GRALL & ASSOCIÉS AVOCATS

Antitrust Alliance

WHO'S WHO LEGAL WWL

Janvier 2018

Flash Concurrence n° 1

Règlement général relatif à la protection des données personnelles (RGPD) : Une nécessaire mise en conformité d'ici le 25 mai 2018

Par Nathalia Kouchnir-Cargill et Eléonore Camilleri

A compter du 25 mai 2018, soit dans seulement quatre mois à présent, entrera en vigueur le Règlement européen 2016/679/UE 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 » (ci-après « le RGPD ») lequel deviendra alors le droit applicable en la matière.

Il s'avère donc nécessaire pour les entreprises de se mettre en conformité avant cette date et ce, d'autant plus que ce texte renforce considérablement les sanctions pécuniaires que pourront prononcer les autorités de contrôle nationales, soit en France la CNIL.

- **Rappel du droit actuellement applicable**

En matière de données personnelles, le droit actuellement applicable en France est issu de la loi dite « *Informatique et libertés* » du 6 janvier 1978 (ci-après « *LIL* »).

Cette loi, ancienne, a été notamment modifiée par la loi du 6 août 2004 « *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* », qui a transposé en droit français la Directive 95/46/CE du 24 octobre 1995 « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ».

Plus récemment, la loi n° 2016-1321 du 7 octobre 2016 « *pour une République numérique* » (LRN) comporte un volet « *protection des données personnelles* » et a modifié la LIL du 6 janvier 1978 aux fins d'anticiper, mais seulement en partie, l'application en France du RGPD, notamment en augmentant déjà d'un cran les sanctions administratives pécuniaires applicables[1].

[1] En particulier, il résulte de la LNR que le plafond maximal des sanctions administratives pouvant être prononcées par la CNIL est passé de 150.000 euros antérieurement à 3 millions d'euros (ce sera encore augmenté avec le Règlement).

- **Entrée en application du RGPD à compter du 25 mai 2018**

A compter du **25 mai 2018**, le RGPD, qui est un texte à effet direct, abrogera la directive 95/46/CE et deviendra le droit applicable en la matière sur l'ensemble du territoire de l'UE et donc de la France.

Sa logique est la responsabilisation des entreprises et la suppression des formalités préalables auprès des autorités de contrôle (la CNIL en France). Il en résulte que sauf exception, il ne devrait plus y avoir de déclaration ou de demande d'autorisation préalable à la mise en place de traitements de données à caractère personnel.

En contrepartie, le Règlement introduit le principe du « ***privacy by design*** » qui impose aux entreprises de mettre en œuvre des mesures techniques et organisationnelles appropriées aux enjeux et aux droits des personnes dont les données sont traitées, dès la détermination des moyens du traitement, puis pendant le traitement.

En outre, le RGPD renforce sensiblement les sanctions que pourront prononcer les autorités de contrôle nationales.

En effet, la CNIL pourra, à compter du 25 mai 2018, prononcer des amendes administratives allant :

- jusqu'à **10 millions d'euros ou 2% du chiffre d'affaires mondial** de l'exercice précédent, en cas de non-respect des obligations prévues par le RGPD et des dispositions sur les codes de conduite et sur la certification,
- et jusqu'à **20 millions d'euros ou 4% du chiffre d'affaires mondial** de l'exercice précédent, en cas de non-respect des principes fondamentaux, des droits des personnes, des dispositions sur les transferts à l'étranger et des obligations liées aux traitements spécifiques.

- **Un projet de « *loi d'adaptation* » pour permettre l'application effective du RGPD en France**

Le RGPD est en principe applicable directement dans l'ensemble des Etats membres de l'Union à compter du 25 mai 2018, sans nécessiter de transposition en droit national.

Toutefois, le texte final du RGPD est le résultat d'un compromis, laissant coexister des dispositions harmonisées avec de multiples renvois aux droits nationaux. Les États membres conservent en conséquence de nombreuses marges de manœuvre (le Gouvernement français en a identifié 56).

Il en résulte que bien qu'il s'agisse en principe d'un texte d'effet direct, le RGPD va faire l'objet, en France, d'une prochaine loi et de décrets d'application.

C'est ainsi que le 13 décembre dernier, la Garde des Sceaux a présenté en Conseil des ministres le projet de loi relatif à la protection des données personnelles dont l'objet est d'adapter la loi « *Informatique et Libertés* » du 6 janvier 1978 aux dispositions du RGPD.

A ce titre et ainsi que l'a souligné la CNIL elle-même[2], on peut regretter le calendrier fort tardif retenu pour l'examen de ce texte eu égard à la date d'application du RGPD.

