**Politique générale sur le Traitement des Données à caractère personnel**

**IAME France**

**Mars 2019**

Champ d’application

IAME France (ci-après « La Société ») accorde une attention particulière au respect des droits, à la confidentialité et à la protection des Données personnelles en tant que droits fondamentaux de la personne protégés par le droit de l’Union européenne ou les lois nationales.

Cette politique explique les principes les plus importants de la protection des Données à caractère personnel et explique comment ces principes doivent être appliqués, notamment en application du nouveau règlement européen 2016/679 sur la protection des données, applicable dans tous les États membres de l'Union européenne à partir du 25 mai 2018.

Cette politique couvre toutes les Données personnelles collectées, traitées, partagées ou utilisées de quelque manière par la Société et s’applique à tous les travailleurs, employés ou travailleurs indépendants et collaborateurs, qui doivent se conformer aux principes qui y sont énoncés et aux obligations prévues par la loi sur le sujet.

Définitions

**Autorité de protection** : La CNIL ou toute autre autorité compétente pour la protection des Données personnelles.

**Base de données** : Tout fichier ou ensemble de fichiers de Données à caractère personnel, divisé en une ou plusieurs unités situées sur un ou plusieurs sites. Par exemple, constituent une base de données (papier) des archives dans lesquelles sont conservées la documentation concernant les employés. Les bases de données peuvent également être électroniques.

**Communication** : Fait de transmettre des Données personnelles à un ou plusieurs destinataires (autres que la Personne concernée, le Sous-traitant de données ou le Personnel autorisé), sous quelque forme que ce soit, y compris par le biais de leur mise à disposition ou de leur consultation.

**Données biométriques** : Données personnelles obtenues à partir d'un traitement technique spécifique lié aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent ou confirment l'identification unique, telles que des données de reconnaissance faciale ou des empreintes digitales.

**Données relatives aux condamnations pénales et aux infractions pénales** : Données à caractère personnel relatives aux condamnations pénales et aux infractions pénales ou aux mesures de sûreté connexes (par exemple, données relatives à la divulgation des condamnations pénales, casiers judiciaires, registre des sanctions administratives en fonction de l'infraction et des accusations en instance, ou statut du défendeur ou du suspect en vertu des articles 60 et 61 du code de procédure pénale).

**Données personnelles** : Toute information concernant une personne physique, identifiée ou identifiable, même indirectement, par référence à toute autre information, y compris un numéro d'identification personnel. Entrent dans cette définition, par exemple : les coordonnées de contact (nom, prénom, numéro de téléphone, email) dans les contacts Outlook ; les informations contenues dans les CV des candidats ; les informations sur les utilisateurs d'un ordinateur ou d'un site Web (adresse IP ou MAC, géolocalisation, par exemple) ; les photographies, les informations concernant une entreprise ou un professionnel. Les informations cryptées ou codées sont également des Données personnelles dans la mesure où il est possible de les réassocier, même indirectement, à la personne à laquelle elles font référence (que les codes permettant le déchiffrement soient détenus par la Société ou par des tiers).

**Catégories particulières de données** : Données personnelles révélant l’origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l’appartenance à un syndicat, ainsi que les données génétiques, données biométriques destinées à identifier de manière unique une personne physique, données liés à la santé (par exemple, certificat médical et registres médicaux ; un courrier électronique dans lequel le salarié déclare être malade, etc.) ou à la vie sexuelle ou à l'orientation sexuelle de la personne.

**Destinataire** : Personne physique ou morale, autorité publique, service ou autre organisme qui reçoit la communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

**Diffusion**: Publication ou divulgation de Données à caractère personnel sous quelque forme que ce soit, à un nombre indéterminé de destinataires (par exemple, la publication de données à caractère personnel peut être la diffusion dans un journal ou sur une page Web).

**Référent données personnelles** : il s’agit de la personne identifiée dans la Société qui représente le responsable de traitement pour la gestion pratique et opérationnelle des activités de traitement de Données à caractère personnel et agit en tant que point de contact pour toutes questions concernant la protection des Données à caractère personnel.

**Personne concernée** : personne physique identifiée ou identifiable intéressée à qui les Données personnelles font référence.

**Loi applicable en matière de protection des données à caractère personnel** : désigne le Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du Traitement des Données à caractère personnel et à la libre circulation de ces Données, abrogeant la directive 95/46/CE (« Règlement général sur la protection des Données » ou « RGPD »), la Loi informatique et liberté n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par l’ordonnance n°2018-1125 du 12 décembre 2018, ainsi que toute disposition légale ou règlementaire en matière de protection des Données à caractère personnel.

**Organisation internationale** : Une organisation et ses organismes subordonnés régis par le droit international public, ou tout autre organisme établi par ou sur la base d'un accord entre deux ou plusieurs États.

**Personnel autorisé** : Personnel sous l'autorité du responsable du traitement ou du sous-traitant du traitement, qui est désigné par le responsable du traitement ou le sous-traitant pour traiter ou utiliser des

Données à caractère personnel sur la base d'instructions spécifiques.

**Registre des activités de traitement** : Le document (papier ou électronique) contenant une description analytique des traitements effectués par la Société.

**Sous-traitant de données** : La personne physique, personne morale, l'administration publique, le service et tout autre organisme, association ou organisme qui traite des Données à caractère personnel pour le compte de la Société.

**Demande d'exercice de droits** : Demande, sous quelque forme que ce soit (verbalement ou par écrit), relative à l'exercice des droits prévus par la loi applicable sur la protection des Données à caractère personnel (par exemple, droit d'accès, droit à l’effacement, droit de rectification, droit à la limitation du traitement, etc.).

