

## RGPD : quelles conséquences pour l'employeur ?

02.11.2017



À partir du 25 mai 2018, chaque entreprise belge devra respecter les dispositions du **Règlement général sur la protection des données (ou RGPD; en anglais : GDPR, General Data Protection Regulation)** qui définit, au niveau européen, les **nouvelles règles relatives à la protection des données personnelles des citoyens européens**. Le RGPD modifiera le fonctionnement de l'entreprise dans les domaines où elle entre en contact avec le traitement de données personnelles, de façon structurelle.

Cette nouvelle réglementation aura donc bel et bien un impact sur le traitement des salaires et la gestion des ressources humaines de chaque employeur. Dans les prochains mois, vous devrez donc modifier certains éléments dans votre entreprise et dans votre gestion des ressources humaines, afin de vous conformer au RGPD et ainsi éviter des amendes.

Bien entendu, Group S adaptera également son mode de fonctionnement pour respecter ces nouvelles règles et vous aidera à les appliquer dans la gestion quotidienne de votre personnel.

### **Le RGPD et la gestion des ressources humaines**

---

#### **Le traitement des données personnelles**

Chaque employeur traite des données personnelles de personnes actives au sein de son entreprise, notamment par :

- la gestion des salaires et l'administration du personnel ;
- la conservation de dossiers personnels ;
- l'élaboration d'une base de données de candidats, de travailleurs, de travailleurs intérimaires, de consultants, etc. ou la tenue d'un registre des présences ;
- la mise en place d'un système de télésurveillance, d'e-monitoring, de track and trace ;
- la publication de photos sur l'intranet ;

- etc.

Selon la réglementation actuelle, l'employeur doit, lors du traitement de données personnelles, veiller aux éléments suivants :

- le traitement doit :
  - avoir un objectif ;
  - se dérouler de façon intègre et confidentielle ;
  - être pertinent et juste ;
  - être licite, loyal et transparent ;
- la conservation des données est limitée ;
- il ne peut s'agir de données sensibles (liées à la race, la religion, etc.)

## **Respecter la réglementation sur la vie privée aujourd'hui**

L'employeur qui traite des données personnelles doit avoir une raison fondée de le faire. Autrement dit, le traitement doit :

- être nécessaire à l'exécution du contrat ou à sa préparation ;
- résulter d'une obligation légale (par exemple, pour des déclarations fiscales ou sociales) ;
- avoir un intérêt justifié (par exemple, dans le cas d'évaluations) ;
- avoir l'accord du travailleur (à défaut d'une autre disposition).

## **Respecter la réglementation sur la vie privée en 2018**

En mai 2018, cette réglementation sera plus stricte. L'employeur devra donc suivre de nouvelles règles et tenir compte d'un certain nombre d'éléments supplémentaires. S'il ne respecte pas les dispositions du RGPD, il risquera une amende pouvant atteindre 4 % du chiffre d'affaires global de l'exercice précédent, avec un maximum de 20 millions d'euros.

## **Que faire pour respecter le RGPD ?**

1. Informer le travailleur ;
2. Tenir un registre des activités ;
3. Nommer un délégué à la protection des données ;
4. Prévoir les pertes et les fuites de données ;
5. Veiller au respect du RGPD en externe ;
6. Veiller au respect du RGPD en interne.

### **1. Informer le travailleur**

Selon la réglementation actuelle, l'employeur doit communiquer au travailleur les éléments suivants :

- l'identité du responsable du traitement des données ;
- la finalité du traitement ;
- les données traitées ;
- l'identité de celui qui traite les données ;
- le droit du travailleur d'accéder à ces données et de les rectifier.

Le RGPD élargit cette obligation. L'employeur devra donc fournir au travailleur des informations supplémentaires :

- le fondement légal pour le traitement de ces données ;

- la possibilité de retirer son autorisation ;
- le délai de stockage des données ;
- l'existence du droit à la portabilité des données ;
- l'existence du droit de consultation, de correction, d'effacement, de limitation et d'opposition ;
- la possibilité d'introduire une plainte auprès de la Commission de protection de la vie privée ;
- les coordonnées d'un délégué à la protection des données (voir plus loin).

Que devra faire l'employeur ?

L'employeur sera tenu de communiquer ces informations aux travailleurs déjà en service, aux nouveaux travailleurs et aux candidats par des séances d'information ou des documents ad hoc (règlement de travail, contrats individuels et conventions).

## **2. Tenir un registre des activités**

L'employeur devra pouvoir prouver que les données personnelles de ses travailleurs sont traitées dans le respect des dispositions du RGPD. Il existera donc une obligation de documentation.

Que devra faire l'employeur ?

L'employeur devra établir un registre des activités de traitement et le mettre à jour régulièrement. Ce registre reprendra l'ensemble des processus de traitement et, pour chaque processus, mentionnera les éléments suivants :

- l'identité du responsable du traitement des données ;
- les données traitées ;
- la provenance des données traitées ;
- les raisons de ce traitement ;
- qui reçoit les données (ex. : le secrétariat social afin de traiter les salaires) ;
- le délai de conservation des données ;
- les mesures de sécurité mises en place.

Dans certains cas, il faudra également estimer l'effet de la protection des données. La Commission de protection de la vie privée doit encore déterminer le type de traitement qui requerra une telle procédure.

## **3. Nommer un délégué à la protection des données (*Privacy Officer*)**

Un délégué à la protection des données devra parfois être désigné pour veiller au respect du RGPD dans l'entreprise. Ce délégué devra être formé afin d'accomplir sa mission avec l'expertise nécessaire.

Que devra faire l'employeur ?

L'employeur vérifiera s'il est tenu de nommer un délégué à la protection des données. Si c'est le cas, il lui fournira la formation nécessaire et garantira qu'il puisse remplir correctement sa mission.

## **4. Prévoir les pertes et les fuites de données**

Selon le RGPD, l'employeur devra également prévoir un niveau de sécurité suffisant au sein de l'entreprise et mettre au point une procédure permettant de détecter, rapporter et examiner les éventuelles fuites de données. Il ne s'agit pas uniquement des fuites « actives » dues à la cybercriminalité, mais également des fuites accidentelles (par exemple : un courrier électronique a été envoyé à la mauvaise personne, un ordinateur de l'entreprise a été volé, des notes ont été oubliées dans le train, etc.).

Que devra faire l'employeur ?

L'employeur devra définir une procédure reprenant les actions qui seront prises en cas de fuite de données. Il devra former les personnes concernées en conséquence et leur préciser leur responsabilité respective, tenir un registre des fuites de données et, dans certains cas, faire une déclaration à la Commission de la vie privée.

### **5. Veiller au respect du RGPD en externe**

Si l'employeur fait appel à un tiers pour traiter les données personnelles de ses travailleurs, il devra s'assurer que ce dernier respecte bien le RGPD. Le tiers devra d'ailleurs fournir à l'employeur les garanties nécessaires prouvant qu'il respecte le RGPD.

Que devra faire l'employeur ?

L'employeur devra répertorier les différents sous-traitants qui traitent des données personnelles de personnes actives dans son entreprise et s'assurer qu'ils respectent bien le RGPD.

### **6. Veiller au respect du RGPD en interne**

L'employeur devra également identifier les données personnelles traitées au sein de son entreprise et vérifier que ce traitement respecte les règles énoncées ci-dessus.

Que devra faire l'employeur ?

L'employeur devra établir une cartographie du traitement, afin d'identifier les contrôles qui sont suffisants et ceux qui doivent être élargis ou approuvés. Cette cartographie pourra ensuite être utilisée pour accorder la gestion du personnel avec les dispositions du RGPD.

---