La protection des données personnelles dans l'entreprise

19 avril 2018

• Application du Règlement Général de Protection des données dès le 25 mai 2018, à l'échelle de l'Union européenne.

• Le 12 avril 2018, l'Assemblée nationale a adopté en nouvelle lecture un projet de loi relatif à la protection des données personnelles.

• Ces textes concerneront les pratiques des entreprises et des sous-traitants auxquels elles ont recours pour le traitement des données.

• Cette règlementation aura un impact considérable sur la cartographie des traitements de données personnelles des salariés par les services RH des entreprises.

• La mise en conformité avec ces nouvelles règles européennes, et bientôt nationales, doit donc être dans l'esprit de tous.

1. De nouvelles obligations et plus de responsabilisation

1.1 Désigner un Délégué à la protection des données (DPO)

Interlocuteur principal en matière de données personnelles, il est en charge de conseiller et d'informer le responsable de traitement mais également de contrôler la bonne application de la règlementation. Salarié de l'entreprise ou extérieur à celle-ci, il peut bénéficier d'une formation spécifique dispensée par la CNIL.

Sa désignation est obligatoire pour les autorités et organismes publics ainsi que pour les entreprises privées dont les activités principales consistent en des opérations de traitement de données sensibles à grande échelle ou 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. Elle est possible et recommandée dans les autres cas.

1.2 "Privacy by design": analyse de l'impact des opérations de traitement sur la protection des données···

Cette analyse d'impact est réalisée par le responsable du traitement. Elle a pour contenu et pour objet de "décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité, et d'aider à gérer les risques pour les droits et libertés des personnes physiques, liés au traitement de leurs

données, en les évaluant et en déterminant les mesures nécessaires pour y faire face".

Elle n'est obligatoire qu'en cas de traitement de données susceptible d'engendrer un risque grave pour les droits et libertés des personnes. Outre les cas listés dans le règlement, la CNIL sera habilitée à définir les hypothèses dans lesquelles l'analyse d'impact est requise. Il est par ailleurs très fortement recommandé d'en réaliser une lorsqu'au moins deux des neuf facteurs de risque identifiés par le groupe de travail G29 sont réunis. Parmi ces critères figurent la collecte de données de personnes "vulnérables", en ce inclus les salariés, de telle sorte qu'une telle analyse d'impact sera fréquemment requise en matière de traitement de données RH. En cas de doute sur la gravité du risque, la CNIL peut être consultée librement par l'entreprise.

1.3 ⋯ justifiant la suppression des déclarations préalables à la CNIL

Les grands principes de protection des données seront maintenus (conditions de licéité du traitement, finalité du traitement, proportionnalité des données, durée de conservation limitée) mais les entreprises n'auront plus de formalités de déclaration préalable à effectuer auprès de la CNIL.

1.4 Cartographier le traitement des données personnelles

Pour les entreprises de plus de 250 salariés, tenue obligatoire d'un registre de documentation interne recensant les différents traitements de données personnelles, leurs catégories, leurs objectifs, les acteurs qui les traitent, les flux (origine et destination des données). Les mentions obligatoires sont listées à l'article 30§1 du règlement.

La mise en place de ce document est recommandée pour les entreprises dont l'effectif est inférieur afin de favoriser la transparence dans le traitement des données.

2. Un renforcement des droits des personnes concernées

2.1 Des cas limités de licéité du traitement

Le fondement juridique de chaque traitement doit être identifié pour lui appliquer le régime de protection correspondant. Lorsqu'il s'agit du consentement des salariés, ce dernier doit être libre et explicite ; il peut être retiré à tout moment. Le consentement est nécessaire pour le traitement de données sensibles (santé, appartenance syndicale, etc.) sauf lorsque l'information est nécessaire à la satisfaction d'une obligation légale.

2.2 De nouveaux droits à rappeler lors de la collecte des données

Les salariés doivent être systématiquement informés de leurs droits au moment où les données sont collectées. Il s'agit, outre des droits d'accès, de rectification et d'opposition, de demander la limitation du traitement ou l'effacement des données collectées, ainsi que du droit à la portabilité des données. Les salariés doivent également être avisés de leur droit de formuler une réclamation auprès de la CNIL.

2.3 Des délais de réponse et de réaction raccourcis

Les demandes d'exercice des droits listés ci-dessus doivent en principe recevoir une réponse dans un délai d'un mois, contre deux jusqu'à présent.

Toute violation de données personnelles doit être notifiée à la CNIL sous 72 heures et, si elle est susceptible d'engendrer un risque élevé pour les droits et liberté des personnes concernées, elle doit leur être communiquée dans les meilleurs délais.

3. Un durcissement des sanctions encourues en cas de violation du règlement

3.1 Un maintien des pouvoirs d'enquête et d'injonction de la CNIL

La CNIL peut accéder aux locaux de l'entreprise et demander communication des documents nécessaires à la vérification du respect de la réglementation. Si elle constate une violation, elle peut délivrer un avertissement ou ordonner la limitation du traitement. Ces mesures correctrices pourront, selon le projet de loi, être assorties d'astreintes d'un montant maximum de 100.000 euros par jour de retard.

3.2 Des amendes administratives aux montants dissuasifs

En fonction de la nature de la violation, la CNIL pourra prononcer des amendes d'un montant maximal de :

• 10.000.000 euros, ou pour les entreprises 2% du chiffre d'affaire annuel mondial (le montant le plus élevé étant retenu), en cas de manquement aux dispositions incombant au responsable de traitement, en matière de certification, ou de suivi du code de conduite,

• 20.000.000 euros, ou pour les entreprises 4% du chiffre d'affaire annuel mondial (le montant le plus élevé étant retenu), en cas de manquement aux dispositions relatives aux droits des personnes (droit d'accès aux données, de rectification, d'opposition, de suppression etc.), de non-respect d'une injonction ou de transfert de données dans un Etat tiers hors des hypothèses autorisées.

Le montant de la sanction prononcée devra néanmoins être proportionné à la gravité de la violation et à l'attitude du responsable de traitement.

3.3 Des sanctions pénales inchangées

Les manquements les plus graves à la réglementation sont toujours passibles de 5 ans d'emprisonnement et de 300.000 euros d'amende. Il s'agit en particulier de la collecte illicite de données, la mise en œuvre d'un traitement sans mesures de sécurité suffisantes et la conservation de données personnelles au-delà de la durée autorisée (art. L. 226-16 et suivants du code pénal).

Auteurs

Dominique Mendy

Partner

Thierry Meillat

Partner

> Read the full article online