**Tiers** : personne physique ou morale, autorité publique, service ou autre organisme autre que la personne concernée, le responsable du traitement, le sous-traitant du traitement et le personnel autorisé (les personnes autorisées à traiter des Données à caractère personnel sous l'autorité directement du propriétaire ou du responsable).

**Responsable de traitement** : La personne physique, personne morale, l'administration publique et tout autre organisme, association ou organisme dont elle est responsable, qui prend, même conjointement avec un autre responsable, les décisions relatives aux finalités, aux méthodes de traitement des Données à caractère personnel et aux outils utilisés, y compris le profil de sécurité. Aux fins de la présente politique et en ce qui concerne le traitement des Données qui y sont décrites, le responsable de traitement est la Société.

**Transfert** : transfert des Données à caractère personnel dans un État ou une organisation internationale en dehors de l'Union européenne ou de l'Espace économique européen.

**Traitement** : Toute opération ou ensemble d'opérations concernant la collecte, l'enregistrement, l'organisation, la conservation, la consultation, le traitement, la modification, la sélection, l'extraction, comparaison, utilisation, interconnexion, blocage, communication, diffusion, suppression et destruction de données, même si elles ne sont pas enregistrées dans une base de données.

**Violation des données à caractère personnel** : Toute atteinte à la sécurité qui implique une destruction, une perte, une modification, une divulgation, une mise à disposition ou un accès accidentel ou illicite à des Données à caractère personnel transmises, stockées ou autrement traitées.

1. SYNTHESE DES TRAITEMENTS DES DONNEES PERSONNELLES MIS EN ŒUVRE PAR LA SOCIETE

L'utilisation des Données personnelles par la Société inclut la collecte, la gestion, le stockage et l’hébergement, principalement aux fins suivantes :

|  |  |
| --- | --- |
| Personnes concernées | Principales finalités d’utilisation des données à caractère personnel |
| Employés, collaborateurs, personnel en stage de formation et alternants | Gestion du personnel et obligations contractuelles et légales connexes |
| Candidats | Recherche et sélection du personnel |
| Personnel tiers (personnel embauché par des fournisseurs / entrepreneurs) | Accès aux locaux de l'entreprise  Exécution du contrat |
| Utilisateurs des sites Web de la Société (enregistrés ou non) | Gestion de sites Web |
| Fournisseurs personnes physiques / Personnel des fournisseurs personnes morales | Gestion des obligations contractuelles et légales |

Le détail des traitements effectués par la Société est reporté au Registre des activités de traitement tenu par le Référent données personnelles.

1. RÔLES ET RESPONSABILITÉS

La mise en œuvre d'une politique appropriée de protection des Données à caractère personnel exige, avant toute chose, que les personnes impliquées dans le Traitement des Données à caractère personnel soient clairement définies et identifiées, ainsi que leurs rôles et leurs droits et devoirs respectifs. Les personnes impliquées dans le Traitement des Données à caractère personnel au sein de la Société et / ou en son nom seront identifiées ci-dessous. Certains rôles sont expressément prévus par la Loi applicable en matière de protection des Données à caractère personnel, tandis que d'autres sont identifiés au sein de la Société, qui a décidé d’adopter un modèle d'organisation pour gérer les problématiques en lien avec la protection des Données à caractère personnel (tel que décrit à l'annexe 1).

* 1. Le Responsable de traitement

Le Responsable de traitement à caractère personnel est la Société.

* 1. Le Personnel autorisé à traiter les Données

Le Personnel autorisé est toute personne physique formée, entraînée et désignée pour effectuer les opérations de Traitement des Données à caractère personnel, y compris la collecte des Données, leur traitement (via des systèmes d'application ou manuellement), leur archivage, leur communication et leur diffusion (par exemple, les employés de la Société).

Ce Personnel autorisé :

* ne peut être qu’une personne physique ;
* doit respecter les limites suivantes concernant les traitements effectués :

1. ils doivent être nécessaires à la poursuite des finalités pour lesquelles les Données sont collectées par la Société ;
2. Ils doivent être conformes aux instructions fournies par la Société (toute instruction, donnée par écrit ou même oralement, si nécessaire) ;
3. Ils doivent être exécutés selon les besoins des tâches assignées au même personnel autorisé.

En ce qui concerne le Personnel autorisé travaillant dans l'entreprise (employés, salariés, stagiaires), il est précisé que :

Le personnel autorisé doit être soumis à une obligation de confidentialité spécifique qui peut être prévue dans leur contrat de travail ou par le biais d’accords de confidentialité spécifiques.

* La Société doit assurer la formation constante du Personnel autorisé pour le Traitement qui y est effectué. Le Personnel autorisé est tenu de participer aux sessions de formation organisées par la Société.
* Le Personnel autorisé doit contacter rapidement le Référent données personnelles en cas de suspicion d'une Violation potentielle des données personnelles.
  1. Le Référent données personnelles

La Société doit identifier le Référent données personnelles, qui effectue diverses tâches relatives à la protection des données à caractère personnel, telles que, par exemple :

