ARTICLE

RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES : QUELS CHANGEMENTS POUR LES PROFESSIONNELS ?

Protection des données I 25/01/2018 I Vincent Larrory

Adopté le 26 avril 2016 en vue de permettre à l'Europe de s'adapter aux nouvelles réalités du numérique, le nouveau règlement général sur la protection des données[1] (ci-après, « **RGPD** ») entrera en application le **25 mai 2018**. La mise en conformité au RGPD impose aux entreprises d'engager ou de poursuivre de nombreuses actions.

Champ d'application

Le RGPD aura vocation à s'appliquer aux **traitements de données à caractère personnel**, **automatisés ou non**[2], et effectués par un **responsable de traitement** ou par un **sous-traitant** établi **sur le territoire de l'Union européenne** (ci-après, « **UE** »)[3].

Si le responsable de traitement ou le sous-traitant **n'est pas établi en UE**, le règlement s'appliquera dès lors que les activités de traitement seront liées **à l'offre de biens ou de services à des personnes se trouvant sur le territoire de l'UE**, ou **au suivi du comportement de ces personnes**[4].

De nouvelles obligations pour les entreprises

- **Registre des activités de traitement**

Reposant sur une logique de responsabilisation, le RGPD prévoit désormais la tenue d'un **registre des activités de traitement de données personnelles** pour les entreprises **comptant plus de 250 salariés**[5].

Ce registre devra contenir des **informations nouvelles** qui viendront s'ajouter à celles figurant d'ores et déjà dans le registre tenu par le correspondant informatique et libertés.

Le registre devra notamment comporter des informations relatives aux **transferts de données** à caractère personnel **vers un pays tiers ou à une organisation internationale**.

- **Analyse d'impact relative à la protection des données**

Lorsqu'un **type de traitement**, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable de traitement devra effectuer une **analyse d'impact** des opérations de traitement envisagées sur la protection des données à caractère personnel.

---

1 Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

2 RGPD, article 2

3 RGPD, article 3

4 RGPD, article 3

5 RGPD, article 30

Cette analyse **consistera notamment à** :

- décrire clairement les opérations envisagées et les finalités du traitement ;
- évaluer les risques pour les droits et libertés des personnes concernées ;
- indiquer les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données.

Ainsi, le responsable de traitement devra désormais procéder lui-même à une évaluation de son projet préalablement à la mise en place du traitement.

En outre, sauf exceptions, le RGPD ne prévoit plus de demande d'autorisation auprès de l'autorité de contrôle pour la mise en œuvre des traitements les plus sensibles[6].

En cas de violation de données personnelles…

Le responsable de traitement devra désormais avertir la Commission nationale de l'informatique et des libertés (ci-après, « **Cnil** ») dans les meilleurs délais et, si possible, **72 heures au plus tard** après avoir pris connaissance, de toute violation de données à caractère personnel[7].

En cas de sous-traitance, le RGPD prévoit que le sous-traitant devra notifier au responsable du traitement toute violation de données à caractère personnel **dans les meilleurs délais après en avoir pris connaissance**.

RGPD : LES 6 ÉTAPES RECOMMANDÉES PAR LA CNIL

1. Désigner un pilote pour la gouvernance des données personnelles de votre structure ;
2. Cartographier les traitements de données personnelles ;
3. Prioriser les actions à mener ;
4. Gérer les risques en menant une analyse d'impact sur la protection des données ;
5. Organiser les processus internes, pour assurer un haut niveau de protection des données personnelles en permanence ;
6. Documenter la conformité en constituant et regroupant la documentation nécessaire.

---

6 RGPD, article 36

7 RGPD, article 33