NT/ Le Règlement Général de Protection des Données personnelles du Parlement européen (RGPD).

Dès le 25 mai 2018, le règlement général de protection des données (RGPD) du Parlement européen entrera en vigueur.
Les services RH, notamment, devront réexaminer l'ensemble des traitements portant sur les données personnelles des salariés.

Vidéo-surveillance, fichiers professionnels, enregistrements téléphoniques, géolocalisation... Les services de ressources humaines sont amenés à collecter de plus en plus de données personnelles des salariés : nom, prénom, date de naissance, numéro de sécurité sociale, adresse postale et courriel, numéro de téléphone, photos et vidéos, etc. La mise en œuvre de tels traitements suppose que l'employeur puisse garantir la protection des données personnelles collectées.

Ce texte sera directement applicable en droit français. Des marges de manœuvre en droit national sont toutefois expressément autorisées par le règlement.
Un projet de loi relatif à la protection des données personnelles est en cours de discussion à l'Assemblée nationale (6 février 2018). Il réformera la loi Informatique et libertés du 6 janvier 1978.

UNE RESPONSABILISATION ACCRUE DES EMPLOYEURS

La mise en œuvre de la nouvelle règlementation risque de créer une attention accrue des salariés sur la façon dont leurs données personnelles sont traitées. De plus, les pouvoirs de contrôle et de sanction de la Cnil sont considérablement renforcés.

Les grands principes de protection des données seront maintenus par le RGPD : conditions de licéité du traitement (article 6 du RGPD), finalité du traitement (objectif clair et déterminé), proportionnalité des données (ne pas collecter de données qui ne sont pas nécessaires), durée de conservation limitée.
En revanche, la responsabilité de l'employeur sera renforcée. "L'employeur n'aura plus besoin de demander à la Cnil l'autorisation de mettre en œuvre un traitement de données. Les entreprises devront faire elles-mêmes leur propre évaluation de la compatibilité entre le traitement envisagé et les exigences légales".
Le RGPD obligera les entreprises à documenter le mieux possible leur décision de mettre en œuvre un traitement automatisé des données personnelles de leurs salariés.

L'obligation de prendre en compte les règles de protection des données pèse sur le responsable du traitement, ici l'employeur.
Lorsque l'entreprise a recours à un sous-traitant, par exemple un éditeur de logiciels, elle devra s'assurer et démontrer que le logiciel est bien conforme au RGPD (article 28 du RGPD).

Le contrôle de la Cnil se fera a posteriori.
En cas de manquement, le règlement alourdira les sanctions applicables par la Cnil. Cette dernière pourra condamner l'entreprise à une amende pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial de l'entreprise.
Elle pourra également effectuer des contrôles sur place dans tous les locaux servant à la mise en œuvre d'un traitement de données personnelles, et effectuer des contrôles en ligne sous une identité d'emprunt (selon le projet de loi relatif à la protection des données personnelles).

LA CRÉATION D'UN REGISTRE DES ACTIVITÉS DE TRAITEMENT

L'entreprise doit tenir à la disposition de la Cnil les documents ayant servi de base au traitement de données. Elle doit pouvoir prouver qu'elle s'est posé les bonnes questions avant de collecter les informations des salariés.
Les entreprises de 250 salariés et plus devront ainsi mettre en place un registre des activités de traitement effectuées sous sa responsabilité. Avec une liste de mentions obligatoires précise, établie à l'article 30 du RGPD.

Une analyse d'impact devra également être mise en œuvre avant tout traitement de données présentant un risque élevé pour les droits et libertés des personnes physiques. Ces données dites "sensibles" restent les mêmes qu'auparavant : appartenance politique, syndicale, origine ethnique, religion etc. Seules les données biométriques ont été ajoutées par le RGPD, avec des conséquences qui devraient être limitées à certains secteurs.

UNE MEILLEURE INFORMATION DES SALARIÉS

Le RGPD complète les informations à fournir lorsque des données à caractère personnel sont collectées. Ses articles 13 et 14 listent les mentions d'information obligatoires, qui seront à mettre à jour par les services RH. L'information est à délivrer au moment où les données sont collectées.

Le salarié pourra demander l'accès à toutes ses données personnelles ayant été collectées. Il aura également le droit de demander à l'entreprise les finalités du traitement de données, les destinataires de ces données, la durée de conservation etc. (article 15 du RGPD).
Le délai dans lequel l'entreprise doit accéder à sa demande est raccourci, et passe de deux à un mois (une prolongation exceptionnelle d'un mois est toutefois possible pour les demandes complexes et/ou nombreuses).

La personne concernée par le traitement aura le droit d'être informée en cas de violation de ses données, par exemple dans le cas d'un piratage informatique (article 34 du RGPD).
Ce droit n'est ouvert que dans le cas où la violation est suffisamment grave, c'est à dire si elle "est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique". L'employeur devra également informer rapidement la Cnil (article 33 du RGPD).

LE DROIT À L'OUBLI, À LA RECTIFICATION, AU GEL DES DONNÉES

Un salarié (ou un ancien salarié) peut obtenir l'effacement des données à caractère personnel qui le concernent.
L'entreprise doit accéder à sa demande dans certains cas limitativement énumérés : lorsque les données ne sont plus nécessaire au regard des finalités pour lesquelles elles ont été collectées, lorsque la personne concernée s'oppose au traitement, lorsque le traitement est déclaré illicite, etc. (article 17 du RGPD).

Le salarié peut également demander à l'entreprise de rectifier ses données à caractère personnel lorsque ces dernières sont inexactes (article 16 du RGPD).
Le RGPD maintient également un droit au gel temporaire des données personnelles (en cas notamment de contestation de l'exactitude des données, ou en attendant la vérification du traitement si ce dernier est contesté en justice) (article 18 du RGPD).

LA MISE EN PLACE D'UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Certaines entreprises devront désigner un délégué à la protection des données (data protection officer, ou DPO) (article 37 du RGPD).
C'est le cas des entreprises dont les activités de base "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".
Simplement gérer les salariés et la paie ne correspond pas à cette définition, car il s'agirait alors d'une activité accessoire auxiliaire et non d'une activité de base.
Cette obligation concernera les entreprises dont le traitement des données constitue l'activité principale : les cabinets de recrutement, les agences d'intérim, etc.

Le correspondant informatique et libertés (CIL) est un embryon du DPO, leurs rôles étant sensiblement identiques : s'assurer de la conformité de l'entreprise aux règles concernant la protection des données, et effectuer l'interface avec la Cnil.
Les CIL actuellement en place dans les entreprises ont donc vocation à devenir les futurs DPO, même si l'entreprise peut choisir de faire autrement.