1. Fournir, au nom de la Société, au personnel autorisé des instructions d'utilisation pour assurer que les données personnelles sont traitées légalement et correctement, exclusivement aux fins inhérentes à l'exercice des fonctions exercées, et d'une manière exacte, actualisée, pertinente, complète et non excessive par rapport aux fins pour lesquelles elles sont collectées et traitées.
2. S’assurer que seuls les outils mis à disposition par la Société pour le Traitement des Données sont utilisés ;
3. Mettre en œuvre toutes les exigences opérationnelles jugées nécessaires par la Société, afin que le Traitement des Données à caractère personnel se déroule dans le respect des réglementations et des dispositions en vigueur ;
4. Adopter des mesures pour contrôler l'application effective des mesures de sécurité et des instructions par la Société en matière de Traitement des Données pour les Sous-traitants et le Personnel autorisé ;
5. Gérer les Demandes d’exercice des droits des Personnes concernées et y répondre dans les délais prévus par la Loi applicable en matière de protection des Données à caractère personnel (un mois à compter de la réception de la Demande) ;
6. Surveiller le bon déroulement des activités de Traitement par le Personnel Autorisé et par les Sous-traitants ;
7. Identifier, en cas de nouveaux traitements devant être mis en place, leur conformité ;
8. Notifier l’Autorité de contrôle et éventuellement les Personnes concernées en cas de Violation de données à caractère personnel.
   1. Le Sous-traitant de données

Dans les cas où, dans le cadre des activités confiées par la Société à des prestataires de services ou des sociétés externes, des Données à caractère personnel sont traitées pour le compte de la Société :

1. Il est nécessaire de vérifier au préalable que ce Sous-traitant répond aux exigences en matière d'expérience, de fiabilité et de compétence, y compris en ce qui concerne les aspects de protection des Données à caractère personnel ;
2. Le Personnel autorisé ne procédera pas de manière indépendante à la sélection des fournisseurs qui agissent en tant que Sous-traitant du Traitement, mais consultera le Référent données personnelles qui procédera au choix final ;
3. Il est nécessaire de conclure un contrat concernant le Traitement des Données à caractère personnel - DPA - avec les prestataires qui traitent des Données à caractère personnel en tant que Sous-traitant de données. Le modèle de contrat est disponible auprès du Référent données personnelles ;
4. Il est conseillé de garder une liste à jour des prestataires agissant en tant que Sous-Traitant de données et de maintenir des contrats concernant le Traitement des données signées avec ces fournisseurs.
5. PRINCIPES FONDAMENTAUX À RESPECTER DANS LE TRAITEMENT DES DONNÉES PERSONNELLE
   1. Les principes généraux

Les Données personnelles doivent être traitées selon les principes suivants :

-**Légalité, proportionnalité et transparence** : …dans le respect de la Loi applicable en matière de protection des Données à caractère personnel ; de manière transparente, c'est-à-dire en conformité avec ce qui est énoncé et indiqué dans la politique de confidentialité ;

-**limitation des finalités** : … collectées et enregistrées à des fins spécifiques, claires, explicites et légitimes ;

-**Exactitude :** …exactes, concernant l'identité de la personne concernée et, le cas échéant, mise à jour et complète, de manière à ne pas donner lieu à des erreurs d'identification de la personne concernée. Par conséquent, des procédures doivent être mises en place pour rectifier ou supprimer les Données rapidement si inexactes ;

-**Minimisation des Données** : …pertinentes, c’est-à-dire qu’il doit exister un lien clair et étroit entre les Données collectées et les finalités du Traitement poursuivi, sans excéder les finalités pour lesquelles elles sont collectées (c’est le principe dit de proportionnalité qui interdit la collecte, la gestion et le traitement de Données à caractère personnel qui sont superflues par rapport aux finalités déclarées du Traitement);

-**Restriction de la durée de conservation** : … conservées sous une forme permettant l'identification de la Personne concernée pendant une période ne dépassant pas le temps nécessaire aux fins pour lesquelles les Données ont été collectées;

-**Intégrité et confidentialité** : …traitées de manière à garantir une sécurité adéquate des Données à caractère personnel, y compris au moyen de mesures techniques et organisationnelles appropriées, afin de prévenir un Traitement non autorisé ou illégal, ainsi que la perte, la destruction ou des dommages accidentels.

Selon le type de Traitement de Données (par exemple, le marketing), la catégorie de Données à caractère personnel (par exemple, les Données relatives à l'état de santé) ou le type de personnes concernées auxquelles les Données à caractère personnel (par exemple, les enfants) se rapportent, des obligations supplémentaires peuvent s’appliquer.

Les Données personnelles traitées en violation des principes et des règles prévus pour la protection des Données personnelles ne peuvent et ne doivent pas être utilisées.

* 1. Les bases légales du Traitement

Quand peut-on utiliser des Données à caractère personnel ?

Les Données ne peuvent être collectées et utilisées conformément aux principes énoncés ci-dessus que s'il existe l'une des bases juridiques suivantes :

* + La personne a consenti au traitement de ses données personnelle
  + Le traitement est nécessaire :
  + au respect d'une obligation légale (nationale ou découlant du droit de l’Union européenne)
  + à l’exécution d'un service faisant l'objet d'un contrat ou d'une demande formulée directement par la Personne concernée (par exemple, une demande d'assistance par courrier électronique ou des demandes précontractuelles);
  + à la sauvegarde des intérêts vitaux de la Personne concernée ou d'une autre personne physique;
  + pour la poursuite des intérêts légitimes du Responsable de traitement ou de tiers, à condition que ces intérêts ne prévalent pas sur les libertés et droits fondamentaux de la Personne concernée, en particulier si elle est mineure.

Il convient de noter que ces bases juridiques sont alternatives. Le consentement n’est ainsi pas toujours nécessaire, notamment lorsque d’autres bases légales sont applicables.

