SOCIETE DE GESTION PREVOIR	*Procédure réf. 165*

PROTECTION DES DONNEES PERSONNELLES

Emetteur :	**Destinataires :**
- Direction générale	- Tous collaborateurs

Mise à jour du : 15 juin 2018

SOMMAIRE

1. OBJET ET PERIMETRE DE LA PROCEDURE

La présente procédure est applicable à la société de gestion de portefeuille SOCIETE DE GESTION PREVOIR (la « Société »).

Elle précise les conditions de recueil et de traitement des données personnelles des personnes physiques (collaborateurs, clients, tiers…).

Elle respecte les dispositions du Règlement Général sur la Protection des Données (RGPD) applicable depuis le 25 mai 2018. RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors qu'elle est établie sur le territoire de l'Union européenne et que son activité cible directement des résidents européens. Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes.

Par « *données personnelles* », on entend : « *toute information se rapportant à une personne physique identifiée ou identifiable* ».

Une personne peut être identifiée :

- directement (exemple : nom, prénom) ;

- indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : numéro de sécurité sociale) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, détenant tel compte).

Une base marketing contenant de nombreuses informations précises sur la localisation, l'âge et les comportements d'achats de consommateurs, y compris si leur nom n'est pas stocké, est considérée comme un traitement de données personnelles, dès lors qu'il est possible de remonter à une personne physique déterminée en se basant sur ces informations.

Un « *traitement de données personnelles* » est une opération, ou ensemble d'opérations, portant sur des données personnelles quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Exemples : tenue d'un fichier de ses clients, collecte de coordonnées de prospects via un questionnaire, mise à jour d'un fichier de fournisseurs, etc…

En revanche, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers « papier » sont également concernés et doivent être protégés dans les mêmes conditions.

La Commission nationale de l'informatique et des libertés, (CNIL) est le régulateur français des données personnelles.

La CNIL accompagne les acteurs privés et publics dans la mise en œuvre de leur conformité en matière de protection des données personnelles.

Elle reçoit et traite les réclamations des particuliers et dispose des pouvoirs de contrôles sur place ou en ligne.

Elle peut imposer à un acteur de régulariser son traitement (mise en demeure) ou prononcer des sanctions (amende, etc.).

2. PRINCIPES GENERAUX

La Société doit respecter les principes généraux suivants :

- <u>Instaurer la confiance avec les personnes qui confie ses données personnelles</u>

La Société respecte les droits pour des personnes lui confiant ses données personnelles, lui permettant de maîtriser ses données en leur conférant des droits : droits d'accès, de rectification, d'effacement, d'opposition, etc…

Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire que la Société ne peut pas collecter ou traiter des données personnelles simplement au cas où cela serait utile un jour. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de l'activité professionnelle.

Pour chaque traitement il convient de vérifier :

- que les données traitées sont nécessaires aux activités de la Société ;
- que la Société ne traite aucune donnée dite « sensible » ou, si c'est le cas, que la Société a bien le droit de les traiter (voir paragraphe suivant) ;

- que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
- que la Société ne conserve pas les données au-delà de ce qui est nécessaire.

➢ Etre vigilant sur les « données à risques »

Certaines données ou certains types de traitements nécessitent une vigilance particulière :

Sont notamment concernées les données dites « sensibles » :

- révélant l'origine prétendument raciale ou ethnique ;
- portant sur les opinions politiques, philosophiques ou religieuses ;
- relatives à l'appartenance syndicale ;
- concernant la santé ou l'orientation sexuelle ;
- génétiques ou biométriques.

Les données d'infraction ou de condamnation pénale font également l'objet de règles particulières. Ces données ne peuvent être utilisées que sous certaines conditions strictement encadrées par la loi Informatique et libertés et par le RGPD.

