Outils juridiques

Le Règlement général sur la protection des données personnelles. « RGPD »

Le Règlement Général sur la Protection des Données du 27 avril 2016 (RGPD)[1] est un acte législatif émanant de l'Union Européenne, relatif à la sécurité des réseaux informatiques et au traitement des données. Il entrera en application dans toutes les entreprises, associations, administrations et collectivités locales à compter du 25 mai 2018.

Auparavant, nous étions sous le coup de la loi « informatique et liberté »[2] qui reposait sur une logique de « formalités préalables » sous la forme de déclarations et autres demandes d' autorisations auprès de la CNIL .

Avec le RGPD, nous passons aujourd'hui à un système « d'autorégulation » dans lequel les SIAE devront être en mesure de prouver à tout moment leur respect des règles.

l' enjeu est de taille, car en contrepartie de la réduction du contrôle en amont, la CNIL voit ses pouvoirs de contrôle et de sanction renforcés par la possibilité d'infliger des amendes allant dans les cas les plus graves jusqu'à 4% du chiffre d'affaires.

«Rassurez vous!», avant d'en arriver là, la CNIL pourra prononcer un rappel à l'ordre ou un avertissement, vous adresser une mise en demeure , prononcer une injonction assortie d'une astreinte, limiter temporairement ou définitivement un traitement de données ou encore suspendre les flux des données….Il est donc essentiel que vous vous mettiez en conformité….

L'objectif principal du RGPD est d'assurer la protection des données à caractère personnel des salariés, candidats à un emploi, consultants extérieurs, clients, prospects, fournisseurs, partenaires commerciaux, patients, de mieux protéger les citoyens.

SI VOUS UTILISEZ MING, NOUS AVONS FORMALISE UN CONTRAT DE SOUS TRAITANCE (OBLIGATOIRE) REPRENANT LES OBLIGATIONS RESPECTIVES DE LA SIAE ET DE L'URIAE EN MATIERE DE TRAITEMENT DES DONNEES PERSONNELLES.

EN RESPECTANT LES TERMES DE CE CONTRAT, VOUS SEREZ ASSURES QUE LE TRAITEMENT DES DONNEES RELATIVES AU SUIVI SOCIO PROFESSIONNEL DE VOS SALARIES EN INSERTION EST CONFORME AU RGDP.

CE CONTRAT SERA ENVOYÉ AUX UTILISATEURS DE MING DANS UNE DIZAINE DE JOURS.

---

[1] R*ÈGLEMENT (UE) n° 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 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, et abrogeant la directive 95/46/CE*

[2] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

I/ QUELLES DONNEES PROTEGER?

A/ LES DONNES PERSONNELLES

« *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* »,

Vous compilez beaucoup d'informations pour assurer la rémunération, les déclarations sociales obligatoires, la tenue du registre unique du personnel, la gestion administrative (ex : type de permis de conduire détenu, CMU, RSA; l'organisation du travail (ex : photographie facultative de l'employé pour les annuaires internes et organigrammes) ou encore l'action et le suivi social menées par la structure d'insertion…**Toutes ces informations constituent des « données à caractère personnel » et doivent être PROTEGEES, À FORTIORI S'IL S'AGIT DE DONNEES SENSIBLES.**

B/ LES DONNEES SENSIBLES

Les données sensibles sont celles qui font apparaître, directement ou indirectement, **les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci.**

Par principe, la collecte et le traitement de ces données sont interdits.

Cependant, dans la mesure où la finalité du traitement l'exige (ex suivi socio professionnel), ne sont pas soumis à cette interdiction les traitements pour lesquels la personne concernée **a donné son consentement exprès .**

Autres données à risque :

- données génétiques,
- **données relatives aux infractions pénales, aux condamnation etc.,**
- **données comportant des appréciations sur les difficultés sociales des personnes,**
- données biométriques,
- données comprenant le numéro NIR (sécurité sociale)

ATTENTION **POUR LA COLLECTE DES DONNEES SENSIBLES** Vous devez , recueillir l'accord éclairé, exprès et écrit des salariés concernés. CF ANNEXE 3

B/ CE QUI PERMET D'IDENTIFIER UN INDIVIDU

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, physiologique, génétique, psychique, 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, ADN) ;
- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, et militant dans telle association).

