés seront informés de la violation des données personnelles, si nécessaire au vu des circonstances, et les mesures que ces personnes peuvent prendre pour atténuer les préjudices subis
- si la violation des données personnelles peut engager ou non la responsabilité d'une personne ou de tiers ;
- les communications internes (et externes si nécessaire) qui devront être publiées et à quel moment ;
- quelles sont les autres parties prenantes, hormis l'APD, qui doivent également être informées ;
- quels enseignements peuvent être tirés de la violation des données personnelles et quelles mesures peuvent être mises en place pour éviter qu'elle ne se reproduise.

  mesures peuvent être mises en place pour éviter qu'elle ne se reproduise.

5.3 L'APD doit-elle être avertie ?

Il n'est pas nécessaire de signaler toutes les violations des données personnelles à l'APD. Par exemple, il n'est pas nécessaire d'avertir l'APD lorsqu'une violation des données personnelles a peu de chances de faire courir un risque à qui que ce soit.

Lorsqu'il convient de signaler la violation des données personnelles à l'APD concernée, c'est le service juridique et de la conformité qui s'en chargera, après concertation avec le MD de la société.

La violation des données personnelles devra être signalée à l'APD concernée sans retard injustifié et si possible dans les 72 heures suivant la détection de ladite violation. Si le signalement n'est pas effectué dans les 72 heures, les raisons du retard devront être indiquées à l'APD.

5.4 Résolution

Après avoir averti l'APD concernée et pris en compte ses éventuelles observations, le service juridique et de la conformité devra consulter le MD de la société en ce qui concerne la gestion et la résolution de la violation des données personnelles, conformément au plan d'action défini.

6. QUELS ÉLÉMENTS DOIVENT ÊTRE SIGNALÉS À L'APD ?

L'APD doit être informée des éléments suivants :

- la nature de la violation des données personnelles, y compris les catégories de données personnelles et de personnes concernées, le nombre de personnes concernées et la quantité de données personnelles en péril ;
- les conséquences probables de la violation des données personnelles ;
- les mesures prises ou proposées pour remédier à la violation des données personnelles ;
- les mesures qui peuvent être prises par les personnes concernées pour limiter les effets néfastes de la violation des données personnelles ;
- le nom et les coordonnées du référent CRH auprès duquel des informations supplémentaires peuvent être obtenues concernant la violation des données personnelles.

7. NOTIFICATION DE LA VIOLATION DES DONNÉES PERSONNELLES AUX INDIVIDUS CONCERNÉS

Les personnes concernées ne devront être informées d'une violation des données personnelles que si celle-ci est susceptible de faire peser un risque élevé sur les droits et les libertés de ces personnes. La communication de la violation des données personnelles aux individus concernés devra se faire conformément au plan d'action élaboré.

La notification envoyée aux individus concernés inclura au moins les informations suivantes : (i) la nature et l'étendue de la violation des données ; (ii) les mesures prises pour limiter les conséquences négatives de la violation des données personnelles ; (iii) une description des conséquences prouvées et présumées de cette violation pour les données personnelles ; (iv) les mesures que la société a prises ou se propose de prendre pour atténuer les effets de la violation des données personnelles.

Il ne sera pas nécessaire d'informer les individus concernés lorsque : (a) la société a mis en place des mesures techniques et organisationnelles qui rendent les données personnelles inintelligibles aux personnes qui ne sont pas autorisées à les consulter, ou lorsque (b) la société a pris à la suite de la violation des mesures grâce auxquelles la menace élevée pesant sur les individus concernés aura peu de chances de se concrétiser.

8. REGISTRE DE VIOLATIONS DE DONNÉES

La société doit tenir un registre dans lequel sont consignées toutes les violations des données personnelles. Le service juridique et de conformité tiendra un registre des violations des données personnelles dont la société l'informe (un « **registre** »).

