Offices de Tourisme de France
FÉDÉRATION NATIONALE

FICHE SOCIALE N°32
Avril 2018

Ius Laboris FRANCE
CAPSTAN AVOCATS

Le Règlement Général sur la Protection des Données (RGPD)

Le règlement général sur la protection des données (RGPD), qui prendra effet le 25 mai 2018, fournit un cadre de conformité modernisé, fondé sur la responsabilité, en matière de protection des données.

Il convient donc de préciser un peu les contours de ce règlement.

1 – Le cadre législatif et réglementaire actuel en matière de traitement des données personnelles

En France, la réglementation en matière de traitement des données personnelles des salariés est issue de différents textes européens et nationaux (directive européenne 95/46/CE, loi informatique et libertés de 1978, Code du travail ; Code pénal).

De manière générale, il convient de rappeler que le cadre législatif et réglementaire actuel repose sur des obligations de déclaration auprès de la CNIL qui sont différentes selon le type de données personnelles traitées :

- Dispense de déclaration (ex : gestion de paie) ;
- Déclaration simplifiée (ex : géolocalisation des véhicules, système de gestion du personnel) ;
- Déclaration normale (sauf en cas de désignation d'un Correspondant Informatique et Libertés) ;
- Demande d'autorisation pour le traitement des données « sensibles » (ex : origine, opinions, vie sexuelle…)

Plus spécifiquement en droit social, le traitement des données personnelles est soumis au principe posé par l'article L 1121-1 du Code du travail qui dispose que : « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ».

Dans ce cadre, tout traitement de données personnelles des salariés doit faire l'objet d'une consultation préalable des institutions représentatives du personnel en cas de projet important modifiant les conditions de travail et d'une information préalable des salariés dès lors qu'ils constituent un dispositif de contrôle sur leur activité.

Ce cadre réglementaire et législatif national avait été récemment renforcé par la loi du 7 octobre 2016 « pour une République numérique » qui prévoyait notamment une nouvelle procédure CNIL en cas de non-respect des obligations de la Loi informatique et libertés.

2 – Le nouveau règlement européen applicable à compter du 25 mai 2018

A compter du 25 mai 2018, la directive 95/46/CE sera abrogée par le nouveau Règlement générale de protection des données qui a notamment pour objectif d'harmoniser toutes les règlementations européennes en matière de traitement des données personnelles.

➢ Champ d'application du RGPD

Le RGPD s'applique :

- Aux responsables de traitement établis sur le territoire de l'UE ;

Fédération Nationale des Offices de Tourisme et Syndicats d'Initiative
79/81 rue de Clichy • 75009 Paris
Tél. : 01 44 11 10 30 • Fax. : 01 45 55 99 50
www.offices-de-tourisme-de-france.org
www.tourisme.fr

- A tout traitement de données personnelles relatives à des personnes qui se trouvent sur le territoire de l'UE ;
- Aux sous-traitants établis ou non dans l'UE.

Pour contrôler la mise en conformité du RGPD, la CNIL devient la seule autorité compétente sur le territoire français.

En matière de relations de travail, l'article 88 du RGPD dispose que les Etats-membres peuvent prévoir, par la loi ou au moyen de conventions collectives, des règles plus spécifiques pour assurer a protection des droits et libertés en ce qui concerne les traitements des données à caractère personnel des salariés.

➢ Les principes fondamentaux du traitement des données personnelles

Le RGPD rappelle que tout traitement de données personnelles doit répondre aux six principes fondamentaux suivants :

- Licéité, loyauté, transparence ;
- Finalités déterminées, explicites et légitimes ;
- Minimisation des données traitées (données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités) ;
- Exactitude ;
- Durée limitée ; n'excédant pas celle nécessaire au regard des finalités du traitement ;
- Intégrité et confidentialité

Pour être licite, le traitement d'une donnée personnelle doit reposer sur l'une des six bases juridiques suivantes :

- Consentement pour une ou plusieurs finalités spécifiques ;
- Exécution d'un contrat en cours ;
- Obligation légale ;
- Traitement nécessaire aux fins des intérêts légitimes poursuivis par le responsable de traitement, à moins que ne prévalent les libertés et droits fondamentaux de la personne concernée ;
- Sauvegarde des intérêts vitaux de la personne ;
- Mission de service public.

