Société d'Avocats
Chellat Pilpré Huchet
Inscrits au Barreau de l'Essonne

Brève – Février 2018
Droit des affaires – Actualités Juridiques

Le règlement européen sur la protection des données personnelles va entrer en vigueur le 25 mai 2018.

Ce règlement impose de prendre des « mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque ».
Ceci constitue à la fois une reprise et un approfondissement des obligations imposées par la loi « informatique et libertés », qui stipule : **« le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »**
Le RGPD alourdit en revanche grandement les sanctions en cas de non-respect de la règle, prévoyant une amende allant jusqu'à 10 millions d'euros voire 2% du chiffre d'affaires annuel mondial, alors qu'aujourd'hui le plafond de l'amende pécuniaire est fixé à 3 millions d'euros.

La commission nationale de l'informatique et des libertés propose sur son site (www.cnil.fr) un guide à destination des professionnels pour mettre en place les mesures visant à obtenir la sécurité des données personnelles exigée par le règlement.

La plupart des mesures étant d'ordre technique, elles ne seront pas détaillées ici et nous nous limiterons aux mesures juridiques.

1. La charte informatique

Selon la CNIL, toutes les entreprises devraient adopter une charte informatique, et lui donner une force contraignante en l'intégrant au règlement intérieur.

Cette charte doit comporter :

- Le rappel des règles de protection des données et les sanctions encourues
- Les moyens d'authentification utilisés par l'entreprise
- Les conditions d'utilisation des dispositifs personnels
- Les modalités d'intervention des équipes chargées de la gestion du parc informatique
- Les modalités d'utilisation des moyens informatiques et de télécommunication mis à disposition par l'entreprise (messagerie électronique, téléphonie, espaces de stockage…)
- L'obligation pour les salariés de signaler toute violation suspectée de son compte informatique
- L'obligation pour les salariés de verrouiller leur session avant de quitter leur poste
- Les procédures à respecter en cas de copies de données
- L'interdiction pour les salariés de confier leurs identifiants à un tiers, de copier, installer ou modifier des logiciels sans autorisation, de supprimer des informations ne relevant pas de leurs tâches
- Les sanctions encourues en cas de non-respect de la charte.

2. Clauses de confidentialité pour les salariés ayant accès aux données

Outre les clauses à faire signer à l'ensemble des salariés pour autoriser la collecte et le traitement de leurs propres données personnelles, aux fins de gestion du personnel, il conviendra de faire signer, à tout salarié devant accéder aux données personnelles des autres salariés ou des clients, des clauses de confidentialité. Ces clauses devront rappeler la durée illimitée de cette obligation, qui ne cessera pas en cas de rupture du contrat, ainsi que la possibilité de sanction disciplinaire en cas de violation.

3. Gestion de la sous-traitance

Les premiers sous-traitants concernés sont les opérateurs de maintenance informatique, lesquels devront accepter de signer des avenants ou de mettre à jour leurs contrats pour maîtriser l'accès aux données par ces prestataires, en y insérant une clause dite « de sécurité ».

La CNIL préconise la mise en place de registres reprenant les dates et les natures détaillées des interventions de maintenance et de télémaintenance ainsi que les noms de leurs auteurs.

Par ailleurs, tout sous-traitant ou prestataire devant avoir accès ou traiter les données personnelles de l'entreprise doit présenter des garanties en matière de protection des données, incluant le chiffrement des transmissions de données, et des garanties de protection du réseau, de traçabilité, de gestion des habilitations et d'authentification. Ces garanties doivent être mises par écrit dans un contrat définissant, outre les obligations des parties (notamment de confidentialité), l'objet, la durée, et la finalité du traitement. Il est notamment impératif de prévoir un avertissement immédiat en cas de faille de sécurité ou d'incident et ce, dans les plus brefs délais dès lors qu'une violation de données à caractère personnel est suspectée.

Enfin, en cas de recours aux services de cloud, la CNIL recommande de recueillir des garanties quant à la localisation géographique des données, et au respect des conditions légales et des éventuelles formalités auprès de la CNIL pour les transferts de données en dehors de l'Union Européenne.

Pour plus d'informations, ou pour revoir vos contrats et vous proposer des modèles adaptés, n'hésitez pas à nous contacter !