La finalité du registre des violations des données personnelles est : (i) de tirer des enseignements de la violation des données personnelles et de la façon dont elle a été gérée ; (ii) d'être en mesure de donner des réponses précises aux questions émanant des individus concernés ou de l'APD le cas échéant, et (iii) de fournir une synthèse à l'APD sur demande de cette dernière.

Pour chaque violation des données personnelles, les informations suivantes seront consignées dans le registre :

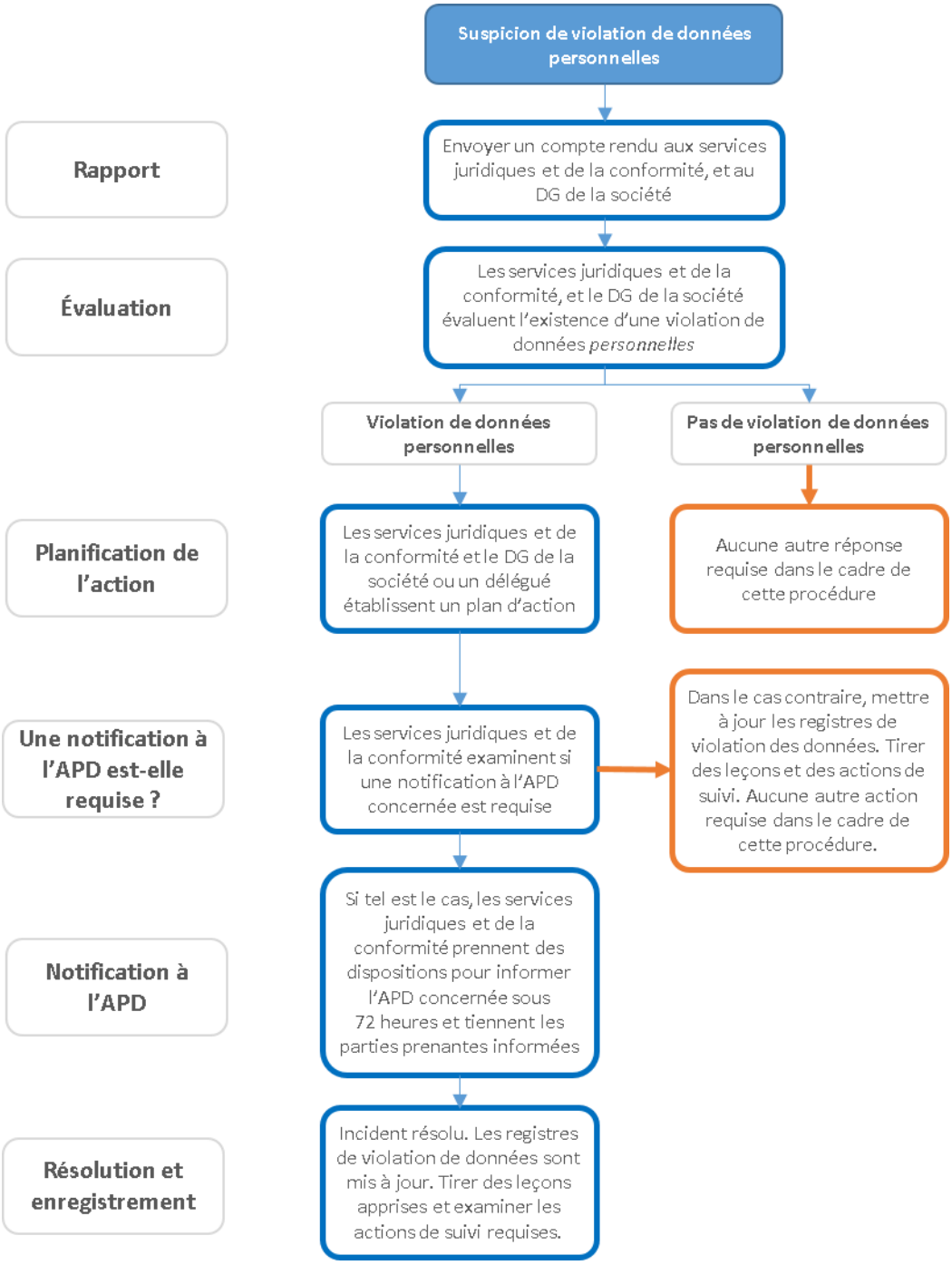
- la date et l'heure du signalement de la violation des données personnelles ;
- le nom et les coordonnées des individus concernés ;
- les faits et les caractéristiques de la violation des données personnelles ;
- la personne à laquelle la violation des données personnelles a été signalée et pourquoi ;
- les mesures de suivi prises après la découverte de la violation des données personnelles (par exemple, des mesures visant à empêcher que la violation des données personnelles ne se reproduise).