Vous devez donc protéger toutes les informations qui pourraient permettre d'identifier directement ou indirectement les personnes et notamment:

> Noms, prénoms ;
> Adresses ;
> Numéros de téléphone ;
> Numéros de permis de conduire ;
> Numéros de compte bancaire ;
> Numéros de sécurité sociale ;
> Situations familiales ;
> Etats de santé : maladie, handicap, grossesse, etc... ;
> Photocopies ou scans de cartes d'identité, permis de conduire, cartes vitales, etc...

> Justificatifs de domicile ;
> Revenus ;
> Identifiants, codes d'accès, mots de passe ;
> Adresses IP ;
> Données biométriques ;
> Données de géolocalisation ;
> Enregistrements vidéo de caméras ;
> Parcours professionnels ;
> Etc...

II/ DUREE DE CONSERVATION DES DONNEES?

Les données personnelles relatives aux salariés ne peuvent être conservés que pour la durée nécessaire :

> A l'exécution de leur contrat de travail ;
> Au respect d'obligations légales ;
> A l'accomplissement de l'objectif du traitement.

Exemples :

> Durée de conservation de 2 ans maximum après le dernier contact pour les données recueillies lors d'un recrutement non abouti.

> Durée de conservation de 5 ans maximum pour les données relatives à la paie des salariés.

Attention, à compter du 25 mai 2018, toute faille de sécurité dans le traitement des données personnelles des salariés doit être signalée à la CNIL et au(x) salarié(s) concerné(s) dans les 72 heures.

III/ COMMENT SE METTRE EN CONFORMITE AVEC LE RGPD?

1ère étape : DESIGNER LA PERSONNE RESSOURCE

A/ SIAE de moins de 250 salariés: Désigner un « RESPONSABLE DE TRAITEMENT »

Le responsable du traitement est « la personne physique ou morale, qui seul ou conjointement avec d'autres détermine la finalité et les moyens du traitement des données à caractère personnel».

Son rôle est :

•De suivre la mise en œuvre de la politique de sécurité informatique ;

•Maîtriser la protection des données personnelles ;

• Connaître le contenu du RGDP ;

•S'entretenir avec les principaux acteurs de la structure

- Etablir et suivre l'avancement du calendrier de mise en conformité ;
- Fixer les tâches et actions à réaliser par les intervenants : service informatique, service RH et paies, service comptabilité, service , clients, service fournisseurs, SAV, etc...

B/ **SIAE de 250 salariés et plus : Désigner un « DATA PROTECTION OFFICER» DPO**

Son rôle est :

- D'assurer une gestion cohérente et conforme du traitement des données personnelles
- De veiller à la compréhension et à la réussite de la mise en conformité ;
- Connaître le contenu du règlement européen ;
- Maîtriser l'informatique et la cybersécurité ;
- Informer et conseiller le dirigeant ;
- Apporter son expertise technique et juridique sur les mesures de sécurité à mettre en place ;
- Contrôler la bonne application de la gestion des données personnelles ;
- Etre le contact entre l'entreprise et la CNIL ;

- Etre le contact entre l'entreprise et les personnes concernées par le traitement des données : salariés, clients, patients, etc... ;
- Etre consulté pour toute décision relative à des données personnelles ;
- Etre alerté et consulté en cas de fuite de données personnelles ;
- Réaliser les analyses d'impact, déterminer les actions correctives et en suivre la bonne exécution.

2ème étape : RECENSER TOUS LES TRAITEMENTS DE DONNEES PERSONNELLES

Le registre listant vos traitements de données vous permettra d'avoir une vision d'ensemble.

- **Identifiez les activités de votre structure qui nécessitent la collecte et le traitement de données** (exemples : recrutement, gestion de la paye, suivi socio professionnel, formation, gestion des badges et des accès,, gestion des clients prospects, etc.).
- **Appuyez-vous sur le modèle de registre proposé par la CNIL (cf annexe 2).**

Dans votre registre, créez une fiche pour chaque activité recensée, en précisant :

- **l'objectif poursuivi** (la finalité - exemple : suivi socio professionnel) ;
- **les catégories de données utilisées** (exemple pour la paie : nom, prénom, date de naissance, salaire, etc.) ;
- **qui a accès aux données**(exemple: direction, RH, CIP, encadrant technique etc…)
- **la durée de conservation de ces données**

Le registre est placé sous la responsabilité du dirigeant de l'entreprise. Pour avoir un registre exhaustif et à jour, il faut en discuter et être en contact avec toutes les personnes de l'entreprise susceptibles de traiter des données personnelles.

