Nomos
société d'avocats

nomosnetcom.fr **Décembre 2017**

Le G29 publie son projet de lignes directrices sur la notification des violations de données

[DONNEES PERSONNELLES]
Projet de lignes directrices sur la notification des violations de données, adopté le 3 octobre 2017

La notification des violations de données à caractère personnel est une des nouvelles obligations les plus commentées du Règlement Général sur la Protection des Données (« RGPD »), qui entrera en application dans moins de six mois, le 25 mai 2018. En octobre, le G29 a publié son projet de lignes directrices afin de guider la mise en conformité des responsables de traitement.

En vertu des articles 33 et 34 du RGPD, les responsables de traitement seront dans l'obligation de notifier à l'autorité de contrôle compétente, 72 heures au plus tard après en avoir pris connaissance, toute violation de données à caractère personnel présentant un risque pour les droits et libertés des personnes concernées. Lorsque le risque est élevé, les responsables devront également informer les personnes concernées.

Les lignes directrices du G29 s'articulent autour de cinq thèmes :

(1) **Notion de violation de données** : la définition générale donnée à l'article 4(12) du RGPD ne suffit pas forcément à appréhender et qualifier chaque situation en pratique. Le G29 propose de classer les violations en trois catégories :

- Atteinte à la confidentialité : il s'agit des situations les plus médiatisées, celles où les données sont accessibles où divulguées aux tiers sans autorisation, le cas échéant de manière accidentelle.

- Indisponibilité : cela recouvre les cas où les données sont détruites en tout ou partie, mais également où les données ne sont temporairement plus accessibles, même pour une très courte période dès lors que cela entraine des risques (ex : inaccessibilité de données médicales nécessaires à une décision urgente).

- Atteinte à l'intégrité : il s'agit des cas où les données sont modifiées sans autorisation, le cas échéant de manière accidentelle.

(2) **La qualification des niveaux de risque pour les droits et libertés des personnes concernées** : l'obligation de notifier une violation, et le cas échéant d'informer les personnes concernées, varie en fonction de la qualification du niveau de risque pesant sur les droits et libertés des personnes concernées.

Une des difficultés principales pour les responsables de traitement est donc d'être en mesure de faire cette évaluation. Le G29 recommande l'utilisation de sept critères : (i) le type de violation ; (ii) la nature, la sensibilité et le volume de données violées ; (iii) la capacité à identifier les personnes concernées facilement ; (iv) la gravité des conséquences pour les personnes affectées ; (vi) les caractéristiques spécifiques des personnes affectées ; (v) le nombre de personnes affectées ; et (vi) les caractéristiques spécifiques du responsable de traitement.

Dans son avis, le G29 détaille chacun de ces critères et la manière dont ils doivent être utilisés. Surtout, une liste de cas de violation types et des obligations de notification et d'information correspondantes est fournie en annexe.

(3) **Le moment où le responsable de traitement doit notifier** : en vertu de l'article 33 du RGPD, le responsable de traitement doit notifier les violations au plus tard 72 heures après en avoir eu « connaissance ».

Le G29 estime que la « connaissance » du responsable de traitement est établie dès lors que celui-ci dispose d'un « degré raisonnable de certitude » qu'un incident de sécurité s'est produit et que des données personnelles sont concernées. Surtout, le G29 estime que le responsable de traitement doit être présumé avoir connaissance de la violation au même moment que son sous-traitant, alors même que ce dernier peut parfois tarder à informer le responsable.

Cependant, le G29 précise qu'une rumeur ou une information parue dans la presse ne caractérise pas nécessairement la connaissance par le responsable de traitement. Celui-ci garde la possibilité de mener des investigations préalables afin de confirmer ou non l'information.

(4) **La communication aux personnes concernées** : par principe, la communication aux personnes concernées devra être effectuée directement et individuellement (par email, SMS etc.) et distinctement de toute autre information. Lorsque cela est impossible, le responsable devra tout de même s'assurer qu'il exploite tous les canaux de communication utiles. Un simple communiqué de presse ne devrait pas être suffisant.

Le G29 précise également que les autorités de protection pourront indiquer aux responsables de traitement s'il convient ou non d'informer les personnes concernées, confortant ainsi l'analyse du niveau de risque.

(5) **L'obligation de documenter toute violation** : la tenue d'un registre relatif aux violations de données fait partie intégrante de l'obligation générale dite « *d'accountability* ». Le G29 insiste ici sur le fait que toutes les violations doivent être répertoriées, même celles qui ne nécessitent pas d'être notifiée aux autorités.

La documentation des événements liés aux incidents de sécurité est susceptible de justifier d'éventuels retards de notification aux autorités (au delà du délai de 72 heures).

Le projet de lignes directrices était ouvert aux commentaires jusqu'au 28 novembre 2017, et va à présent pouvoir être finalisé par le G29 pour son adoption définitive.

Sylvain NAILLAT