**Exigences applicables au consentement :**

|  |
| --- |
| Un consentement doit être obtenu selon les principes suivants :   * + **Éclairé** : une mention d’information complète a été transmise ;   + Émis en réponse d'une demande **spécifique** qui doit être:     - Séparé du reste du texte;     - Formulé dans un langage simple et clair;   + **Libre** : le consentement ne doit pas être obligatoire pour utiliser un service ou conclure un contrat, etc.   + **Documenté**: si le Traitement est basé sur le consentement, la souscription, la forme écrite ou la signature de l'intéressé n'est pas requise (sauf dans le cas de Catégories particulières de données), mais le Responsable de traitement doit avoir la possibilité de démontrer que la Personne concernée a donné son consentement à l'égard de ce traitement particulier. La date et le lieu du consentement doivent faire l’objet d’un suivi. En outre, des règles spécifiques s'appliquent au Traitement de Catégories particulières de données et de Données relatives à des condamnations pénales et à des infractions.   + **Toujours révocable**, sans que la révocation ait des effets négatifs pour la Personne concernée. Les modalités selon lesquelles le consentement peut être révoqué ne doivent pas entraîner d'effort excessif pour la Personne concernée : le retrait du consentement doit être possible dans les mêmes modalités par lesquelles il a été accordé. |

La Société doit identifier une base juridique appropriée avant de procéder au Traitement des Données personnelles des Personnes concernées. Pour plus d'informations, reportez-vous aux instructions destinées au Personnel autorisé.

* 1. Limites à la communication / partage de Données

Les Données personnelles ne peuvent être communiquées (par exemple par courrier électronique) ou partagées (par exemple via un service de cloud) avec des tiers que sous réserve du respect de l’une des conditions suivantes :

1. que la personne à qui les Données personnelles sont communiquées est un Sous-traitant de la Société qui agit pour le compte de la Société et s'engage à respecter la législation en matière de protection de la vie privée au moyen d'un contrat spécial concernant le Traitement des Données personnelles ;
2. que la Personne concernée a donné son consentement valable pour une telle communication ;
3. que la communication a lieu conformément à une obligation légale (par exemple, la communication des données du travailleur à la sécurité sociale) ou sur ordre d'une autorité judiciaire (par exemple, la communication de données à un magistrat);
4. cette communication est essentielle pour pouvoir donner suite à la demande formulée directement par la Personne concernée ;
5. cette communication est essentielle pour la sauvegarde des intérêts vitaux de la Personne concernée.

Par conséquent, avant de transmettre, de communiquer ou de partager avec des tiers des Données personnelles collectés par la société, il est toujours nécessaire de vérifier que l'une des conditions ci-dessus est remplie.

* 1. Limites concernant le Transfert de Données en dehors de l'EEE

Avant de transférer des Données à caractère personnel à des tiers situés dans des pays non membres de l'Union européenne ou ne faisant pas partie de l'Espace économique européen (par exemple, si les Données sont stockées sur des serveurs situés en dehors de l'EEE, si elles sont envoyées en dehors de l'EEE par courrier électronique ou tout autre moyen, directement par la Société ou ses fournisseurs), le Personnel doit vérifier que les contrats avec les tiers pour le Transfert répondent à l’une des conditions suivantes:

* La Commission européenne a établi que le pays en question offre un niveau de protection adéquat des Données à caractère personnel ; pour cela il faut vérifier s'il y a une décision d'adéquation;
* En l'absence d'une décision d'adéquation, il a été prévu des garanties suffisantes, telles que, à titre d'exemple:
* La stipulation de clauses contractuelles types (ou clauses contractuelles types "CSC") adoptées par la Commission européenne;
* L’adoption de règles d'entreprise contraignantes ou "BCR";
* Un code de conduite approuvé conformément à l'article 40 du règlement, ainsi que l'engagement contraignant et impératif du Responsable du traitement ou du Sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes:
* Un mécanisme de certification approuvé conformément à l'article 42 du règlement ;
* Un autre mécanisme de Transfert approuvé par la Commission européenne (par exemple, les mécanismes du bouclier de sécurité ou « *Privacy Shield* »").
  1. Conservation des Données personnelles

Conformément aux règlements et aux réglementations applicables en matière de protection des données, la société conserve les Données sous une forme permettant l'identification de la personne concernée pendant une période ne dépassant pas la réalisation des finalités pour lesquelles les Données sont collectées. En outre, la société est invitée à adopter des règles de conservation qui tiennent compte de l’adoption de mesures de sécurité techniques et organisationnelles appropriées. La société a identifié les conditions de conservation des Données personnelles.

Les Données personnelles sont stockées sous forme papier et électronique, en adoptant les mesures de sécurité requises par la législation en vigueur et exclusivement pendant le temps nécessaire pour se conformer aux obligations légales requises à cet effet.

* 1. Obligations de sécurité

Les mesures de sécurité pour conserver et protéger les Données sont mises en place en fonction des règles de l’état de l’art, des exigences techniques, de la nature des Données et des caractéristiques spécifiques du Traitement, de manière à minimiser, par l'adoption de mesures de sécurité appropriées, les risques de destruction ou de perte, même accidentels, des Données, d'accès non autorisé ou de traitements non autorisés ou non conformes aux finalités de la collecte.

Les mesures de sécurité peuvent être définies comme toutes les mesures techniques et organisationnelles prises pour garantir que :

-Les Données personnelles ne sont pas détruites ou perdues, même de manière accidentelle ;

-seules les personnes autorisées ont accès aux Données personnelles ;

-aucun Traitement n'est contraire à la loi ou non conforme à la finalité pour laquelle les Données personnelles ont été collectées.

* 1. Violation de Données personnelles (Data Breach)

En cas de Violation des données personnelles, à savoir toute perte, destruction, modification ou diffusion des Données ou tout accès non autorisé à celles-ci, toute personne se rendant compte d’une telle violation doit en informer immédiatement le Responsable de traitement.

Une Violation de données doit être communiquée par la Société à l'Autorité de contrôle compétente selon les conditions suivantes et conformément à la Loi applicable en matière de protection des Données à caractère personnel.

