Dossier pratique

Droit du travail

Mettez-vous en conformité avec le RGPD

Editions Legiest

909 Avenue des Platanes
Immeuble la Salicorne – 34070 Lattes
Tel : 04 99 61 65 48
Mail : contact@legiest.fr

Employeur : Respectez le règlement général sur la protection des données (RGPD)

Depuis le 25 mai 2018, les entreprises doivent se mettre en conformité avec le nouveau règlement européen 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 » (RGPD)

L'employeur est amené à traiter, au quotidien, de nombreuses données à caractère personnel pour la gestion de son personnel : coordonnées bancaires et numéro de sécurité sociale pour la paie et les déclarations sociales obligatoires, tenue du registre du personnel, mutuelles d'entreprise, annuaire comportant des photographies des salariés…

Les dispositifs de contrôle de l'activité des salariés mis en œuvre dans l'entreprise peuvent constituer également, des traitements de données à caractère personnel.

I. QUI EST CONCERNÉ PAR LE RGPD ?

Tout organisme quelle que soient sa taille, son pays d'implantation et son activité, peut être concernée. En effet, le 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 ;

• que son activité cible directement des résidents européens. Par exemple, une société établie en France, qui exporte l'ensemble de ses produits en dehors de l'Union européenne doit respecter le RGPD. De même, une société établie en dehors de l'Union européenne, proposant un site de e-commerce en français livrant des produits en France doit respecter le RGPD.

Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes

- Un employeur est donc considéré comme un « Responsable de traitement », au sens de l'article 4 du règlement européen.

II. QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable ». Vos salariés, vos fournisseurs ainsi que les clients sont donc concernés.

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, abonnée à tel magazine et militant dans telle association).

- Toutes les données personnelles de vos salariés sont concernées et devront être recensées, c'est-à-dire les éléments les plus communs (identité, photo, adresse mail, numéro de téléphone..), gestion de la paie mais aussi des informations portant sur les caractéristiques physiques, culturelles, sociales, jusqu'à des éléments comportementaux digitaux comme les adresses IP, les identifiants et mots de passe ou les habitudes de navigation Internet.

III. QU'EST-CE QU'UN TRAITEMENT DE DONNÉES PERSONNELLES ?

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).

Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous 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 votre activité professionnelle.

IV. LES ACTIONS A METTRE EN PLACE POUR VOUS METTRE EN CONFORMITE

1. Recensez vos données dans un registre de données

Le chef d'entreprise ou le responsable du traitement doit tenir un registre sous forme écrite qui recense l'ensemble des traitements de données personnelles récoltées par votre entreprise concernant vos salariés, candidats à un poste, clients ou fournisseurs.

Toutes les données personnelles de vos salariés sont concernées et devront être recensées, c'est-à-dire les éléments les plus communs (identité, photo, adresse mail, numéro de téléphone, numéro de sécurité sociale...), gestion de la paie mais aussi des informations portant sur les caractéristiques physiques, culturelles, sociales, jusqu'à des éléments comportementaux digitaux comme les adresses IP, les identifiants et mots de passe ou les habitudes de navigation Internet.

Le chef d'entreprise doit pouvoir prouver à tout moment qu'il est en conformité.

Le registre peut être demandé en cas de contrôle ou en cas de litige devant un tribunal.

Ce registre comporte toutes les informations suivantes:

a) le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;

b) les finalités du traitement;

c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;

d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;

e) 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).

f) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts hors UE, les documents attestant de l'existence de garanties appropriées;

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 comme l'inauguration d'une boutique).En constituant votre registre, vous aurez une vision d'ensemble sur vos traitements de données.

2. Faites le tri dans vos données

Pour chaque fiche de registre créée, vérifiez :
• que les données que vous traitez sont nécessaires à vos activités (par exemple, il n'est pas utile de savoir si vos salariés ont des enfants, si vous n'offrez aucun service ou rémunération attachée à cette caractéristique) ;
• que vous ne traitez aucune donnée dite « sensible » ou, si c'est le cas, que vous avez bien le droit de les traiter ;
• que seules les personnes habilitées ont accès aux données dont elles ont besoin ;
• que vous ne conservez pas vos données au-delà de ce qui est nécessaire.

3. Respectez les droits des salariés

➢ Informez les salariés

À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.
Vérifiez que l'information comporte notamment les éléments suivants :
• pourquoi vous collectez les données ;
• ce qui vous autorise à traiter ces données ;
• qui a accès aux données ;
• combien de temps vous les conservez ;
• les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits (via leur espace personnel sur votre site internet, par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;
• si vous transférez des données hors de l'Union européenne, précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données.

- **Permettez aux salariés d'exercer facilement leurs droits**

Les personnes dont vous traitez les données et notamment les salariés ont des droits sur leurs données, qui sont renforcés par le RGPD : droit d'accès, de rectification, d'opposition, d'effacement, à la portabilité et à la limitation du traitement. Vous devez leur donner les moyens d'exercer effectivement leurs droits en mettant en place un processus interne permettant de garantir l'identification et le traitement des demandes dans des délais courts (1 mois au maximum).

4. Sécurisez les données

Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident. Différentes actions doivent être mises en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder.

A savoir : 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.

Lorsque votre 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 vos traitements de données répondent à au moins 2 de ces 9 critères, vous devez, a priori, conduire une analyse d'impact sur la protection des données avant de commencer les opérations de traitement.
En complément de l'établissement du registre et de la description du traitement, cette analyse de l'impact sur la vie privée vous permettra d'identifier les risques associés à ces données personnelles.

Lorsque vous transférez des données en dehors de l'Union européenne
Vérifiez si le pays hors Union européenne vers lequel vous transférez les données dispose d'une législation de protection des données et si elle est reconnue adéquate par la Commission européenne. Une carte du monde présentant les législations de protection des données est à votre disposition sur le site de la CNIL. Sinon, vous devrez encadrer juridiquement vos transferts pour assurer la protection des données à l'étranger.