➢ Le nouveau principe de responsabilité (« accontability ») imposé à l'employeur

A compter du 25 mai, le régime déclaratif auprès de la CNIL est supprimé au profit d'un régime de protection des données dès la conception assis sur un principe de responsabilité et de conformité comportant des mesures appropriées.

L'employeur doit donc être en mesure de démontrer la conformité du système de traitement des données et de celui de ses sous-traitants.

Pour cela, l'employeur doit :

- Réaliser une cartographie de tous les traitements de données personnels mis en place dans l'entreprise afin de déterminer notamment la base juridique et la finalité des traitements réalisés ;
- Tenir un registre détaillé de toutes les activités de traitement (obligatoire dans les entreprises de plus de 250 salariés, mais pratique à développer dans toutes les entreprises) ;
- Mettre en place un « Data protection officer » (obligatoire dans certaines conditions, mais pratique permettant de prouver la mise en conformité au RGPD) ;
- Procéder à l'information des salariés en matière de traitement des données personnelles ;
- Mettre à jour les documents sociaux de la structure (contrats de travail, notes d'information, chartes…) ;
- Mettre en place des procédures permettant le respect des droits des salariés en matière de traitement des données personnelles (droit d'accès, droit d'opposition, droit à l'effacement, droit de modification…) ;
- Mettre en place des procédures de notification d'atteinte à la sécurité des données dans la structure.

3 – Les nouvelles sanctions du non-respect de la législation en matière de traitement des données personnelles

Le RGPD a intensifié les sanctions applicables pour violation de la législation en matière de traitement des données personnelles.

➢ Les actions contentieuses

Une action individuelle peut être menée par toute personne ayant subi un préjudice du fait d'une violation du RGPD pour obtenir réparation auprès du Responsable ou du sous-traitant.

Par ailleurs, une class action a été créée par le RGPD en matière de données personnelles afin que toute personne puisse donner mandat à une association ou à une organisation syndicale représentative d'agir en son nom.

➢ Les sanctions administratives

La CNIL, autorité de contrôle, peut condamner les structures à amendes allant jusqu'à 10 millions d'euros ou jusqu'à 2% du chiffre d'affaires annuel mondial si un responsable de traitement ou un sous-traitant a commis une infraction telle que la non-tenue des registres du d'activités de traitement, le non-respect du principe de protection des données dès la conception, la notification des violations.

Cette amende peut aller jusqu'à 20 millions d'euros ou jusqu'à 4% du chiffre d'affaires mondial en cas de violation des exigences relatives aux transferts hors Union Européenne ou aux principes dits « de base » (ex : objet légitime du traitement).

➢ Les sanctions pénales

Les sanctions prévues par le Code pénal peuvent également toujours être appliquées à l'encontre d'un responsable de traitement.

En effet, des sanctions allant jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende peuvent être décidées en cas de :

- Non-respect des formalités déclaratives ;
- Traitement de données sensibles sans avoir procédé à une analyse d'impact ;
- Collecte de données personnelles par un moyen frauduleux, déloyal ou illite ;
- Conservation de données au-delà des durées prévues par la loi ou dans les déclarations à la CNIL ;
- Transfert de données en dehors de l'Union-Européenne en dehors des conditions légales.

En conséquence, toute structure, quelle que soit sa taille, doit se mettre en conformité avec les exigences posées par cette nouvelle réglementation européenne et obligatoire à compter du 25 mai 2018.

Votre Fédération organise des formations relatives à l'application de ce nouveau Règlement européen :

- **Le jeudi 31 mai 2018 ;**
- **Le mercredi 6 juin 2018 ;**
- **Le mercredi 13 juin 2018.**