astura
AVOCATS À LA COUR

RGDP : RENFORCEMENT DES OBLIGATIONS DU SOUS-TRAITANT – LE GUIDE DE LA CNIL

*Le règlement général sur la protection des données n°2016/679 (le « **RGDP** »), qui entrera en vigueur le 25 mai 2018, instaure de nouvelles obligations à la charge de toute personne morale ou physique traitant des données personnelles.*

Alors que le régime actuel n'imposait des obligations qu'au seul responsable de traitement, le RGDP impose également et désormais directement des obligations au sous-traitant.

Tout prestataire de service qui traite des données personnelles pour ses clients est ainsi contraint de respecter un certain nombre d'obligations conformément au RGDP.

*La Commission Nationale de l'Informatique et des Libertés (la « **CNIL** ») a publié un guide le 29 septembre dernier précisant ce qu'est un sous-traitant en pratique et détaillant les obligations et mesures qu'il doit prendre. Voici une synthèse des points essentiels à retenir pour permettre au sous-traitant de se conformer à ses nouvelles obligations.*

1. QUI EST CONCERNE ?

Le RGDP suit la règlementation actuelle en matière de données personnelles selon laquelle un sous-traitant est celui qui traite des données personnelles pour le compte et sur instruction du responsable de traitement. La CNIL donne quelques exemples pratiques, parmi lesquels :

- les prestataires de maintenance et d'hébergement ;
- les intégrateurs de logiciels ;
- les sociétés de sécurité informatique ;
- les SSII ;
- les agences de marketing ou de communication qui traitent des données pour le compte de clients.

2. MODELE DE CLAUSE A INSERER DANS LES CONTRATS ENTRE RESPONSABLE DE TRAITEMENT ET SOUS-TRAITANT

Le RGDP impose de nouvelles clauses qui doivent figurer dans tous les contrats entre les responsables de traitements et les sous-traitants.

Il convient d'intégrer lesdites clauses dans votre politique contractuelle pour les contrats à venir et de prévoir des avenants pour les contrats existants afin que ces derniers soient en conformité avec le RGDP au 25 mai 2018.

Pour faciliter cette tâche, la CNIL propose un modèle assez complet dans son guide et le G29 (le groupe des CNIL européennes) doit adopter des clauses contractuelles types.

3. TENUE DES REGISTRES

La CNIL rappelle que tout sous-traitant doit tenir un registre détaillant les traitements effectués sur les données pour le compte de son client (catégories de traitements effectués, coordonnées des clients, éventuels transferts hors Union Européenne).

La CNIL précise par ailleurs que le prestataire sous-traitant n'en reste pas moins responsable de traitement pour ce qui concerne les activités qui lui sont propres (RH, gestion de sa propre clientèle, etc.).

Le prestataire devra donc tenir deux registres distincts : l'un pour les données personnelles qu'il traite pour son propre compte en tant que responsable de traitement, l'autre pour les données personnelles qu'il traite pour le compte de ses clients en tant que sous-traitant.

4. NOMMER UN DELEGUE A LA PROTECTION DES DONNEES (« DPO »)

Le RGDP impose au responsable de traitement comme au sous-traitant de nommer un DPO. Cette obligation est applicable aux entreprises dont les activités principales nécessitent (i) 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 (ii) de traiter des données sensibles (telles que les données de santé) à grande échelle.

Le G29 suggère pour sa part, dans ses lignes directrices adoptées le 5 avril 2017, que le DPO du prestataire soit chargé non seulement de contrôler les activités du prestataire lorsqu'il traite des données en tant que sous-traitant, mais également lorsqu'il traite des données pour son compte en tant que responsable de traitement (RH, gestion de sa propre clientèle, etc.).

Dans tous les cas, la CNIL recommande de nommer un DPO même si le sous-traitant n'est pas contraint de le faire afin de disposer d'un expert dédié en matière de protection de données personnelles et de piloter la conformité au RGDP.

5. ASSISTER LE CLIENT DANS LA MISE EN ŒUVRE DU TRAITEMENT

La CNIL précise le rôle du sous-traitant dans ses obligations d'information et d'assistance. Ainsi, le sous-traitant devra notamment :

- aider le client à permettre aux personnes concernées d'exercer leurs droits (accès, rectification, effacement, portabilité, opposition, ne pas faire l'objet d'une décision individuelle) ;

- aider le client à réaliser une analyse d'impact (« **PIA** »), la réalisation du PIA en tant que telle relevant de la responsabilité du client ;

- informer le client si, selon lui, une instruction du client constitue une violation des règles en matière de protection des données personnelles. A cet égard, nous recommandons de veiller à limiter cette obligation à une obligation d'information et non de conseil, le sous-traitant n'étant pas un conseil juridique.