Il convient également d'être particulièrement vigilant lorsque le traitement a pour objet ou pour effet :

1. l'évaluation d'aspects personnels ou notation d'une personne (exemple : scoring financier) ;
2. une prise de décision automatisée ;
3. la surveillance systématique de personnes (exemple : télésurveillance) ;
4. le traitement de données sensibles (exemple : santé, biométrie, etc.) ;
5. le traitement de données concernant des personnes vulnérables (exemple : mineurs) ;
6. le traitement à grande échelle de données personnelles ;
7. le croisement d'ensembles de données ;
8. des usages innovants ou l'application de nouvelles technologies (exemple : objet connecté) ;
9. l'exclusion du bénéfice d'un droit, d'un service ou contrat (exemple : liste noire).

Si les traitements de données répondent à au moins 2 de ces 9 critères, la Société doit conduire une analyse d'impact sur la protection des données (*PIA : Privacy Impact Assesment*), avant de commencer les opérations de traitement.

➢ Mieux gérer l'activité

Avec le temps et le développement de l'activité de la Société, le volume de données augmente et nécessite de mobiliser de plus en plus de moyens humains et techniques (espace de stockage, logiciels adaptés, etc.) pour les gérer, les mettre à jour, et en assurer la sécurité.

Le principe de « minimisation » des données (« *Je ne collecte que les données dont j'ai vraiment besoin* ») et l'obligation de tenir à jour la liste des fichiers permettent de faire le point sur les données que la Société collecte et d'identifier ses besoins réels.

Les données doivent être pertinentes par rapport à l'objectif pour lequel la Société collecte les données.

Appliquer ces principes permet donc d'optimiser les investissements.

➢ Améliorer la sécurité des données

L'actualité témoigne d'un nombre de plus en plus important de failles de sécurité et d'attaques informatiques. Ces dernières peuvent avoir des conséquences désastreuses sur l'activité des entreprises. Le niveau de sécurité de l'entreprise dans sa globalité se pose en préalable à la sécurité des données. Les failles de sécurité ont également des conséquences pour ceux qui ont confié des données personnelles.

Les données personnelles doivent faire l'objet de mesures de sécurité particulières, informatiques et physiques, afin de minimiser les risques de pertes de données ou de piratage.

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données traitées et des risques qui pèsent sur les personnes en cas d'incident.

Différentes actions peuvent être mises en place :

- mises à jour des antivirus et logiciels,
- changement régulier des mots de passe et utilisation de mots de passe complexes,
- profils informatiques distincts au sein des applications
- chiffrement des données dans certaines situations
- procédure de sauvegarde et de récupération des données en cas d'incident
- sécurisation des locaux.

➢ Restreindre les transferts de données en dehors de l'Union européenne

Avant de transférer des données vers des pays hors Union européenne, il convient de vérifier que ces pays disposent d'une législation de protection des données et si elle est reconnue adéquate par la Commission européenne.

Il faut alors encadrer juridiquement ces transferts pour assurer la protection des données à l'étranger.

Une carte du monde présentant les législations de protection des données est disponible sur le site de la CNIL.

3. RESPONSABILITE DE MISE EN OEUVRE DE LA PROTECTION DES DONNEES

La Société a nommé **Madame Corinne de CAUMONT en qualité de « Délégué à la protection des données » (« DPO »).**

Le DPO est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que les collaborateurs de la Société ;
- de contrôler le respect par la Société du règlement et du droit national en matière de protection des données ;
- de conseiller la Société sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Pour assurer ses missions, le DPO doit notamment :

- s'informer sur le contenu des nouvelles obligations ;
- sensibiliser les décideurs sur l'impact de ces nouvelles règles ;
- réaliser l'inventaire des traitements de données de la Société ;
- concevoir des actions de sensibilisation ;
- piloter la conformité en continu.

Le DPO a délégué la réalisation effective de ces missions au Cabinet JORNET FINANCE CONSULTING, représenté par M. Michel JORNET, dans le cadre d'un contrat établi ou modifié à cet effet.

Le DPO reste responsable du respect des dispositions de la RGPD, notamment vis-à-vis des tiers et des autorités,

4. IDENTIFICATION DES DONNEES PERSONNELLES ET DE LEUR TRAITEMENT

La Société établit un **Registre des traitements des données personnelles**. A cet effet, la Société doit identifier les activités qui nécessitent la collecte et le traitement de données.

