RGPD : comment se mettre en conformité ?

Domaine d’application de la réforme

Le règlement européen RGPD concerne toutes les structures qui collectent et traitent des données personnelles.

Les entreprises concernées

Tout organisme (entreprise, association…), privé ou public, est tenu d’appliquer le RGPD dès lors qu’il collecte ou traite des données personnelles pour son compte ou pour celui d’un tiers. Aucun autre critère, comme l’effectif ou encore le chiffre d’affaires, n’entre ici en ligne de compte. Toutes les entreprises sont donc concernées, ou potentiellement concernées, y compris les plus petites.

Les données personnelles

Une donnée personnelle est une information qui permet, à elle seule ou en la croisant avec d’autres données, d’identifier une personne soit directement (nom, prénom), soit indirectement (téléphone, courriel, adresse, photo, voix,

caractéristiques sociales ou physiques, empreintes, ADN…). Dès lors qu'il regroupe ce type d'informations, un fichier (papier ou numérique) est considéré comme un traitement de données personnelles et doit ainsi être constitué et géré conformément au RGPD.

Recenser l'existant…

Pour se mettre en conformité avec le RGPD, les entreprises doivent commencer par recenser leurs fichiers contenant des données personnelles.

Pour se mettre en conformité, le premier travail consiste à recenser l'existant. Ainsi existe-t-il sans doute dans votre entreprise des fichiers de données personnelles tels que nous venons de les définir (fichiers clients, prospects, fournisseurs, employés, fichiers paie, formations, gestion des accès…). Tous doivent être recensés dans un registre. Registre dans lequel, pour chaque traitement, doivent être renseignés sa finalité, le type de données personnelles présentes (noms, salaires, adresses…), les personnes ou les services qui peuvent y accéder et enfin la durée de conservation de ces données.

Important : des modèles de registres sont téléchargeables sur le site de la Cnil (www.cnil.fr). Plus largement, la Cnil, l'organisme de contrôle de la gestion des données personnelles, a édité des fiches techniques et un guide afin d'aider les entreprises à entamer une démarche de mise en conformité avec le RGPD.

… pour identifier les actions

à mener

Responsables des fichiers de données personnelles qu'elles détiennent, les entreprises doivent gérer les traitements de ces données de façon raisonnée.

Le principe du RGPD consiste à responsabiliser les détenteurs de fichiers. Il vous revient donc, en tant que chef d'entreprise, d'adopter une approche raisonnée de ces traitements et de leur gestion. Sachant que les données personnelles ne doivent pas être conservées au-delà de ce qui est nécessaire. Pour chacun des traitements mis en œuvre dans votre entreprise, vous devez donc vous poser les questions suivantes :

Mon entreprise a-t-elle besoin de ces informations ?

Il est possible que vous ayez créé des fichiers il y a quelques années dans un objectif qui n'est plus d'actualité (liste de prospects pour le lancement d'une activité abandonnée…). Si c'est le cas, vous n'avez plus besoin de ces traitements. Supprimez-les.

Vous devez également vérifier que chaque type d'information recueilli pour le traitement est absolument nécessaire (par exemple, est-il pertinent de connaître le nombre d'enfants de chaque salarié si aucun avantage salarial n'est attaché à cette information ?). Si ce n'est pas le cas, supprimez les types de données non pertinents.

Enfin, vous devez faire en sorte que vos fichiers soient mis à jour régulièrement. Autrement dit, que les données qui n'ont plus rien à y faire soient supprimées : données relatives à d'anciens clients dans une base clients, informations dont la durée de conservation est dépassée…

Qui accède à ces données ?

Seules les personnes habilitées doivent pouvoir accéder aux données personnelles. Vous devez donc veiller à les compartimenter (les mettre sous clé s'il s'agit d'informations papier, ou sur un espace à accès restreint lorsqu'elles sont numériques).

Ces informations sont-elles protégées ?

Vous êtes responsable des données personnelles que vous hébergez ou que vous faites héberger par un prestataire. Vous devez donc prendre les mesures nécessaires pour minimiser les risques d'atteinte à leur intégrité et à leur confidentialité. Ainsi, pour chaque traitement, il vous faut évaluer le niveau de sécurité existant (complexité des mots de passe, performance et mise à jour des antivirus, politique de chiffrement, sécurité des locaux, politique de sauvegarde…) et, le cas échéant, le rehausser.

Et attention, avant de lancer un traitement, lorsque les données traitées (ethniques, religieuses, génétiques…) ou l'objectif du traitement (notation des personnes, télésurveillance, traitement relatif à des personnes vulnérables…) sont dits « sensibles », il peut être nécessaire de respecter une démarche particulière (PIA : Privacy Impact Assessment). N'hésitez pas, dans ce cas, à vous rapprocher de la Cnil.

Attention : si, accidentellement ou de manière illicite, votre entreprise est victime d'une violation de données personnelles (données détruites, perdues ou divulguées) et que cette violation est susceptible de présenter un risque pour les droits des personnes concernées, vous devez le signaler à la Cnil dans les 72 heures.

Désigner un DPO

Lorsque la situation est complexe, la Cnil conseille de désigner un délégué à la protection des données (DPO), qui peut être un collaborateur ou un prestataire, et qui peut être mutualisé entre plusieurs entreprises. Le DPO est là pour conseiller le chef d'entreprise sur ses obligations légales en matière de protection des données, contrôler le respect de la réglementation, mais aussi coopérer avec la Cnil. Mais seuls les organismes qui opèrent des traitements à risques ont l'obligation d'en désigner un. Plus précisément, l'article 37 du RGPD impose la désignation d'un DPO lorsque :

– le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

– les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ;

– les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 du RGPD.

Respecter les droits des personnes fichées

Les entreprises doivent respecter les droits des personnes fichées et les informer de ces droits et des moyens pour les exercer.

Les personnes « fichées » ont des droits sur leurs données. Droits que vous devez respecter tant lors de la création qu'au cours de la gestion du traitement.

Ainsi, lorsque vous collectez des données personnelles, vous devez informer les personnes concernées de la finalité du traitement, de la raison de ce recueil de données et du délai pendant lequel elles seront conservées, leur préciser les personnes qui auront accès à ces données (service, prestataire…) et leur indiquer les modalités d'exercice de leurs droits (via une messagerie, un espace dédié sur un site…).

Parmi ces droits figurent, notamment, un droit d'accès leur permettant de connaître l'ensemble des données les concernant, un droit de rectification (permettant de les corriger), un droit d'opposition et d'effacement (lorsque le fichier n'est pas obligatoire) ou encore un droit à la portabilité (afin, par exemple, de transférer les données à un autre prestataire). Il vous revient donc de mettre en place un processus offrant à ces personnes la possibilité d'exercer leurs droits simplement et rapidement.

Pour permettre aux personnes (clients, prospects) dont vous traitez les données d'exercer leurs droits, vous pouvez par exemple prévoir un formulaire de contact spécifique sur votre site Internet ou mettre en place un numéro de téléphone ou une adresse de messagerie dédiée.

Attention : le règlement RGPD ne renforce pas seulement les obligations qui pèsent sur les gestionnaires de fichiers. Il prévoit également un durcissement des sanctions. Ainsi, en cas de manquement grave, une amende pouvant aller jusqu'à 20 M€ ou 4 % du chiffre d'affaires réalisé pourra être infligée. Sachez néanmoins qu'en ces premiers mois d'application, la Cnil devrait être clémente avec les entreprises contrôlées dès lors qu'elles auront entamé leur processus de mise en conformité.