En cas de Violation des Données personnelles, la Société est tenue de :

**i) informer l'Autorité de contrôle compétente de la Violation dans un délai maximum de 72 heures à compter du moment où elle en a eu connaissance,** à moins que la Violation de Données à caractère personnel ne présente pas un risque pour les droits et libertés des personnes physiques. Si la notification à l'Autorité de contrôle n'est pas faite dans un délai de 72 heures, elle doit être accompagnée des raisons du retard.

**La notification doit au moins :**

a) décrire la nature de la violation des Données à caractère personnel, y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif de Données à caractère personnel en cause ;

b) communiquer le nom et les coordonnées d'un contact auprès de qui il est possible d'obtenir davantage d’informations ;

c) décrire les conséquences probables de la Violation des Données personnelles ;

d) décrire les mesures adoptées ou proposées par le Responsable de traitement des données pour remédier à la Violation des Données à caractère personnel et, le cas échéant, pour en atténuer les éventuels effets négatifs.

Dans les cas où et dans la mesure où il n'est pas possible de fournir toutes les informations en même temps à l'Autorité de contrôle, les informations peuvent être fournies par étapes successives sans autre délai injustifié.

**ii) Lorsque la Violation de Données à caractère personnel est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques,** la Société doit informer les Personnes concernées de la Violation des Données à caractère personnel dans les meilleurs délais.

La communication à la Personne concernée doit décrire dans un langage simple et clair la nature de la Violation des Données à caractère personnel et contient au moins :

* + - * 1. Le nom et les coordonnées d'une personne de contact interne pour obtenir des informations complémentaires ;
        2. Une description des conséquences probables de la Violation des Données personnelles ;
        3. Les mesures adoptées ou proposées par le Responsable de traitement des données pour remédier à la Violation des Données à caractère personnel et, le cas échéant, pour en atténuer les éventuels effets négatifs.

La communication à la Personne concernée n’est pas nécessaire si l’une des conditions suivantes est remplie :

1. Le Responsable de traitement des données a mis en place les mesures de protection techniques et organisationnelles appropriées et les a appliquées aux Données à caractère personnel faisant l'objet de la Violation, en particulier celles destinées à rendre les Données à caractère personnel incompréhensibles à quiconque n'est pas autorisé à y accéder, tels que le chiffrement ou la pseudonymisation ;
2. Le Responsable de traitement des données a par la suite adopté des mesures visant à prévenir la survenue d'un risque élevé pour les droits et libertés des personnes concernées ;
3. Cette communication nécessiterait des efforts disproportionnés. Dans ce cas, une communication publique ou une mesure similaire est prise, par laquelle les Personnes concernées sont informées.

La Société doit également documenter toute Violation de Données personnelles, notamment :

- les circonstances s'y rapportant ;

- les conséquences ;

- les mesures prises pour y remédier.

Cette documentation permet à l’Autorité de contrôle de vérifier la conformité de la Société. À cette fin, la Société tient un registre spécial des violations subies (même si celles-ci n'ont pas été notifiées à l'Autorité). Des règles plus spécifiques pour la gestion des violations de Données figurent à **l'annexe 1.**

* 1. Demandes d’exercice des droits par les Personnes concernées

La Loi applicable en matière de protection des Données à caractère personnel attribue aux personnes concernées divers droits concernant le Traitement de leurs Données à caractère personnel.

|  |  |
| --- | --- |
| DROIT D’ACCES | Obtenir une copie des données traitées par le Responsable de traitement concernant la Personne concernée |
| DROIT DE RECTIFICATION / SUPPRESSION | Obtenir la modification, la mise à jour ou la suppression de données qui seraient incorrectes, incomplètes ou obsolètes. |
| DROIT À LA LIMITATION DU TRAITEMENT | Obtenir une limitation de l'utilisation des données (par exemple, suspension de l'utilisation des données à des fins d'analyse de marché) |
| DROIT À LA PORTABILITÉ DES DONNÉES | Obtenir les Données personnelles fournies par la Personne concernée dans un format structuré, couramment utilisé et lisible par un dispositif automatique afin de les transmettre à un autre responsable |
| DROIT D’OPPOSITION | Obtenir l’arrêt du Traitement des données dans certaines circonstances |
| LE DROIT DE NE PAS ÊTRE SOUMIS À UNE DÉCISION FONDÉE SUR UN TRAITEMENT AUTOMATISÉ | Ne pas être soumis à une décision fondée uniquement sur un Traitement automatisé, y compris le profilage, produisant des effets juridiques qui la concernent ou affectent de manière significative de façon similaire sa personne |
| DROIT DE RÉVOCATION DU CONSENTEMENT | Retirer son consentement à tout moment |

La Société met à la disposition des personnes concernées l'adresse électronique [info@iamefrance.com](mailto:info@iamefrance.com) , destinée à recevoir des demandes de protection de Données à caractère personnel par les Personnes concernées. Cette adresse est indiquée dans la politique de confidentialité mise à la disposition des Personnes concernées. En outre, ces derniers peuvent adresser leurs demandes d’exercice de leurs droits en écrivant au siège social de la Société, dont l’adresse est indiquée dans la politique mise à la disposition de la Personne concernée.

Dans le cas d’une demande adressée directement au personnel de la Société par le biais d'autres adresses e-mail, cette demande doit dans tous les cas être prise en charge pour être gérée ultérieurement.

Lorsque le personnel reçoit une demande par courrier électronique concernant la protection des Données à caractère personnel, il est tenu de communiquer cette demande à l'adresse [info@iamefrance.com](mailto:info@iamefrance.com) , en prenant soin de conserver les informations reçues et de ne pas divulguer leur contenu de quelque manière que ce soit.

