astura
AVOCATS À LA COUR

RGPD : ETES-VOUS PRETS ?

*Toute société présente en France, dans l'Union Européenne ou, plus largement, établie à l'étranger mais dont les activités sont dirigées vers un public situé dans l'Union Européenne est invitée à porter une attention particulière au règlement général sur la protection des données n°2016/679 (le « **RGPD** »).*

Le RGPD va entrer en vigueur le 25 mai 2018 dans l'ensemble des Etats de l'Union Européenne. Ce règlement remplace la directive européenne 95/46 relative à la protection des données personnelles et impacte par conséquent la loi française dite « Informatique et Libertés » du 6 janvier 1978 en instaurant de nouvelles obligations à la charge de toute personne morale ou personne physique traitant des données dans le cadre d'une activité autre que personnelle ou domestique.

Les entreprises veilleront à s'y conformer en temps utile, d'autant que le RGPD prévoit de lourdes sanctions avec des amendes administratives pouvant s'élever à 20 000 000 € ou 4% du chiffre d'affaires annuel mondial total de l'entreprise.

Vous trouverez ci-dessous une synthèse des principales obligations à mettre en place le 25 mai 2018 et qui nécessitent une préparation en amont.

1. OBLIGATION DE METTRE EN PLACE UN REGISTRE DES TRAITEMENTS

La plupart des obligations de notifications préalables auprès de la CNIL disparaissent. Sauf exceptions limitées, ces obligations de notifications préalables sont remplacées par l'obligation de tenir à jour un registre des traitements.

- En pratique, il convient d'identifier les traitements opérés par votre entreprise pour procéder à la constitution d'un registre les répertoriant.

- Cette démarche exige une coordination entre divers services de l'entreprise (IT, juridique, RH, marketing, …) qui devra être assurée par le DPO ou à défaut par un référent en données personnelles (voir point 2 ci-dessous).

2. OBLIGATION DE NOMMER UN DPO

De nombreuses entreprises vont être concernées par l'obligation de nommer un délégué à la protection des données (*data protection officer*, « **DPO** »). Il s'agit des entreprises dont les activités principales nécessitent :

- de traiter de manière régulière et systématique des données personnelles à grande échelle (telles que l'exploitation de sites de e-commerce ou la gestion de bases clients) ; ou
- de traiter des données sensibles (telles que les données de santé) à grande échelle.

- En pratique, le DPO doit être une personne nommée (cette dernière peut être interne ou externe à l'entreprise) et déclarée à la CNIL.

- Le DPO doit disposer de moyens nécessaires à sa mission et être associé à toute question relative à la protection des données personnelles, ce qui nécessite de prévoir une procédure de consultation du DPO sur tout projet impliquant un traitement de données personnelles.

A noter : même en l'absence d'obligation de désigner un DPO, la CNIL recommande de désigner une personne dédiée aux données personnelles afin de centraliser les informations sur les traitements de données personnelles et de coordonner les actions.

3. OBLIGATION D'IDENTIFIER LES RISQUES ET, LE CAS ECHEANT, DE MENER UNE ETUDE D'IMPACT SUR LA VIE PRIVEE (PIA)

Pour tous les traitements présentant un risque élevé au regard des droits et libertés des personnes concernées, les entreprises devront mener une étude d'impact sur la vie privée (*privacy impact assessment,* « **PIA** »).

- En pratique, cette exigence nécessite d'identifier les traitements présentant un risque élevé (par exemple, les *credit scoring*, les procédures de *due diligence* dans le cadre de la lutte anti-blanchiment ou encore les systèmes de monitoring des employés) et de préparer les PIA s'y référant.

4. OBLIGATION DE REVOIR SES CONTRATS AVEC LES SOUS-TRAITANTS

Le RGPD impose de nouvelles clauses dans tous les contrats liant les entreprises à des sous-traitants qui traitent des données personnelles.

- Il faut donc prévoir des avenants pour les contrats existants et intégrer dès que possible les clauses mises en conformité avec le RGPD pour les contrats en cours de négociation.

5. SE PREPARER AUX AUTRES OBLIGATIONS

Le RGPD impose de nombreuses autres obligations qui nécessitent de repenser en profondeur les procédures internes en matière de protection des données personnelles, comme la protection des données dès la conception et par défaut (privacy by design et privacy by default), les obligations de conseil imposées aux sous-traitants ou encore la mise en place de mesures de sécurité spécifiques selon le risque encouru.

La CNIL prend de très nombreuses initiatives pour préciser les nouvelles obligations du RGPD et aider les entreprises à s'y préparer. Elle propose notamment une méthodologie pour aider les entreprises à adapter leur processus, dont vous trouverez une synthèse en suivant ce lien : *https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes.*

A PROPOS D'ASTURA

Astura est un cabinet d'avocats indépendant spécialisé dans l'accompagnement des entreprises et de leurs dirigeants. Astura assiste notamment les entreprises pour leur

mise en conformité à la réglementation des données personnelles, la structuration de leurs flux transfrontières et la gestion des contrôles et procédures de la CNIL.

Plus particulièrement Astura est reconnu par Legal 500 dans les domaines suivants :

- **en technologies de l'information** : *Astura est 'un cabinet remarquable, comprenant parfaitement les besoins de ses clients et capable d'agir efficacement et rapidement dans des projets IT complexes'. Matthieu Mélin est recommandé pour 'son expertise, ses connaissances opérationnelles et sa capacité à défendre intelligemment les positions de son client'*

- **en propriété intellectuelle** : *Astura fournit un 'travail efficace et d'excellente qualité'. L'activité est dirigée par Matthieu Mélin qui possède 'une excellente expertise en matière de brevets et de contrats complexes' et 'prend grand soin de ses clients'.*

- **en fusion-acquisitions** : *'excellent, tant sur le plan du conseil que du relationnel', l'équipe possède 'une forte expérience de la représentation des groupes et investisseurs étrangers'. L'activité est dirigée par: Raphaël Dalmas qui 'est toujours concentré sur la recherche de solutions créatives'.*

CONTACTS

Matthieu Mélin
mmelin@astura.fr
T +33 (0)1 84 16 24 31

Raphaël Dalmas
rdalmas@astura.fr
T +33 (0)1 84 16 24 32

Clotilde Chabre
cchabre@astura.fr
T +33 (0)1 84 16 24 36

www.astura.fr