SECRETARIAT SOCIAL LIEGE
UCM

La Question du Mois

Avril 2018

Le 25 mai prochain entre en vigueur le Règlement Général pour la Protection des Données (RGPD). De quoi s'agit-il ? Suis-je concerné ? Quelles démarches dois-je accomplir pour être en ordre ?

Dès l'instant où vous traitez des données à caractère personnel, vous êtes concerné par cette nouvelle réglementation. Il vous incombe dès lors un certain nombre d'obligations.

■ 1. Règlement européen ■

Ces nouvelles obligations trouvent leur origine dans un règlement européen conclu le 27/04/2016 (Règlement 2016/679). Il renforce sensiblement la protection des données à caractère personnel en prévoyant un mécanisme contraignant avec sanctions à la clé en cas d'infraction. De la plus petite PME à la multinationale, il s'applique aussi bien au secteur privé qu'au secteur public. Son entrée en vigueur est fixée au 25/05/2018.

■ 2. Traitement de données à caractère personnel■

Le RGPD s'applique à tout traitement de données à caractère personnel.

Sont des **données à caractère personnel** : toute donnée se rapportant à une personne physique identifiée ou identifiable.
Le champ d'application est extrêmement large. Cela va de l'identification directe (nom-prénom de clients, membres du personnel, fournisseurs, sous-traitants, etc.) à l'identification indirecte (données d'identification et de localisation tels qu'un traceur GPS, une adresse IP, etc.).
En clair, il s'agit de tout élément permettant d'identifier une personne physique.

La notion de **traitement** vise toute opération effectuée sur des données à caractère personnel (collecte, enregistrement, conservation, consultation, communication, etc.).

Au regard de ce qui précède, il est difficile d'imaginer qui ne serait pas concerné par le RGPD.

En votre qualité d'employeur, vous traitez à coup sur des données à caractère personnel.

■ 3. Mener une politique de conscientisation, de sensibilisation et de transparence ■

Il est indispensable de rappeler à chaque intervenant ses obligations en matière de confidentialité et de protection des données à caractère personnel. Cela peut passer par la rédaction d'un code de bonnes conduites où est mis l'accent sur la responsabilisation, à savoir :

- l'utilisation des données à caractère personnel uniquement pour les finalités prévues ;
- en cas de communication de données à un tiers toujours vérifier son habilitation ;
- la mise en place de règles en vue de créer un environnement de travail ordonné ;
- l'obligation de prévenir immédiatement en cas de problèmes de sécurité, perte, fuite, vol de données.

Vous êtes également tenu d'informer en toute transparence et dans un langage clair et compréhensible la personne dont vous traitez les données de l'existence d'un certain nombre de droits (voir point 9).

■ 4. Vérifier vos contrats en cas de sous-traitance

Si vous faites appel à des prestataires de services externes pour l'exécution de certaines missions (ex : secrétariat social, bureau comptable etc.) ou si vous agissez vous-même en qualité de sous-traitant, il est indispensable que le contrat de sous-traitance contienne un certain nombre de garanties pour être en conformité avec le RGPD.

■ 5. Identifier la base légale du traitement ■

En votre qualité de responsable du traitement, vous êtes tenu d'identifier la base juridique qui sert à chacune des activités de traitement (= principe de licéité).

Le RGPD énumère six motifs juridiques valables :

- **Le consentement**

Il s'agit d'une manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair (ex : pas une case pré-cochée dans un formulaire), que des données à caractère personnel la concernant feront l'objet d'un traitement. La preuve de son obtention doit pouvoir être démontrée. Il peut en outre être retiré tout aussi facilement qu'il a été donné.

Dans le cadre des relations de travail, il sera difficile d'invoquer le consentement comme fondement juridique du traitement eu égard au lien de subordination qui unit les parties.

- **Le contrat**

Il constitue une base juridique lorsque le traitement est indispensable à l'exécution du contrat auquel la personne concernée est partie (ex : données personnelles en vue du paiement de la rémunération). Ce fondement peut également couvrir des mesures précontractuelles à condition qu'elles soient exécutées à la demande de la personne concernée (ex : établissement d'un devis).

