Cornillier AVOCATS

RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES
Anticipez vos nouvelles obligations

Le règlement européen sur la protection des données personnelles (RGPD) adopté par le Parlement européen sera directement **applicable en France à compter du 25 mai 2018**. Un projet de loi devrait toutefois être adopté prochainement afin d'adapter la loi « Informatique et Libertés ». Ce nouveau dispositif nécessite que les entreprises fassent un état des lieux des modalités de traitements de données existantes (conditions de collecte, exercice des droits, mesures de sécurité etc.) et **adaptent leurs procédures**.

Les principales nouvelles obligations des entreprises sont les suivantes :

1. Tenir un registre

L'une des principales modifications est la suppression de l'obligation de déclaration préalable à la CNIL. Elle est remplacée par l'obligation pour les entreprises de tenir un **registre**.

Ce registre devra contenir les mêmes informations que celles indiquées dans la déclaration actuelle, à savoir : les nom et coordonnées du responsable du traitement, le type de données traitées, les finalités du traitement, la catégorie de destinataires des données.

La mise en place et l'actualisation régulière de ce registre sont obligatoires puisque c'est ce registre qui permettra à l'entreprise de démontrer qu'elle respecte ses obligations en cas de contrôle de la CNIL.

2. Etre en capacité de démontrer le respect de la réglementation

Les responsables du traitement doivent mettre en place des **mesures de protection des données appropriées**, afin de s'assurer que les données personnelles sont traitées de manière à garantir une sécurité et une confidentialité des données. **La charge de la preuve sera ainsi inversée**. Si la CNIL doit actuellement démontrer les manquements reprochés au responsable du traitement, à l'avenir, il appartiendra à celui-ci d'apporter la preuve qu'il est en conformité.

Pour **prouver sa conformité au règlement,** l'entreprise devra constituer, regrouper et mettre à jour la **documentation nécessaire** (registre, analyses d'impact préalable au traitement à risque, information des personnes et preuve du consentement, procédures internes, clauses contractuelles etc.).

Par ailleurs, en cas de violation de données, le responsable du traitement devra la notifier à la CNIL dans les **72 heures**. Une **information des personnes concernées** pourra être requise.

Il est donc nécessaire d'identifier la procédure à mettre en place pour identifier ces éventuelles violations et procéder à leur notification.

3. Assurer le droit des personnes dont les données sont collectées

Le RGPD **renforce l'information** des personnes qui doit être claire, intelligible et aisément accessible, et contenir de nouvelles mentions.

Lorsque le **consentement** de la personne est requis, il doit relever d'un acte positif et univoque de sorte que le consentement implicite (silence ou case précochée par défaut) ne sera pas valide.

Le RGPD instaure de **nouveaux droits** : droits à la portabilité des données, à l'oubli, et à la réparation du dommage subi.

4. Revoir les conditions contractuelles avec les sous-traitants

Les conditions dans lesquelles les services sont fournis par les **sous-traitants** (hébergement, maintenance etc.) doivent répondre aux exigences du RGPD (pseudonymisation, chiffrement des données, confidentialité, intégrité et disponibilité, résilience, disponibilité et accès...). Les engagements de ces derniers quant au **niveau de service** et **respect des délais** sont un **enjeu dans la négociation de ces contrats**.

Il est donc important de vérifier et d'éventuellement modifier les contrats conclus avec les sous-traitants pour vous assurer qu'ils soient conformes à cette nouvelle réglementation.

5. Désigner un délégué à la protection des données

Le délégué à la protection des données personnelles (**DPO**) a pour fonction de piloter et structurer les processus de gestion des données dans l'entreprise. Il remplace le CIL.

La désignation d'un DPO est **obligatoire** :

- lorsque les activités principales amènent le responsable de traitement ou le sous-traitant à réaliser un suivi régulier et systématique des personnes à grande échelle (par exemple : fourniture de services de télécommunications, email retargeting, profiling, suivi de la localisation, publicité comportementale, suivi des indicateurs de bien-être ou de santé via des objets connectés etc.)
- ou en cas de traitement à grande échelle de données sensibles

Le DPO doit être déclaré auprès de la CNIL.

L'échéance étant fixée au 25 mai 2018, **il est important d'anticiper dès aujourd'hui ce changement** afin de : cartographier vos données, mettre en place des processus et plateformes informatiques sécurisés, former vos collaborateurs, mettre à niveau les contrats avec vos sous-traitants, réaliser des audits pour vérifier votre conformité au regard des nouvelles directives etc.

N'hésitez pas à nous contacter si vous souhaitez être accompagnés dans cette mise en conformité.

tél. 01 40 49 02 19
www.cornillier-avocats.com