Le registre des violations des données personnelles signalées à l'APD doit être conservé par la société pendant au moins cinq ans.

Annexe 1

Graphique de la procédure en cas de violation des données personnelles

Si vous avez des questions ou avez besoin de conseils supplémentaires, veuillez contacter le service des RH ou votre DPO local. Le service juridique et de la conformité peut également vous fournir des explications sur cette procédure.



DROITS ET DEMANDES RELATIFS À LA PROTECTION DES DONNÉES DES PERSONNES

Le Règlement général sur la protection des données (« **GDPR** ») présente un large éventail de droits des personnes au sujet de leurs données personnelles (les « **droits des personnes** »).En conséquence, les personnes peuvent faire des demandes pour réexaminer, modifier, supprimer, corriger le traitement de leurs données personnelles, ou s'y opposer.

Le présent document a pour objet les éléments suivants :(1) expliquer en quoi consistent les Droits des personnes ; et (2) expliquer comment gérer la demande d'une personne à exercer de tels Droits des personnes (une « **demande** ») en conformité avec le GDPR ou d'autres lois applicables. Le graphique en **annexe** à ce document vise à illustrer le mode de gestion des demandes.

1. DROITS DES PERSONNES

Les Droits des personnes dans le cadre du GDPR comprennent :

A. Droit d'accès

Chaque OpCo (l'« **OpCo** »), en tant que Contrôleur des données, sur demande spécifique d'une personne, doit :

- confirmer si elle traite les données personnelles de la personne ;
- expliquer pourquoi et comment elle traite les données personnelles en question et fournir d'autres détails à la personne au sujet du traitement des données personnelles de celle-ci ; et
- fournir un exemplaire des données personnelles à cette personne.

B. Droit à l'effacement (également connu sous le nom de droit de suppression ou « le droit d'être oublié ») et à la rectification

Une personne peut demander un effacement ou une suppression de ses données personnelles dans certaines circonstances, notamment si, à tout moment, elle retire son consentement au traitement de ses données personnelles (lorsque le traitement est effectué conformément au consentement de la personne concernée).La personne peut aussi exiger que l'OpCo « rectifie » ou modifie ses données personnelles si celles-ci sont inexactes ou incomplètes.

Si l'OpCo a partagé les données personnelles avec un tiers (par exemple, un agent de traitement des données comme un fournisseur de services de paie), elle doit alors informer le tiers de l'effacement ou de la restriction des données personnelles en question.

C. Droit à la restriction

Une personne peut également exiger que l'OpCo limite le traitement de ses données personnelles lorsque des plaintes (par exemple, à propos de l'exactitude des données personnelles) sont en cours de traitement. Lorsque ce traitement est restreint, l'OpCo est autorisée à stocker les données personnelles, mais ne doit pas continuer à les traiter sauf si ou jusqu'à ce que la question soit réglée. De même, si l'OpCo a partagé les données personnelles avec un tiers (par exemple, un agent de traitement des données comme un fournisseur de services de paie), elle doit alors informer ce tiers de la restriction imposée sur le traitement des données personnelles de la personne en question jusqu'à nouvel avis. Après la levée de la restriction, le tiers doit également être notifié.

