IMPACT DU RGPD POUR LES DRH

Le Règlement Général sur la Protection des Données (RGPD) fait partie des contraintes réglementaires réelles qu'un DRH doit nécessairement appréhender dans son périmètre d'action.

Même si la CNIL a fait savoir que la date du 25 mai n'était pas à considérer comme un couperet et que ses agents n'avaient pas instruction d'aller à la chasse aux employeurs en infraction, il paraît très imprudent de considérer que ce chantier de conformation aux nouvelles exigences du RGPD peut être considéré comme non prioritaire. Or, si la très grande majorité des entreprises dont l'activité n'est pas directement tournée vers les consommateurs ne manie pas dans le cadre de leur activité opérationnelle de données véritablement sensibles, toutes collectent, utilisent et conservent des données concernant leurs salariés. Les RH sont donc un département souvent considéré comme le maître d'œuvre naturel du « chantier RGPD ».

Ce chantier nous semble pouvoir être appréhendé pour les RH en suivant une méthodologie qui permette progressivement d'intégrer le RGPD et qui leur éviterait surtout de devoir s'y atteler « au pied du mur » et contraintes par différentes parties prenantes (CNIL, organisations syndicales, salariés…). Les grandes lignes de cette méthodologie nous semblent être les suivantes :

- **Réalisation d'une compilation des différents types de données traitées** (sur support informatique et même papier !) : avant l'embauche (CV, tests d'évaluation), au moment de l'embauche (adresse, date de naissance, situation familiale pour la mutuelle, n° de sécu) et pendant la vie du contrat (arrêts maladie, déclarations sociales, entretiens d'évaluation, dossier disciplinaire…). Contrairement à l'idée reçue, le RGPD n'impose pas à l'employeur de solliciter l'acceptation du salarié quant à la détention/l'utilisation/la conservation de ces données, qui sont nécessaires au respect de ses obligations légales et donc nécessaires. Il conviendra toutefois qu'existe un document type d'information des salariés quant à leurs différents droits sur le traitement de leurs données (d'accès, de rectification, de portabilité…).
- **Désignation d'un Délégué à la Protection des Données (DPD) :** il s'agit d'une obligation si l'activité de l'entreprise la conduit à traiter des données personnelles à grande échelle (activité BtoC) ou à traiter des données sensibles (cliniques, banques, assurances…). Le texte ne précise pas qui doit/peut être désigné DPD. Le DRH semble pour la CNIL devoir être exclu, comme le DSI, car ayant trop de pouvoir décisionnel sur les modalités de traitement. Un RRH semble par contre plus correspondre au profil. Ce DPD aura grosso modo les mêmes attributions que l'ancien « CIL », qu'il remplace de fait.
- **Réalisation de « registres de traitements » pour les « organisations » de plus de 250 salariés** (au niveau à notre sens du groupe et non de la seule entreprise) ; cela étant, dans la mesure où les données paie sont par nature susceptibles de comporter un risque pour les droits et libertés et où leur traitement n'est pas occasionnel, tous les employeurs sont, selon nous, concernés par cette obligation. Un tel registre n'est pas complexe en soi à réaliser. Son support peut être un tableur Excel, sur lequel sont renseignés l'identité de la société, l'éventuel DPD, les catégories de personnels visés, les finalités du traitement, les personnes appelées à les manipuler, les mesures de sécurité d'accès et de conservation prises (qui y a accès dans l'entreprise, quels process de sécurité informatique, voire physique, sont mis en place…). La CNIL a mis en ligne un exemple de registre, qui est facile d'utilisation et peut parfaitement être téléchargé et utilisé pour satisfaire à l'obligation.
- **Une « analyse d'impact » pour les traitements considérés comme sensibles** (vidéosurveillance, géoloc) : les déclarations qui avaient été faites auprès de la CNIL pour les mettre en œuvre dispensant pendant 3 ans l'employeur de les refaire. Là encore, la CNIL a mis en ligne un simulateur utilisable en l'état par les employeurs.
- **La validation que les sous-traitants respectent le RGPD :** en matière RH, il sera essentiel de solliciter des fournisseurs du logiciel de paie, du sous-traitant qui réalise la paie, du comptable… afin qu'ils intègrent les exigences du RGPD. Un courrier type peut permettre dans un premier temps d'engager la démarche. L'étape suivante étant de checker que les contrats avec les sous-traitants/fournisseurs satisfont au RGPD.
- **Un toilettage du process de sécurité informatique** devra être réalisé pour les aspects RH. La Charte Informatique est à cet égard l'outil naturel pour formaliser l'organisation de la sécurité des données notamment RH (protection systématique par des mots de passe, verrouillage des PC en cas d'absence même momentanée, accessibilité limitée à certains répertoires…).

A ce stade des démarches, le DRH, qui aura conduit ce chantier, ne pourra pas être considéré par la CNIL comme inerte ou défaillant. Resteront en suspens de nombreux points d'interrogation à traiter, par exemple en matière de durées de conservation des données sociales (5 ans légalement mais en pratique, délai trop court pour parer des demandes indemnitaires prescrites sur une plus longue durée) ou encore la gestion des données personnelles par le CE/CSE pour les œuvres sociales, CE dont l'employeur est le président…

Si la route semble tortueuse, longue et donc décourageante, d'une part elle ne peut être évitée et d'autre part, sa plus grande difficulté semble être de trouver l'énergie et le temps pour s'y engager !

■ **Benjamin Renaud,**
avocat-associé Renaud Avocats