- **Une obligation légale**

C'est le cas lorsque le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (ex : DIMONA, fiches fiscales etc.)

- **La sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique**

Il en est ainsi lorsqu'il s'agit d'un traitement nécessaire pour des questions de vie ou de mort ou destiné à faire face à des menaces qui comportent un risque pour la santé d'une personne.

- **L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement**

- **L'intérêt légitime du responsable du traitement**

L'intérêt légitime peut constituer une base juridique à moins que les droits et libertés de la personne concernée ne prévalent. Dans cette hypothèse, il y a lieu d'effectuer très prudemment une balance entre les intérêts en présence. Pour chaque traitement, il y a lieu d'établir une légitimation spéciale et documentée qui prend en considération les besoins du responsable de traitement par rapport à l'impact sur la personne concernée. Des mesures de contrôle des travailleurs peuvent rentrer dans cette dernière catégorie pour autant qu'elles soient proportionnées, subsidiaires et documentées (ex : instauration de caméras de surveillance dans le respect de la CCT n°68 du CNT).

■ 6. Dresser un inventaire des traitements de données à caractère personnel et en préciser la finalité ■

Vous devez lister minutieusement toutes les données à caractère personnel qui sont à votre disposition. Il vous incombe de vérifier si elles sont exactes et actuelles. Vous devez ensuite en déterminer une finalité (ou sous-finalité). Il s'agit d'un principe fondamental du RGPD. A chaque traitement doit correspondre une finalité. La collecte des données doit se limiter à ce qui est strictement nécessaire à la réalisation de cette finalité. Il est interdit de traiter ultérieurement des données pour une autre finalité que celle prévue initialement.

Exemple : dans le cadre d'une nouvelle embauche, vous êtes en possession de CV. La finalité est le recrutement et la sélection d'un nouveau travailleur. Vous ne pouvez traiter les données recueillies pour une autre finalité (ex : étoffer votre listing clients).

■ 7. Intégrer les données traitées dans un registre des activités de traitement ■

Ce registre doit être tenu (sous format papier ou électronique) dès l'instant où le traitement de données n'a pas un caractère occasionnel. En votre qualité de chef d'entreprise, vous gérez de manière régulière les données de vos travailleurs, clients, fournisseurs. Vous serez dès lors systématiquement tenu d'établir un registre.

Si vous agissez en qualité de sous-traitant, vous devez établir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement.

Il comporte plusieurs mentions obligatoires :

- **Les personnes responsables**

Doit figurer au registre le nom et les coordonnées du responsable du traitement et le cas échéant d'un délégué à la protection des données (DPO). La désignation d'un DPO n'est obligatoire que lorsque le traitement de données à grande échelle est l'activité de base de la PME.

- **Le traitement et ses finalités**

Le registre mentionne, par traitement, ses finalités en détail ainsi que la base légale sur laquelle il repose.

- **Les données traitées et les personnes concernées**

Le registre mentionne, par traitement, les données à caractère personnel traitées (ex : nom, prénom, situation familiale, n° tél, n° de compte en banque, adresse mail etc.) ainsi que les personnes

concernées (ex : travailleurs de l'entreprise, clients, fournisseurs etc.).

- **Les destinataires**

Le registre mentionne l'identité de tous les destinataires des données à caractère personnel. En cas de transfert vers un pays hors Union européenne, il y a lieu de joindre les documents attestant de l'existence de garanties appropriées.

- **Délai de conservation**

Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, dans la mesure du possible, le registre mentionne le délai prévu pour l'effacement des données à caractère personnel.

- **Mesures de sécurité**

Dans la mesure du possible, le registre contient une description générale des mesures de sécurité techniques (antivirus, back-up, firewall etc.) et organisationnelles (politique générale de sécurité, code de bonne conduite etc.).

■ 8. Réaliser une analyse d'impact ■

Vous êtes tenu de réaliser une analyse d'impact lorsqu'un type de traitement est susceptible d'engendrer un **risque élevé** pour les droits et libertés des personnes physique.

Il pourrait en être ainsi en cas de :

- Traitement automatisé de données à caractère personnel (= profilage) ;
- suivi systématique visant à surveiller et contrôler ;
- traitement de données sensibles (santé, données de localisation, données financières) ;
- traitement de données à grande échelle.