D. Droit à l'objection

Les personnes peuvent s'opposer au traitement de leurs données personnelles sur des motifs liés à leur situation particulière. L'OpCo doit cesser le traitement des données personnelles, sauf si elle peut démontrer des raisons impérieuses et légitimes en rapport au traitement (à déterminer au cas par cas).

Toutefois, les personnes peuvent émettre une objection sans avoir à fournir de justifications si une OpCo effectue un traitement à des fins de marketing direct.

Si une décision est prise sur le traitement automatisé de renseignements personnels, notamment le profilage, et lorsque cette décision est susceptible de produire un effet juridique sur la personne ou un effet qui pourrait sensiblement l'affecter, celle-ci a le droit de ne pas être soumise (sauf pour certaines exceptions) à une décision prise *uniquement* sur cette base. Parmi les exemples d'un tel traitement automatisé figurent les décisions de crédit en ligne.

E. Portabilité des données

Si une personne fournit à l'OpCo ses données personnelles, cette personne a le droit, sur demande :

- de recevoir une copie des données personnelles ; et/ou
- lorsque cela est techniquement possible, de demander l'envoi des données personnelles à une organisation tierce dans un format structuré et couramment utilisé.

2. GESTION DES DEMANDES

A. Répondre à une demande

L'OpCo doit communiquer avec la personne qui a fait la demande, et avec tout tiers avec qui les données personnelles ont été partagées, dès lors qu'une modification, une suppression ou une restriction est effectuée.

Les informations ou communications fournies aux personnes en réponse à une demande doivent être :

- réalisées dans un format concis, clair, facile à comprendre et facilement accessible, en utilisant un langage clair ;
- effectuées par écrit (p. ex. par lettre ou courrier électronique) ; et
- lorsqu'une personne fait une demande sous forme électronique (p. ex. par courrier électronique), la réponse peut aussi être fournie sous forme électronique (c.-à-d. par courrier électronique) si cela est possible, sauf si la personne émet une autre demande.

B. Date limite de réponse à une demande

Après réception d'une demande valide, la réponse doit être fournie « sans retard excessif », mais en tout état de cause, au plus tard un mois après réception de la demande. Cette période d'un mois peut être prolongée de deux mois supplémentaires si nécessaire, en tenant compte de la complexité et du nombre de demandes. L'OpCo doit informer la personne de toute prolongation dans le premier mois de réception de la demande, ainsi que des motifs du retard ou de la prolongation. Si l'OpCo possède un motif valable et légitime pour ne pas répondre à une demande dans les délais prescrits ou du tout, elle doit :(a) informer la personne « sans délai » de ces motifs, mais en tout état de cause, au plus tard un mois après réception de la demande ; et (b) informer la personne de son droit de déposer une plainte auprès de l'autorité de protection des données concernée.

C. Coûts de réponse à une demande

Toutes les communications/informations émises par l'OpCo relativement à une demande doivent être gratuites, sauf si la demande de la personne est « *manifestement infondée ou excessive* » (par exemple, des demandes répétées), auquel cas l'OpCo peut :(a) exiger des frais raisonnables à la personne ; ou (b) refuser la demande.

D. Des questions ?

Si vous avez des questions ou besoin d'une aide supplémentaire, l'OpCo peut envoyer les questions aux RH ou à son délégué à la protection des données (local).La personne chargée des questions juridiques et de conformité peut donner des conseils sur l'interprétation de cette procédure.
Vous pouvez toujours exercer vos droits en contactant le responsable GDPR de Marlux/STRADUS au numéro +32 13 679100.

Annexe 1

Gestion des demandes relatives aux données personnelles - graphique

Si vous avez des questions ou avez besoin de conseils supplémentaires, veuillez contacter le service des RH ou votre DPO local. La personne chargée des questions juridiques et de conformité peut donner des conseils sur l'interprétation de cette procédure.