Ce registre regroupe les fiches recensant pour chaque activité :

- l'objectif poursuivi (la finalité - exemple : la fidélisation client) ;
- les catégories de données utilisées (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- l'accès aux données (le destinataire - exemple : service chargé du recrutement, service informatique, direction, prestataires, partenaires, hébergeurs) ;
- la durée de conservation de ces données (durée durant laquelle les données sont utiles d'un point de vue opérationnel, et durée de conservation en archive).

Le registre est placé sous la responsabilité du DPO.

5. RELATIONS AVEC LES SOUS-TRAITANTS

Le règlement européen consacre une logique de responsabilisation de tous les acteurs impliqués dans le traitement des données personnelles, dès lors qu'elles concernent des résidents européens, que ces acteurs soient ou non établis au sein de l'Union européenne. Il impose des obligations spécifiques aux sous-traitants qui doivent notamment aider les responsables de traitement dans leur démarche permanente de mise en conformité de leurs traitements.

Le Sous-Traitant est la personne physique ou morale qui traite des données personnelles pour le compte de la Société (« Responsable de traitement »), dans le cadre d'un service ou d'une prestation.

Le Sous-Traitant est tenu de respecter des obligations spécifiques en matière de sécurité, de confidentialité et de documentation de son activité.

Il doit offrir au Responsable de traitement des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée

Il doit prendre en compte l'objectif de protection des données personnelles et de la vie privée dès la conception de leur service (principe du « *privacy by design* ») ou de leur produit, et ils doivent mettre en place des mesures permettant de garantir une protection optimale des données.

Le Sous-Traitant doit :

- établir avec le Responsable du Traitement un contrat ou un autre acte juridique précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du RGPD (cf. Annexe) ;
- recenser par écrit les instructions du Responsable du Traitement concernant les traitements de ses données afin de prouver qu'il agit sur instruction documentée de celui-ci ;
- demander l'autorisation écrite du Responsable du Traitement si, en tant que sous-traitant, il fait lui-même appel à un sous-traitant ;

- mettre à la disposition du Responsable du Traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et pour permettre la réalisation d'audits (sur la base, par exemple, du référentiel de la CNIL pour la délivrance de labels en matière de procédure d'audit) ;
- tenir un registre qui recense ses clients et décrit les traitements qu'il effectue pour leur compte.

6. RESPECT DES DROITS DES PERSONNES

6.1. L'INFORMATION

La personne concernée par un traitement de données doit recevoir une information délivrée de façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

À chaque fois que la Société collecte des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information à destination de la personne dont la Société recueille les données :

- pourquoi la Société collecte les données (« la finalité ») ;
- ce qui autorise la Société à traiter ces données (le « fondement Juridique ») : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à la Société, de son « intérêt légitime ») ;
- qui a accès aux données (les services internes compétents, un prestataire, etc.) ;
- combien de temps la Société les conserve (exemple : « 5 ans après la fin de la relation contractuelle ») ;
- les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (par exemple, un courrier ou un e-mail adressé au DPO) ;
- si la Société transfère des données hors de l'Union européenne (préciser le pays et l'encadrement juridique qui maintient le niveau de protection des données).

Pour éviter des mentions trop longues au niveau d'un formulaire, il est possible de donner un premier niveau d'information en fin de formulaire et de renvoyer à la **Politique de protection des données personnelles** disponible sur le site internet de la Société (texte en Annexe).

L'information est préalable à la collecte des données

Le support de cette information varie en fonction des caractéristiques du fichier : panneau d'information pour une vidéosurveillance, mention d'information sur un formulaire, lecture de cette information en cas de recueil de données par téléphone. (cf. exemples en Annexe).

6.2. LE RECUEIL DU CONSENTEMENT ET LE DROIT D'OPPOSITION

Le consentement est une démarche active de l'utilisateur, explicite et de préférence écrite, qui doit être libre, spécifique, et informée.

