

## Convergences du droit et du numérique

### Contribution de Sarah Cadiot – Avocate en droit de la protection des données personnelles

Communauté d'appartenance : communauté juridique

#### **Sujet : Moins de Dix-Huit Moins pour se Préparer au Règlement Européen sur la Protection des Données Personnelles**

L'adoption du règlement européen sur la protection des données personnelles (le « [Règlement](#) ») par le Parlement européen le 14 avril 2016 constitue l'aboutissement de longues années de négociations et marque un tournant majeur dans la régulation des données personnelles, tant pour les individus que pour les entreprises.

Le Règlement conserve les principes clefs du droit de la protection des données personnelles prévus par la Directive 95/46/EC. Plus de 25 ans après l'adoption de la Directive, le Règlement modifie ces principes afin qu'ils n'appliquent plus logiquement aux technologies actuelles et, on peut l'espérer, aux technologies de demain. Le Règlement renforce les droits des individus concernant le traitement de données qui leur sont personnelles et, en cela, vient répondre à une demande croissante du public de plus de confiance et de maîtrise de ces données dans l'environnement numérique.

Le nouveau régime demande des efforts de mise en conformité significatifs aux entreprises traitant les données personnelles, quel que soit leur secteur d'activité. Le Règlement apporte un certain nombre de mesures visant à faciliter des obligations jusque-là fastidieuses, très formalistes, et souvent trop peu harmonisées au niveau européen. Néanmoins, ces obligations sont généralement plus importantes et seront soumises à un régime de sanctions financières que les législateurs européens ont volontairement voulu prohibitif, pouvant s'élever jusqu'à quatre pour cent du chiffre d'affaires mondial annuel d'une entreprise.

Les entreprises ont jusqu'au 25 mai 2018 pour se préparer, date à laquelle toutes les dispositions du Règlement entrent en vigueur. Moins d'un an et demi, c'est donc le temps qu'ont les entreprises pour se poser les bonnes questions et mettre en œuvre la bonne de stratégie de mise en conformité. C'est un délai qui peut paraître long mais qui, pour les entreprises, doit être utilisé afin de préparer une stratégie qui correspond à leurs besoins, leur capacité organisationnelle et leur public.

#### **Éléments de contribution**

Cette contribution vise à proposer des pistes d'analyse de questions clés soulevées par le futur cadre européen de la protection des données personnelles. Il s'agit de s'interroger sur les questions que les entreprises doivent garder à l'esprit pour la préparation à ces nouvelles obligations et restrictions.

Les éléments ci-dessous se sont pas une liste exhaustive des problématiques importantes soulevées par le Règlement et doivent être compris par chaque entreprise selon ses moyens, ses effectifs, et ses activités de traitement différemment.

➤ Droits des individus

Le Règlement ne crée qu'un seul nouveau droit – le droit à la portabilité des données – mais renforce de manière générale les droits des individus face aux entreprises traitant leurs données personnelles, ne serait-ce que par le montant des potentielles amendes et la mauvaise publicité que celles-ci peuvent apporter à une entreprise.

Ces droits, nombreux et tous connectés entre eux, demandent aux entreprises de s'organiser notamment au niveau humain, par exemple en mettant un place un protocole de prise en charge des questions et plaintes liées aux données personnelles, mais également au niveau technologique, pour s'assurer que les décisions liées à l'exercice de ces droits se traduisent par les actions nécessaires dans les bases de données.

➤ Principe d'*accountability*

C'est un des principes clés du Règlement, que la Commission Nationale de l'Informatique et des Libertés (CNIL) définit comme « l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données ».

Le Règlement vise à assouplir le système actuel de déclaration et autorisation préalables très contraignants qui s'effectue auprès de la CNIL. Il renverse la logique en demandant aux entreprises d'être les maîtres de leur propre conformité, mettant en place en système de contrôle *ex post* pour la plupart des cas de traitements de données personnelles. Apparemment plus simple et moins coûteux, ce nouveau régime demande un certain travail en interne aux entreprises, notamment de repenser leurs pratiques de gestion des données personnelles et de documenter ces pratiques.

➤ Obligations relatives à la transparence

Les législateurs européens ont compris que l'individu doit être tenu informé des traitements auxquelles sont soumises leurs données personnelles, et ont par conséquent décidé de renforcer les obligations de transparence. Ces obligations demandent des mises à jour aux entreprises, et permettent par la même occasion de repenser le rapport de l'entreprise à son public concernant le traitement des données.

➤ Responsabilités accrues du sous-traitant

La spécificité du droit européen de la protection des données personnelles a longtemps été la dichotomie entre responsable de traitement et sous-traitant dont le résultat est un régime d'obligations allégé pour ces derniers. Le Règlement conserve ces deux rôles mais accroît

considérablement les obligations imposées aux sous-traitants. Jusque-là relativement épargnés, ceux-ci vont devoir trouver les moyens de se mettre en conformité avec leurs nouvelles obligations.

➤ Sécurité des données

La sécurité des données et des opérations de traitement qui utilisent ces données est déjà inscrite dans les obligations de la Directive. Le Règlement voit plus loin et tape plus fort, demandent notamment aux entreprises d'informer la CNIL, et les individus concernés dans certaines situations des violations de données personnelles dans un délai de soixante-douze heures après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.