- **Une nécessaire mise en conformité des entreprises au RGPD en 10 points clés**

Afin d'être à jour le 25 mai 2018, date d'application du RGPD, les entreprises ont tout intérêt à d'ores et déjà se préparer en mettant en place les 10 mesures suivantes :

1. **Former** et **sensibiliser** les opérationnels et la direction sur les nouvelles obligations du Règlement et désigner le cas échéant un **pilote interne** chargé de la mise en conformité et d'assurer une protection des données en continu

[2] Dans sa délibération n° 2017-299 du 30 novembre 2017 portant avis sur un projet de loi d'adaptation au droit de l'Union européenne de la loi n°78-17 du janvier 1978 (demande d'avis n°17023753)

2. Réaliser un **audit des traitements** de données personnelles actuellement mis en œuvre ou envisagés, de leurs impacts et des risques associés

3. **Etablir un registre** des activités de traitement, contenant des informations sur chaque traitement mis en place

4. Sur la base de ce registre, **identifier les actions à mener** pour se conformer au droit des données personnelles

5. Réaliser une **analyse d'impact** (« *Privacy Impact Assessment* » ou « *PIA* ») pour chaque traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes

6. Mettre à jour/rédiger **la politique de confidentialité** du site internet de l'entreprise et **les mentions « *informatique et libertés* »** des emails de prospection

7. Insérer des **clauses "Données à caractère personnel"** adaptées dans les différents contrats de l'entreprise

8. Mettre en place des **procédures internes** de notification en cas de violation des données et d'information-type des personnes concernées

9. Préparer des **documents-types** de nature à s'assurer de la conformité au droit applicable en ce qui concerne les réponses aux demandes d'exercice des droits des personnes et la gestion des réclamations et plaintes

10. Constituer et **regrouper la documentation nécessaire** pour prouver la conformité de l'entreprise au Règlement en cas de contrôle de la CNIL

* * *

Afin d'accompagner au mieux ses clients dans le cadre de cette mise en conformité avec le RGPD, le Cabinet Grall & Associés propose des solutions adaptées aux besoins des entreprises selon l'importance des données traitées par elles et leurs domaines d'activités :

- **Première étape : Audit des traitements de données personnelles actuellement mis en œuvre ou envisagés par l'entreprise suivi de la rédaction d'un rapport d'état des lieux et des risques associés avec des préconisations de mise en conformité**

La première étape de la mise en conformité avec le RGPD consiste en la réalisation d'un audit, qui portera à la fois sur les traitements des données à caractère personnel actuellement réalisés ainsi que sur les futurs traitements de données que l'entreprise envisage de développer. Une fois les différents traitements identifiés, il sera possible d'appréhender très précisément les risques liés à chacune de ces opérations de traitement, actuelles ou envisagées par l'entreprise.

L'audit devra identifier les risques liés à la fois à la collecte et au traitement de données internes à l'entreprise, telles que les données des salariés des entreprises, et ceux liés au traitement de données externes à l'entreprise, telles que les données collectées auprès des distributeurs ou les données des consommateurs.

L'audit devra également identifier les cas de transfert de données en dehors de l'Union européenne.

- **Deuxième étape : Mise en place des outils de conformité**

Cette étape se décompose en trois sous-étapes :

- **Première sous-étape :** Rédaction d'une politique de confidentialité, de clauses « *Données à caractère personnel* » mais également « *Sécurité* », élaboration des mentions « *informatique et libertés* » adaptées au type de collecte.

- **Deuxième sous-étape :** Mise en place de procédures internes et de

documents types de nature à s'assurer de la conformité au droit applicable en ce qui concerne :

- les réponses aux demandes d'exercice des droits des personnes,
- la notification en cas de violation des données,
- l'information-type des personnes concernées,
- la gestion des réclamations et plaintes.

- **Troisième sous-étape le cas échéant selon les besoins de l'entreprise :** la création d'un registre des activités de traitements, l'organisation juridique du transfert de données hors UE, la réalisation d'études d'impact, la mise en place d'un DPO, la certification des traitements de données, l'adhésion à des codes de bonne conduite par secteur et en fonction des besoins de l'entreprise et selon sa taille

Parallèlement, le Cabinet propose des formations pour sensibiliser les opérationnels et la direction sur les nouvelles obligations du RGPD

Afin de respecter l'ensemble des règles prévues par le RGPD et compte tenu des sanctions encourues, la Cabinet Grall & Associés propose des modules de formation pour sensibiliser le personnel et les membres de la direction de l'entreprise.

GRALL & ASSOCIÉS AVOCATS

Antitrust Alliance

WHO'S WHO LEGAL WWL

Êtes-vous inscrit à la prochaine formation

GRALL INSTITUTE

FORMATIONS 2018

Positionnement du prix de vente / revente et droit de la concurrence

- Le 2 février 2018

Voir le détail de cette formation

Les enquêtes de concurrence diligentées par les services de la DGCCRF, de l'autorité de la concurrence, et par la Commission européenne

- Le 7 février 2018

Voir le détail de cette formation

L'essentiel du droit du commerce électronique : la vente en ligne en 10 points clés

- Le 15 février 2018

Voir le détail de cette formation

Contact

63, avenue de Villiers

75017 Paris - Palais P 40

+33 (0)1 53 57 31 70

contact@grall-legal.fr

www.grall-legal.fr