Si la demande a été envoyée par la poste, il incombera au personnel de la transmettre au Responsable de la conformité Données personnelles. Enfin, si le personnel reçoit des demandes sous forme orale, il doit en prendre note et en transmettre le contenu par écrit à l’adresse [info@iamefrance.com](mailto:info@iamefrance.com) , en prenant soin de ne pas diffuser le contenu de la demande.

Dans tous les cas, le personnel doit procéder à la transmission de la demande sans délai et au plus tard deux jours à compter de la réception de la demande par la Personne concernée.

* + 1. Vérification du demandeur (preuve d'identité)

En cas de réception de la demande d'une Personne concernée qui entend exercer ses droits à la protection des Données personnelles, il peut être approprié de vérifier l'identité de la personne qui fait la demande dans certaines circonstances.

Cette vérification est superflue si l’identité de la Personne concernée est évidente. C’est notamment le cas lorsque la personne concernée a envoyé une demande à partir de la même adresse électronique qui lui a été précédemment attribuée par la Société ou lorsqu’elle fournit des détails permettant son identification.

Si, en revanche, la demande provient d'une adresse électronique ou d'un lieu de résidence autre que celui connu de la Société, ou s'il existe des raisons valables de douter de l'identité du demandeur, le personnel recevant la demande sera tenu d'effectuer les vérifications complémentaires suivantes :

* 1. Si la Personne concernée envoie sa demande depuis une adresse autre que celle connue de la société, il sera nécessaire de demander à cette dernière de confirmer son identité et de préciser l'adresse e-mail fournie à la société. Dans le cas où l'accès aux données est demandé, le demandeur doit communiquer toute information demandée afin d'exclure l'accès non autorisé aux Données de la personne concernée.
  2. Si la Personne concernée n'est pas en mesure de fournir ces informations, d'autres informations telles que la date de naissance et des informations supplémentaires sur les interactions entre la personne concernée et la société peuvent être demandées.
  3. Enfin, s'il n'est pas possible de vérifier l'identité de la Personne concernée d’une autre manière, une copie d'un document permettant l'identification de la personne concernée, par exemple la carte d'identité, le permis de conduire, peut être demandée.
     1. Vérification du contenu de la demande

La société doit procéder à la vérification préliminaire du contenu des demandes.  
En présence de demandes ambiguës de la Personne concernée (par exemple parce qu'elle ne spécifie pas quel droit elle souhaite exercer), il sera possible de contacter cette dernière pour lui demander de préciser le contenu de sa demande ou de fournir des détails supplémentaires.

* + 1. Réponse aux demandes

Sauf dans les cas où la loi prévoit un délai de réponse plus court, les décisions doivent être communiquées à l'intéressé dans un délai d'un mois à compter de la communication par l'intéressé d'informations suffisantes pour donner suite à sa demande.

Il est possible de prévoir un délai plus long (au maximum trois mois à compter de la réception de la demande) uniquement dans les cas où cela est strictement nécessaire pour exécuter une demande d'une complexité particulière - nécessitant des investigations supplémentaires- ou en raison de la gestion d’un grand nombre de demandes simultanées. En cas de prolongation, l'intéressé doit être informé de la raison du retard dans un délai d'un mois à compter de la réception de la demande.

Si une demande est rejetée partiellement ou totalement, le demandeur recevra une explication écrite indiquant la ou les raison (s) du refus. Les demandeurs qui souhaitent contester la décision de rejet de leur demande doivent être informés de la possibilité de soumettre une plainte à une Autorité de contrôle et d’un recours juridictionnel.

La Société conservera la documentation de la demande et des décisions liées à celle-ci. Cette documentation sera conservée conformément aux politiques de conservation de documents de la société et dans un format qui identifie le demandeur uniquement pendant le temps nécessaire à des fins légitimes. Pour connaître les délais et les méthodes de conservation des données, veuillez-vous reporter aux politiques adoptées en interne concernant la protection des Données à caractère personnel et la conservation des données.

La décision d'accepter ou de rejeter une demande doit être fondée sur la Loi applicable en matière de protection des Données à caractère personnel.

1. OBLIGATIONS EN CAS DE NOUVEAU TRAITEMENT DE DONNÉES PERSONNELLES
   1. Le « nouveau » traitement des Données personnelles

Dans les cas de nouveaux traitements ou de modifications du traitement de Données à caractère personnel déjà existants, le Personnel autorisé doit contacter le Référent données personnelles avant le début ou la modification du traitement. Ce Responsable doit identifier les risques éventuels et les éventuelles lacunes en matière de conformité avec la législation applicable en matière de protection des Données à caractère personnel.

* 1. L’analyse d’impact sur la protection des données et les traitements "à risque"

Les traitements qui impliquent l’utilisation de nouvelles technologies et qui, compte tenu de la nature, de l’objet, du contexte et des finalités du Traitement, peuvent présenter un risque élevé pour les droits et libertés des personnes, doivent être soumis à une analyse préalable : une analyse d'impact de la société sur la protection des données (conformément à l'article 35 du règlement sur la protection de la vie privée).

L’analyse d’impact sur la protection des données est requise notamment dans les cas suivants :

* 1. Une évaluation systématique des aspects personnels des personnes, fondée sur un traitement automatisé, y compris le profilage, sur la base de laquelle sont prises des décisions ayant des effets juridiques ou ayant une incidence importante sur ces personnes ;
  2. Le Traitement, à grande échelle, des Catégories particulières de données à caractère personnel (données sensibles, judiciaires, biométriques ou génétiques) ;
  3. Le Traitement permet la Surveillance systématique à grande échelle d'une zone accessible au public.