Exemple : vous surveillez les habitudes de navigation de vos travailleurs afin de prévenir un usage privé excessif de l'outil informatique durant les heures de travail. Une analyse d'impact sera très probablement nécessaire.

Votre analyse d'impact doit être menée avant le début du traitement (= le plus en amont possible). Elle doit être répétée régulièrement de manière à ce que l'évaluation des risques et les mesures y afférentes restent d'actualité.

Elle contient :

- une description détaillée et claire des opérations de traitement envisagées et des finalités ;
- une évaluation de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques.

Pour plus de précisions : consultez la recommandation du 28 février 2018 de la Commission de la protection de la vie privée.

■ 9. Droits de la personne concernée ■

Vous devez informer la personne dont vous traitez les données de l'existence d'un certain nombre de droits :

- **Droit à l'information**

Lors de la collecte de données à caractère personnel, vous êtes tenu de fournir une série d'informations. Il s'agit des mêmes informations que celles figurant au registre des activités de traitement auxquelles s'ajoutent :

- les droits d'accès, effacement, rectification, limitation, opposition et portabilité ;
- si le traitement se fonde sur le consentement : le droit de retirer son consentement à tout moment ;
- en cas de prise de décision automatisée, la logique sous-jacente ;
- des explications sur l'intérêt légitime du responsable du traitement si le traitement repose sur cette base juridique (ex : surveillance par caméra des travailleurs, contrôle de l'outil informatique etc.) ;
- la source des données en cas de collecte indirecte (= une autre source que la personne elle-même) ;
- si la personne concernée est obligée de fournir ses données par la loi ou un contrat : les conséquences en cas de refus (ex : impossibilité d'établir la fiche de paie) ;
- le droit d'introduire une réclamation auprès de l'Autorité de protection des données.

- **Droit d'accès**

La personne concernée a le droit d'obtenir la confirmation que ses données sont ou ne sont pas traitées. En cas de traitement, elle a le droit d'obtenir une copie de ses données.

- **Droit de rectification**

La personne concernée a le droit d'obtenir, dans les meilleurs délais, la rectification de données inexactes ou incomplètes.

- **Droit à l'effacement**

La personne concernée peut exiger que vous effaciez ses données lorsqu'il n'y a plus de motif fondé de les traiter :

- les données à caractère personnel ne sont plus nécessaires à la réalisation de la finalité poursuivie ;
- vous traitez les données de manière illicite ;
- vous êtes tenu à une obligation légale d'effacement ;

- la personne concernée retire son consentement et le traitement n'a pas d'autre base juridique (ex : volonté de quitter un réseau social) ;
- après l'exercice réussi du droit d'opposition.

Vous êtes bien entendu en droit de refuser l'effacement des données lorsque le traitement est nécessaire au respect d'une obligation légale (ex : délai de conservation des documents sociaux obligatoires).

- **Droit à la limitation du traitement de données**

Dans certaines circonstances (ex : contestation de l'exactitude de certaines données, données devenues inutiles mais nécessaires pour la défense d'un droit), la personne concernée peut exiger une « limitation » du traitement de ses données. Cela signifie que vous ne faites que conserver les données et vous vous abstenez de toute activité de traitement (= gel des données). Si vous avez transmis ces données à des tiers, vous devez les aviser de leur obligation à la limitation de traitement (à moins que cela s'avère impossible ou exige des efforts disproportionnés).

- **Droit d'opposition**

Si la personne concernée s'oppose aux activités de traitement, vous devez cesser de les traiter sauf si vous invoquez des motifs légitimes et impérieux qui prévalent sur ses intérêts, droits et libertés.

- **Droit à la portabilité des données**

Cela permet à la personne concernée d'obtenir ses données à caractère personnel pour les réorienter vers d'autres services. Pour que ce droit puisse être exercé, il doit s'agir de données automatisées venant de la personne elle-même sur base du consentement ou d'un contrat.