Vous n'avez pas en revanche à mentionner au registre les traitements purement occasionnels (exemple : fichier constitué pour une opération événementielle ponctuelle .

En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données

L'établissement de ce registre des traitements est obligatoire dans les entreprises de plus de 250 salariés. MAIS AUSSI

- **Q**uel que soit le nombre de salariés, lorsqu'un traitement de données personnelles est **non occasionnel** ou porte sur des données dites « sensibles »
- Quel que soit le nombre de salariés, lorsqu'un traitement est susceptible de comporter un risque de violation des droits et libertés individuelles des personnes concernées par le traitement ;
- Quel que soit le nombre de salariés, lorsqu'un traitement est relatif à des condamnations pénales et des infractions.

A cet égard, seule une STRUCTURE ne traitant pas de **données à caractère personnel** de manière "**occasionnelle**" peut s'affranchir de l'obligation de rédiger un **registre des traitements**.

En pratique, cela signifie que la SIAE en question ne doit pas posséder de fichier relatif aux données de ses salariés, de ses prospects et/ou de ses clients (ou à tout le moins aucun fichier ne mentionnant de données à caractère personnel de ces personnes).

Dans toutes les autres hypothèses (ce qui représente 99% des entreprises), la **réalisation d'un registre des traitements est obligatoir**e.

3ème étape : DETERMINER LES ACTIONS A MENER

Il s'agit de lister, à partir du registre des traitements, l'ensemble des actions à mener et d'établir un plan d'action en fixant des dates limites.

Nous vous conseillons de présenter votre plan d'actions par niveaux de risques que présentent les traitements sur les droits et libertés des personnes concernées :

Risques élevés ? Risques moyens ? Risques faibles? Un peu comme vous le faites dans votre déclaration unique des risques professionnels…..

Le responsable de traitement ou le DPO doit déterminer et mettre en place les mesures techniques et organisationnelles nécessaires pour assurer la confidentialité des données personnelles et éviter tout risque de fuite, divulgation, ou violation.

Exemples d'actions de prévention pouvant être mises en œuvre :

> Etablissement d'une charte informatique et libertés

> Sécurité physique des serveurs informatiques ;
> Mise à jour des logiciels de protection ;
> Mise en place de pare-feu ;

> Mise en place d'une procédure en cas de violation des données, et notamment l'envoi d'un formulaire à la CNIL. Pour télécharger le formulaire, cliquez ici

> Gestion des modifications des données collectées ;

> Sensibilisation des salariés à la sécurité des données personnelles ;

> Formation du personnel ;

> Création de documents d'information à destination des salariés ;

> Définition précise des rôles des personnes en charge des RH et des données auxquelles chacune a accès ; cloisonnement informatique de leurs accès ;

> Etablissement de clauses contractuelles pour la sous-traitance notamment ;

> Cryptage de données ;

> Etc...

Outils juridiques

Vous pouvez télécharger le guide de la CNIL sur les sécurisation des données personnelles en cliquant sur ce lien

4ème étape : INFORMER LES SALARIES

Vous devez également informer vos salariés, de manière claire et précise, sur le traitement de leurs données personnelles. Vous pouvez le faire via le règlement intérieur de l'entreprise, une note de service, le contrat de travail du salarié, ou encore le livret d'accueil remis à chaque nouveau salarié.

Cette information aux salariés doit mentionner :

> Les modalités du traitement des données personnelles et leurs objectifs ;
> Le rappel des droits du salarié sur ses données personnelles ;
> La possibilité de transférer les données personnelles du salarié à une autre entité juridique, si l'entreprise appartient à un groupe.

5ème étape : TENIR A JOUR LE DOSSIER RELATIF AU TRAITEMENT DES DONNEES.