L'analyse d'impact sur la protection des données contient au moins :

1. Une description systématique des traitements envisagés et des finalités du traitement, y compris, le cas échéant, de l'intérêt légitime poursuivi par le Responsable de traitement ;
2. ii) une évaluation de la nécessité et de la proportionnalité des traitements par rapport aux finalités ;
3. Une évaluation des risques pour les droits et libertés des personnes concernées ;
4. iv) les mesures envisagées pour faire face aux risques, y compris les garanties, les mesures de sécurité et les mécanismes visant à assurer la protection des Données à caractère personnel et à démontrer le respect du droit applicable en matière de protection des Données à caractère personnel, en tenant compte des droits et intérêts légitimes des personnes concernées.

Si, une fois l’analyse d’impact réalisée, il apparaît que le Traitement peut présenter un risque élevé en l’absence de mesures adoptées par la Société, celle-ci peut également, avec l’aide du Référent données personnelles, consulter au préalable la CNIL.

* 1. Protection des données dès la conception et par défaut

Conformément aux principes de protection des données dès la conception (« *Privacy by design*») et de protection des données par défaut (« *Privacy by default* »):

- le personnel autorisé doit, avant le début de tout Traitement de Données à caractère personnel (à la fois lors de la détermination des outils de Traitement des Données et au moment du traitement), s'assurer qu'il a été effectué les évaluations et les mesures techniques et organisationnelles nécessaires pour mettre effectivement en œuvre les principes de protection des Données et intégrer les garanties nécessaires pour protéger les droits des Personnes concernées, en tenant compte de l'état de l’art et des coûts de mise en œuvre, ainsi que la nature, la portée, le contexte et la finalité du Traitement, mais également des risques pour les droits et libertés des personnes physiques.

-le Personnel autorisé doit s'assurer que la Société a mis en place des mesures techniques et organisationnelles adéquates pour garantir que, par défaut, seules les Données à caractère personnel nécessaires à chaque finalité spécifique du Traitement soient traitées. Cette obligation s'applique en fonction du nombre de Données personnelles collectées ; de la portée du Traitement ; de la période de conservation des données ; de l'accessibilité.

* 1. Registre des activités de traitement

La Société conserve une trace des activités de Traitement de Données à caractère personnel effectuées par la Société en tant que Responsable de traitement.

Afin de maintenir la mise à jour constante de ce Registre, le Référent données personnelles est tenu d’intégrer toute variation par rapport aux informations enregistrées, et dans tous les cas de le mettre à jour au moins une fois par an. Dans tous les cas, il est également conseillé au personnel autorisé de signaler rapidement dans le Registre toute modification substantielle du type de données traitées, des Personnes concernées, des finalités du Traitement, des Transferts et du partage des données avec des tiers.

En cas de nouveaux traitements ou de modifications de ceux déjà existants, le Référent données personnelles doit être immédiatement notifié afin de mettre à jour le Registre des activités de traitement.

1. REGLES SUR L'UTILISATION CORRECTE DES OUTILS INFORMATIQUES
   1. Utilisation de l'ordinateur personnel et des ordinateurs portables

L'ordinateur personnel confié à l'employé et / ou au collaborateur est un outil de travail. Toute utilisation non inhérente à l'activité professionnelle peut contribuer à générer des coûts de maintenance et, surtout, des menaces à la sécurité. L'accès à l'ordinateur est protégé par des informations d'identification, qui doivent être conservées par la personne autorisée avec la plus grande diligence et ne doivent pas être divulguées. Les informations d'identification sont également activées pour l'accès au réseau, pour l'économiseur d'écran et pour les programmes.

Il est interdit d'installer des programmes de l'extérieur sauf avec l'autorisation expresse du Référent données personnelles, car il y a un grave danger d'importer des virus informatiques et d’affecter la stabilité des applications informatiques. L'utilisation de programmes autres que ceux officiellement installés par la structure n'est pas autorisée. De plus, le personnel autorisé ne peut pas modifier les fonctions configurées sur son propre ordinateur sans l'autorisation préalable du Référent données personnelles. Le Personnel autorisé ne doit pas laisser un ordinateur sans surveillance, connecté au réseau, en raison de l'utilisation possible par un tiers sans qu'il puisse prouver l'utilisation abusive. En cas d’absence temporaire, l’économiseur d’écran doit être activé. L'ordinateur doit être éteint tous les soirs avant de quitter les bureaux ou en cas d'absence prolongée du poste de travail. Il est interdit d'installer sur les ordinateurs un périphérique de stockage ou de communication. Toute personne autorisée au Traitement doit porter une attention particulière aux applications de source externe, en avertissant le Référent données personnelles au cas où des virus, les logiciels malveillants ou ransomware sont détectés. Le personnel autorisé ne doit pas stocker des fichiers dont la nature est scandaleuse ou prônant la discrimination par rapport au sexe, la langue, la religion, la race, l'origine ethnique, l'appartenance syndicale, et/ou politique.

L'utilisateur est responsable de l'ordinateur portable Pc qui lui est attribué et doit le conserver avec soin pendant tout déplacement et pendant son utilisation sur le lieu de travail. Les ordinateurs portables utilisés à l'extérieur (conférences, visites en entreprise, etc.) doivent être conservés dans un endroit protégé. Les règles d'utilisation pour les ordinateurs connectés au réseau s'appliquent aux ordinateurs portables, une attention particulière étant accordée à la suppression de tous les fichiers traités sur ces ordinateurs avant le retour.