Un consentement spécifique de la personne concernée est notamment requis :

- en cas de collecte de données sensibles,
- de réutilisation des données à d'autres fins,
- d'utilisation de cookies pour certaines finalités,
- d'utilisation des données à des fins de prospection commerciale par voie électronique.

Le consentement est préalable à la collecte des données.

Les personnes doivent pouvoir s'opposer à la réutilisation de leurs coordonnées à des fins de sollicitations, notamment commerciales, lors d'une commande ou de la signature d'un contrat. Une case à cocher (non cochée par défaut) doit leur permettre d'exprimer leur choix directement sur le formulaire à remplir. La simple mention de l'existence de ce droit dans les conditions générales n'est pas suffisante (cf. exemple en Annexe).

Toute personne a le droit de s'opposer, pour des motifs légitimes, au traitement de ses données, sauf si celui-ci répond à une obligation légale (exemple : MIF ou LCB-FT).

Il est rappelé que le KYC MIF répond à une obligation légale et qu'en conséquence, le client ne peut s'y opposer.

6.3. L'EXERCICE DES DROITS D'ACCES ET DE RECTIFICATION

Les personnes dont la Société traite les données (clients, collaborateurs, prestataires, etc.) ont des droits sur les données qui les concernent : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement.

Ainsi, toute personne peut :

- accéder à l'ensemble des informations la concernant ;
- connaître l'origine des informations le concernant ;
- accéder aux informations sur lesquelles le responsable du fichier s'est fondé pour prendre une décision le concernant ;
- en obtenir la copie (des frais n'excédant pas le coût de la reproduction peuvent être demandés) ;
- exiger que ses données soient, selon les cas, rectifiées, complétées, mises à jour ou supprimées.

Le droit d'accès doit s'exercer dans le respect du droit des tiers.

La Société doit leur donner les moyens d'exercer effectivement leurs droits.

Le droit d'accès peut s'exercer :

- par écrit : courrier postal, accompagné d'une copie d'une pièce d'identité. Idéalement, en recommandé avec accusé de réception ;
- sur place : avec présentation d'une pièce d'identité. Il est possible de se faire accompagner par la personne de son choix. La consultation doit durer suffisamment longtemps pour prendre note commodément et complètement. Il est possible de demander une copie des données.

A cet effet, la Politique de protection des données personnelles mentionne sur le site internet de la Société, une adresse courrier et une adresse de messagerie dédiée, donnant la possibilité aux personnes concernées d'exercer leurs droits.

Toute demande est traitée par le DPO qui est en charge :

- d'enregistrer la demande dans un registre ;
- de donner toutes instructions pour apporter une solution conforme à la demande de client (recueil des données concernées, demande de rectification ou d'effacement auprès du collaborateur ou du Prestaitre concerné…) ;
- d'apporter à l'auteur de la demande la réponse adéquate ;
- de s'assurer que l'identification et **le traitement de la demande ait lieu dans un délai d'un mois maximum**.

En cas de refus de la demande d'accès, le DPO doit motiver sa décision et informer le demandeur des voies et délais de recours permettant de la contester.

Lorsque le DPO constate que la Société ne dispose d'aucune donnée sur la personne qui exerce son droit d'accès (exemple : les données ont été supprimées), il doit néanmoins répondre au demandeur dans le délai d'un mois.

7. INFORMATION DE LA CNIL

Si la Société subit une violation de données (des données personnelles ont été, de manière accidentelle ou illicite, détruites, perdues, altérées, divulguées ou il a été constaté un accès non autorisé à des données), **le DPO doit la signaler à la CNIL dans les 72 heures si cette violation est susceptible de représenter un risque pour les droits et libertés des personnes concernées.**

Cette notification s'effectue en ligne sur le site internet de la CNIL[1].

Si ces risques sont élevés pour les personnes concernées par ces données, le DPO doit les en informer.

[1] Lien : https://notifications.cnil.fr/notifications/index