Nous vous conseillons d'établir et de tenir à jour un dossier regroupant l'ensemble des documents relatif au traitement des données afin de pouvoir justifier de votre mise en conformité en cas de contrôle.

Vous devrez en effet être en mesure, à tout moment, de prouver votre mise en conformité. Ce dossier devra contenir :

> Le registre des traitements ;

> Le plan d'actions ;

> Les documents mis en place et utilisés :

> Les modalités d'informations des personnes : mentions d'informations, modèles de recueil du consentement, procédure pour l'exercice des droits, etc... ;

> Les modalités selon lesquelles les sous-traitants s'engagent à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel :

Outils juridiques

ANNEXE 1
NOTE DE SERVICE
INFORMATION AU PERSONNEL
Le traitement des données personnelles ou RGPD

Le RGPD (Règlement général sur la protection des données) du 27 avril 2016 est un acte législatif européen relatif à la sécurité sur les réseaux informatiques, applicable à compter du l **25 Mai 2018**.

Son objectif est d'assurer la protection des données à caractère personnel des citoyens européens : salariés, candidats à un emploi, clients, prospects, fournisseurs, partenaires commerciaux, patients, etc...

Quelles sont les données personnelles protégées ?

Il s'agit de l'ensemble des données personnelles permettant d'identifier de manière directe ou indirecte une personne et figurant dans des fichiers numériques :

- Noms, prénoms ;
- Adresses ;
- Numéros de téléphone ;
- Numéros de permis de conduire ;
- Numéros de compte bancaire ;
- Numéros de sécurité sociale ;
- Situations familiales ;
- Photocopies ou scans de cartes d'identité, carte vitale, permis de conduire, etc...
- Justificatifs de domicile ;
- Revenus ;
- Identifiants, codes d'accès, mots de passe ;
- Parcours professionnels ;
- Etc...

Ces données sont conservées au sein de La structure en toute sécurité et leurs traitements sont consignés dans le registre des traitements des données personnelles de l'entreprise.

Quels sont vos droits en tant que salarié ?

Que ce soit dans le cadre de votre recrutement, de votre embauche, de l'établissement de vos fiches de paies, de la tenue de vos entretiens professionnels, etc..., nous sommes amenés à traiter vos données personnelles, et ce de manière constante et régulière : identité, adresse, numéro de téléphone, numéro de sécurité sociale, état de santé, situation familiale, RIB, etc...

- **Votre droit à l'information :**

Vous êtes informé des raisons pour lesquelles nous collectons vos données personnelles, des destinataires de vos données, et de la durée pendant laquelle nous conservons vos données à savoir :

(Indiquer précisément les motifs justifiant la collecte, la manière dont sont traitées les données ainsi que les durées de conservation des données).

Dans notre structure,, la personne en charge du traitement des données personnelles est ..... *(Indiquer les nom, prénom, qualité et coordonnées du responsable du traitement)*.

Si l'entreprise appartient à un groupe : Notre entreprise appartenant au groupe ....., vos données personnelles sont susceptibles d'être transférées à un autre établissement ou une autre entreprise du groupe.

- **Votre droit d'accès :**

Vous avez accès, à tout moment, à l'ensemble de vos données personnelles. Vous pouvez demander à les consulter.

- **Votre droit de rectification :**

Vous pouvez, à tout moment, demander à ce que vos données personnelles éventuellement inexactes ou incomplètes soient corrigées ou complétées.

- **Votre droit à l'oubli :**

Vos données personnelles sont conservées pendant une durée déterminée et limitée. Au-delà de cette durée, vos données sont effacées.

- **Votre droit à la limitation :**

La collecte de vos données personnelles répond nécessairement à un ou plusieurs motifs légitimes mentionnés dans le registre de traitement des données de l'entreprise.

- **Votre droit d'opposition et à la non-utilisation :**

Vous pouvez demander à ce que certaines de vos données personnelles ne soient pas collectées et / ou à ce que certaines de vos données collectées ne soient pas utilisées, à condition toutefois que cela n'ait pas d'incidence sur le bon fonctionnement de l'entreprise.

- **Votre droit à la portabilité :**

Vous pouvez, à tout moment, obtenir vos données personnelles collectées et les réutiliser pour les transmettre à un tiers (réseau social, fournisseur d'accès internet, site de streaming, autre employeur, etc...).