* 1. Utilisation du réseau internet

Le réseau interne contient des informations strictement professionnelles et ne peut pas être utilisé à des fins différentes ; par conséquent, aucun fichier non lié au travail ne peut être stocké même pour de courtes périodes, sur le réseau interne. Les identifiants d’accès au réseau et aux programmes sont secrets et doivent être communiqués et gérés conformément aux procédures indiquées ; il est absolument interdit d'entrer dans le réseau et les programmes avec d'autres noms d'utilisateur.

Le nettoyage périodique (au moins tous les six mois) des archives est une bonne pratique à mettre en place, et notamment la suppression des fichiers obsolètes ou inutiles ; Il incombe à l'utilisateur d'imprimer des fichiers uniquement si cela est strictement nécessaire et de les retirer rapidement des imprimantes.

* 1. Utilisation du téléphone de l'entreprise

Le téléphone, mis à disposition par la Société, est un outil nécessaire à la réalisation de l'activité professionnelle : les personnes et / ou employés sont responsables de l'utilisation correcte du téléphone. Il est recommandé d'éviter d'utiliser le téléphone de la Société pour des raisons autres que celles strictement liées au travail lui-même.

* 1. Utilisation du courrier électronique

La boite mail affectée par la Société à l'utilisateur est un outil de travail : les utilisateurs des boîtes mail sont responsables de l'utilisation correcte de celles-ci. Il est interdit d'utiliser les boîtes mail de la Société pour envoyer des messages personnels ou pour participer à des débats, des forums ou des listes de diffusion, sauf autorisation expresse.

La boîte mail doit être organisée, en supprimant les documents inutiles et particulièrement les pièces jointes encombrantes ; il est impératif de vérifier les pièces jointes des courriers électroniques avant de les utiliser (ne téléchargez pas de fichiers exécutables ni de documents provenant de sites Web inconnus ou de sites FTP). Il est interdit d'envoyer des chaînes télématiques. Dans tous les cas, les pièces jointes de ces messages ne doivent pas être activées.

* 1. Utilisation du réseau Internet

L’outil informatique nécessaire à la navigation sur Internet est un outil indispensable au bon fonctionnement de la Société : le réseau informatique de la Société permet d’accéder à toutes les ressources informatiques utiles à l’activité (zone partagée, imprimantes, applications, etc.).

La Société peut se doter d'un logiciel de filtrage Web afin d'empêcher l'accès à des sites pouvant exposer les utilisateurs et la Société à des risques de sécurité, à la perte de données ou sans rapport avec le travail. La navigation sur Internet n'est pas autorisée pour des raisons autres que celles strictement liées au travail lui-même (en particulier, il est interdit de naviguer sur des sites dont le contenu est contraire à la loi ou qui peuvent révéler des opinions politiques, religieuses, philosophiques, etc…). Il est interdit de télécharger des logiciels gratuits (freeware) et des partagiciels provenant de sites Internet, sauf autorisation expresse ; il est également interdit de participer à des forums non professionnels, d’utiliser des services de messagerie en ligne (à l’exclusion des outils autorisés) d’utiliser des pseudonymes (ou surnoms), pour effectuer des opérations d’achats en ligne.

* 1. Protection antivirus

Tout personnel autorisé doit se comporter de manière à réduire le risque d’attaque par virus ou tout autre logiciel malveillant du système informatique de la Société. Chaque personne autorisée est tenue de vérifier le bon fonctionnement et la mise à jour du logiciel installé, conformément aux procédures établies.

Si le logiciel antivirus détecte la présence d'un virus, la personne autorisée doit immédiatement suspendre le traitement en cours sans éteindre l'ordinateur et signaler sans délai l'incident. L'utilisation d'une unité de stockage (clé USB, disque dur amovible, etc.) d'origine inconnue n'est pas autorisée ; toute application extérieure à la Société doit être vérifiée au moyen du programme antivirus avant son utilisation et, si un virus est détecté, doit être remise au Responsable du traitement.

1. Contrôles

La Société se réserve le droit de procéder à des contrôles réguliers et / ou occasionnels de l’utilisation du réseau, du courrier électronique et d’Internet pour vérifier que leur utilisation est conforme aux dispositions de la présente section 5.

**Annexe 1 - Lignes directrices pour la gestion des atteintes à la sécurité des Données ("violation de données")**

Si le Personnel de Traitement autorisé détecte une éventuelle Violation des Données, il doit en informer le plus tôt possible le Référent données personnelles.

Le Référent données personnelles doit recevoir des informations sur l'événement, telles que la date et l'heure de l'événement, les Données personnelles concernées, l'objet de la Violation de données (par exemple, système d'information, rapport papier, ordinateur, clé USB), comment s'est produite la Violation de données. En tout état de cause, le personnel autorisé doit partager avec le Référent données personnelles les informations qu’il juge utiles pour lui fournir le plus grand nombre d’informations sur les caractéristiques de la prétendue Violation de données.

En tout état de cause, il est interdit au personnel autorisé de divulguer à l’extérieur de la Société les informations relatives à une Violation présumée des données.

Signalement de la Violation de données présumée :

Le Référent données personnelles qui reçoit le rapport détermine si la Violation de données en est bien une.

Si un Sous-traitant détecte une possible Violation de données, il doit immédiatement informer la Société par téléphone et / ou par courrier électronique. En outre, le Sous-traitant doit contacter le Responsable de traitement de manière régulière pour fournir, en cas de Violation de données à caractère personnel que celle-ci traite pour le compte et sur instruction de la société, la collaboration nécessaire pour identifier la cause de la Violation présumée de données, pour déterminer les mesures de sécurité nécessaires à adopter pour éviter que la Violation de données ait des conséquences négatives sur les droits des personnes concernées et, en tout état de cause, pour coopérer dans la gestion de la Violation.