

LA CNIL LANCE UNE CONSULTATION SUR TROIS THÈMES D'INTERPRÉTATION DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Date: 13 March 2017

Privacy, Data Protection and Information Management Alert

By: Claude-Étienne Armingaud, Clémence Marolla, Etienne Drouard

Le 23 février 2017, la Commission Nationale de l'Informatique et des Libertés (« **CNIL** ») a lancé une consultation publique sur trois thèmes : la notification de violation de données à caractère personnel, le profilage et le consentement. Toutes les entités intéressées sont invitées à y participer jusqu'au 23 mars 2017. La consultation est accessible à l'adresse suivante : <https://www.cnil.fr/fr/consultation-reglement-europeen>.

Cette nouvelle série de consultations s'inscrit dans le prolongement de celles lancées par la CNIL de juin à juillet 2016 sur le délégué à la protection des données, la portabilité des données, les études d'impact sur la vie privée et la certification de la conformité.

Ensemble, elles ont vocation à aider la CNIL à analyser les questions des justiciables (entreprises, particuliers, administrations) interpréter les dispositions du Règlement Général pour la Protection des Données à caractère personnel (« **RGDP** ») dont l'application interviendra le 25 mai 2018, à la lumière des impacts pressentis par les différents acteurs concernés.

NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL

L'article 33 du RGDP introduit une obligation générale de notification des violations de données à caractère personnel. Ainsi, en cas de faille de sécurité susceptible de porter atteinte aux droits et libertés des personnes, le responsable du traitement aura l'obligation de notifier cette violation à l'autorité de protection des données compétente ainsi qu'aux personnes concernées. En outre, le RGDP présume notamment qu'une notification aux personnes concernées n'est pas nécessaire lorsque le responsable de traitement avait appliqué des mesures de protection techniques et organisationnelles, telles que le chiffrement, aux données concernées par la violation.

Les contours d'une telle obligation pourraient gagner à être précisés, à commencer par l'entité qui sera chargée d'effectuer cette notification. Ainsi, dans le cas où une société appartient à un groupe, quelle entité devra porter la charge de cette notification et, avec elle, supporter les conséquences médiatiques qui ne manqueront pas d'en découler ?

Dans le cadre des notifications aux personnes concernées, la CNIL souhaite recueillir l'avis des acteurs impliqués pour mieux définir la notion de « *risque pour les droits et libertés des personnes physiques* » absente du RGDP. De même, l'exception à l'obligation de notification lorsque le responsable du traitement a mis en œuvre des mesures de chiffrement n'est pas davantage précisée puisque le RGDP ne définit pas quels procédés de chiffrement sont considérés comme satisfaisants.

De telles clarifications sont néanmoins indispensables afin de permettre aux organismes privés ou publics, responsables de traitement ou sous-traitants, de se conformer à leurs obligations.

PROFILAGE

Le profilage est défini à l'article 4 du RGDP comme « toute forme de traitement de données à caractère personnel permettant d'analyser ou prédire des éléments concernant une personne, comme les préférences personnelles, le déplacement, la situation économique ou encore, le comportement ».

L'article 22 du RGDP prévoit que la personne disposera d'un droit d'opposition à ce qu'un tel dispositif de profilage soit mis en œuvre à son égard si ce dernier « produit des effets juridiques la concernant ou l'affect[e] de manière significative ».

Malgré l'uniformisation promise par le RGDP, chaque régulateur national devra donc définir précisément les pratiques des entreprises qui entrent dans ce régime du profilage. C'est sur ce point que la CNIL souhaite recueillir les avis des professionnels du secteur puisque les notions d'« effets juridiques » ou d'« affecter de manière significative » sont particulièrement floues. Ainsi, en l'absence de règles directrices européennes, l'objectif d'harmonisation du RGDP pourrait être compromis dès lors qu'il n'est pas certain que l'ensemble des CNIL européennes adoptent la même interprétation.

La CNIL soulève également, parmi d'autres, la question de l'intégration du principe de « privacy by design and by default » dans la mise en œuvre du profilage et interroge les contributeurs sur les limites du profilage, en particulier sur l'opportunité d'exclure certains types d'informations de son champ d'application. Une telle exclusion reviendrait à proscrire certaines activités de profilage, alors que le RGDP ne prévoit aucune exclusion de principe.

CONSENTEMENT

D'après l'article 4 du RGDP, le consentement constitue « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Cette question de la définition du consentement est primordiale : elle permettra de donner une base légale à certains types de traitements, notamment s'agissant du traitement de données dites « sensibles ».

Ainsi, les concepts de « déclaration » ou d'« acte positif clair » devront être clarifiés. La voie d'une case à cocher est-elle la seule option possible ? Ou la volonté de la personne concernée de s'inscrire par une démarche active à un service tout en étant suffisamment informée serait-elle suffisante à caractériser un acte positif clair ?

En outre, quelles dispositions le responsable devra-t-il prendre en considération lorsque la personne concernée retire son consentement ?

Ce sont autant de questions sur lesquelles les professionnels de tous les secteurs sont sollicités pour apporter leurs éclairages à la CNIL afin que la transposition concrète des principes posés par le GDPR ne vienne pas compromettre leur activité économique.

Si le débat est ouvert en France, il ne manquera pas d'affecter l'ensemble des acteurs concernés, non seulement ceux situés dans l'Union Européenne, mais également ceux situés hors de l'Union européenne destinant des biens ou services aux consommateurs européens ou procédant à l'analyse du comportement de ces personnes, lorsque ce comportement a lieu au sein de l'Union.

A quatorze mois de l'applicabilité directe du RGDP dans tous les États membres, les questions qui demeurent sans réponse précise sont inquiétantes tant elles sont structurantes et liées à des niveaux de sanctions lourdes (jusqu'à 4% du chiffre d'affaires annuel mondial) pour les entreprises.

Dans ce compte à rebours qui presse les régulateurs à dégager des règles claires d'interprétation, les consultations en cours sont quasiment aussi importantes qu'un débat parlementaire, sans que les rapports de force ne soient aussi lisibles que dans un débat démocratique.

KEY CONTACTS



CLAUDE-ÉTIENNE ARMINGAUD

PARTNER

PARIS

+33.1.58.44.15.16

CLAUDE.ARMINGAUD@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.