La collecte et le traitement de certaines de vos données personnelles nécessite votre consentement, que vous pouvez retirer à tout moment. Par exemple : les photos de vous ou sur lesquelles vous apparaissez.

Dès lors que vous nous présenterez une demande, nous vous répondrons dans le délai d'un mois à compter de la réception de celle-ci, à condition toutefois que l'exécution de votre contrat de travail ne soit pas remise en question.

Quelles sont vos obligations en tant que salarié ?

En tant que salarié, vous avez des droits mais aussi des obligations.

La protection des données personnelles concernant l'ensemble des citoyens européens, elle s'applique également aux : à préciser clients, prospects, fournisseurs, consultants, patients *(à adapter selon les spécificités de l'entreprise)* de notre entreprise dont vous êtes ou pouvez être amené à traiter des données personnelles dans le cadre de vos fonctions.

Le registre des traitements des données personnelles de l'entreprise mentionne l'identité et la qualité de l'ensemble de nos salariés amenés à traiter des données personnelles (services RH, comptabilité, informatique, clients, fournisseurs, etc...).

Chacun est responsable dans ce domaine.

Vous n'êtes autorisé à traiter que les données personnelles relevant de vos fonctions et engagez votre responsabilité personnelle en cas d'écart.

Pour plus d'informations sur vos droits et obligations en la matière, n'hésitez pas à vous rapprocher du responsable du traitement *et / ou* du DPO.

Fait à .....

Le.....

.....

Le Directeur

Outils juridiques

ANNEXE 2
MODELE DE REGISTRE

Identification du traitement				Acteurs	
Nom / sigle	N° / REF	Date de création	Dernière mise à jour	Responsable du traitement	Fi

Outils juridiques

ANNEXE 3

Acceptation exprès de collecte de données sensibles par le salarié en insertion.

Les données sensibles concernent par exemple, les origines ethniques des personnes, les appréciations sur les difficultés sociales auxquelles elles sont exposées, les problèmes de santé qu'elles rencontrent, ou encore aux condamnations prononcées à leur encontre.

Je soussigné (e) Mr /Mme x , autorise l'association/ L'entreprise X, agréée (EI, ACI, AI , ETTI) à collecter des données relatives à ma situation personnelle que je voudrais bien leur communiquer, dans la mesure où ces informations sont effectivement nécessaires au déroulement et à la pertinence de l' accompagnement socio professionnel mis en oeuvre.

J'ai connaissance que ces données sensibles seront conservées pendant toute la durée du contrat de travail qui me lie avec l'entreprise / association puis anonymisées dès mon départ de la structure.

Je pourrai revenir sur la présente autorisation et retirer mon consentement à tout moment.

Fait à XXX
Le

Le salarié

Outils juridiques

ANNEXE 4

Clause de confidentialité à insérer dans les contrat de travail des salariés ayant à traiter des données personnelles

Je soussigné(e) Monsieur/Madame ……., exerçant les fonctions de ……. au sein de la société/ l'association …, étant à ce titre amené/e à accéder à des données à caractère personnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ainsi qu'aux articles 32 à 35 du règlement général sur la protection des données du 27 avril 2016, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles ne soient communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions ;
- ne divulguer ces données qu'aux personnes dûment autorisées, en raison de leurs fonctions, à en recevoir communication, qu'il s'agisse de personnes privées, publiques, physiques ou morales ;
- ne faire aucune copie de ces données sauf à ce que cela soit nécessaire à l'exécution de mes fonctions ;
- prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données ;
- prendre toutes précautions conformes aux usages et à l'état de l'art pour préserver la sécurité physique et logique de ces données ;
- m'assurer, dans la limite de mes attributions, que seuls des moyens de communication sécurisés seront utilisés pour transférer ces données ;
- en cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après la cessation de mes fonctions, quelle qu'en soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.
J'ai été informé(e) que toute violation du présent engagement m'expose à des sanctions disciplinaires et pénales conformément à la réglementation en vigueur, notamment au regard des articles 226-16 à 226-24 du code pénal.

Fait à …, le …, en deux exemplaires
Signature