6. ALERTER LE CLIENT EN CAS DE FAILLE DE SECURITE

Le sous-traitant doit notifier au client toute violation de données personnelles dans les meilleurs délais après en avoir pris connaissance.

Le client devra ensuite, si nécessaire, notifier à l'autorité compétente et communiquer aux personnes concernées cette violation. A cet égard, la CNIL indique que le client peut également demander au sous-traitant qu'il effectue cette notification et cette communication pour son compte. D'un point de vue juridique, cette mission du sous-traitant pourrait être encadrée par mandat, en vertu duquel le sous-traitant représente le client en son nom et pour son compte.

7. OBTENIR L'ACCORD DU CLIENT EN CAS DE SOUS-TRAITANCE ULTERIEURE

Le sous-traitant doit obtenir l'autorisation du client s'il sous-traite les missions confiées par le client à un autre sous-traitant. Cette autorisation peut être accordée à un sous-traitant particulier ou être donnée de manière générale. Dans ce cas, le sous-traitant devra informer le client, qui pourra formuler des objections, de tout changement de sous-traitant. Nous ajoutons que, quel que soit le cas de figure, un agrément du client sera nécessaire aux fins de respecter la loi du 31 décembre 1975 relative à la sous-traitance.

La CNIL rappelle que le sous-traitant reste pleinement responsable vis-à-vis de son client de l'exécution par les sous-traitants ultérieurs de leurs obligations.

8. PRENDRE EN COMPTE LE *PRIVACY BY DESIGN* ET *PRIVACY BY DEFAULT*

Le sous-traitant doit mettre à la disposition du client des outils qui lui permettent de respecter le principe de protection des données dès la conception (« *privacy by design* ») et par défaut (« *privacy by default* »). La CNIL donne des exemples pratiques des fonctionnalités de ces outils, qui peuvent notamment :

- permettre au client de paramétrer par défaut et a minima la collecte de données et ne pas rendre techniquement obligatoire le renseignement d'un champ facultatif ;
- ne collecter que les données strictement nécessaires à la finalité du traitement ;
- purger automatiquement et sélectivement les données d'une base active à l'issue d'une certaine durée ;
- gérer des habilités et droits d'accès informatiques donnée par donnée.

9. RISQUES EN CAS DE NON-RESPECT DES OBLIGATIONS INCOMBANT AU SOUS-TRAITANT

La CNIL rappelle que le non-respect du RGDP peut s'élever jusqu'à 10 ou 20 millions d'euros ou jusqu'à 2% ou 4% du chiffre d'affaire annuel mondial d'une entreprise et donne des exemples qui pourraient s'appliquer au sous-traitant, parmi lesquels :

- le fait d'agir en dehors des instructions du responsable de traitement ;
- le fait de ne pas informer le responsable de traitement qu'une instruction constituerait une violation du RGDP ;
- le fait de sous-traiter sans autorisation préalable du responsable de traitement ;
- le fait de ne pas tenir de registre des traitements.

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 et les investisseurs dans la conduite de leurs opérations de croissance et de développement domestiques ou internationales.

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

- **en technologies de l'information** : *Astura est 'l'un des meilleurs rapports qualité/prix' du marché en termes de qualité d'expertise et de service. Les avocats 'connaissent réellement les technologies de l'information' et conseillent plusieurs grandes entreprises françaises et internationales dans le cadre de la négociation d'importants contrats informatiques, ainsi que dans la gestion du contentieux et des sujets de données personnelles. Matthieu Mélin compte parmi 'les meilleurs spécialistes' de la place.*

- **en fusion-acquisitions** *: 'Astura offre 'un niveau de prestation exceptionnel', le cabinet s'illustre par 'la grande expérience internationale de ses avocats, leur niveau de réactivité et leur 'capacité à délivrer des conseils sur-mesure', l'équipe 'a l'habitude de travailler pour des sponsors internationaux et comprend les fondamentaux d'un deal et les attentes de ce type de clients', à la tête de l'activité, Raphaël Dalmas est 'extrêmement réactif, adaptable et saisit parfaitement les attentes de ses clients''.*

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