- **Droit ne pas être soumis à une décision individuelle automatisée**

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (y compris le profilage) sans intervention humaine qui l'affecte de manière significative ou qui a des effets juridiques sauf :
- lorsque la loi l'autorise (ex : prévention de la fraude ou de l'évasion fiscale) ;
- lorsque la décision est fondée sur un consentement explicite de la personne ;
- si cela est nécessaire à la conclusion ou à l'exécution d'un contrat (pour autant qu'il n'y ait pas moyen d'y arriver via des méthodes moins « intrusives »).

■ 10. Fuite de données ■

Le RGPD définit une fuite de données comme étant une violation de la sécurité entraînant, de manière accidentelle ou intentionnelle, la destruction, la perte, l'altération ou la transmission non autorisées de données à caractère personnel (ex : perte d'un ordinateur portable, cyberattaque, etc..)
Si cela arrive dans votre entreprise, vous êtes tenu de consigner dans un journal interne la cause, les données affectées, les conséquences, les mesures prises et le cas échéant la raison pour laquelle cette fuite de données n'a pas été notifiée à l'Autorité de protection des données (APD). Pour des raisons de facilité, ce journal peut être intégré dans le registre des activités de traitement.
Une notification à l'APD doit être réalisée si la fuite est susceptible d'engendrer un risque pour les droits et libertés de la personne concernée.
En votre qualité de responsable de traitement, vous devez agir dans un délai de 72 heures après que vous ayez été informé de la fuite.
Si vous agissez en qualité de sous-traitant, vous êtes tenu d'avertir immédiatement le responsable du traitement.

Par ailleurs, une notification à la personne concernée devra être effectuée si la fuite présente un risque élevé pour ses droits et libertés.
Cette notification n'est toutefois pas nécessaire lorsque vous avez pris des dispositions adéquates :
- mesures de sécurité visant à rendre les données personnelles incompréhensibles pour toute personne qui n'est pas autorisée à avoir accès (= méthode de cryptage forte) ;
- mesures de sécurité prises après la fuite qui font en sorte que le risque élevé n'est plus susceptible de se matérialiser (ex : effacement à distance en cas de vol du support) ;
- lorsqu'une communication individuelle exigerait des efforts disproportionnés. Dans ce cas, il sera alors opté pour une communication publique ou une autre mesure similaire.

■ 11. Sanctions en cas de violation du RGPD ■

La personne concernée par une violation du RGPD a le droit d'introduire une réclamation auprès de l'Autorité de protection des données (APD). Cette action ne l'empêche toutefois pas d'introduire en parallèle une action devant les Cours et tribunaux afin d'obtenir réparation de son préjudice.

L'APD peut agir de sa propre initiative et infliger des sanctions.
Elle est composée d'un service d'inspection et d'une chambre contentieuse.

Lors de ses contrôles, l'APD ne devra pas démontrer une faute dans le chef du responsable de traitement (ou du sous-traitant). Ce renversement de la charge de la preuve a pour conséquence qu'il vous incombera de démontrer que vous avez respecté le RGPD.

Si vous avez commis un manquement, la chambre contentieuse de l'APD pourra vous infliger des sanctions. Le panel de sanctions est large. Cela va du simple avertissement, à l'injonction et dans les cas les plus sévères à une amende administrative.

En cas d'amende administrative, deux plafonds sont applicables :

- 10.000.000 € ou 2 % du chiffre d'affaires lorsqu'il s'agit de manquements aux obligations formelles du RGPD ;
- 20.000.000 € ou 4 % du chiffre d'affaires en cas de violation des principes de base du RGPD ou de non-respect d'une injonction.

Les décisions de la chambre contentieuses peuvent faire l'objet d'un recours devant la Cour des marchés de la Cour d'appel de Bruxelles. Ce recours n'a pas d'effet suspensif ce qui signifie que les amendes devront être payées immédiatement.

■ 12. Plus d'informations ■

Le site de la Commission de la protection de la vie privée (prochainement Autorité de protection des données) contient des informations détaillées sur le RGPD. Un guide pratique pour les PME (Vade-mecum) reprend les informations de base. Vous pourrez en outre consulter et/ou utiliser un modèle de registre des activités de traitement mis gratuitement à votre disposition.

Paul Ciborgs

N'hésitez pas à contacter le Secrétariat social pour tout complément d'information à ce sujet.