LE RÉGIME JURIDIQUE DES ANALYSES D'IMPACT SUR LA PROTECTION DES DONNÉES

Par Élise Humbert, avocate au cabinet Seban & Associés

Qu'est-ce qu'une analyse d'impact sur la protection des données ?

Si aucune définition précise de la notion d'analyse d'impact sur la protection des données ne ressort du texte même du Règlement général sur la protection des données (RGPD), les lignes directrices adoptées par le G29 le 4 avril 2017 et précisément dédiées à cet outil nouveau la présente comme « un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au traitement de données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face ».

De façon générale, il peut être retenu qu'il s'agit du travail, réalisé en amont de la mise en œuvre d'un nouveau traitement, de confrontation approfondie des bénéfices d'un traitement, des risques qu'il est susceptible de faire peser sur le droit à la vie privée des personnes concernées et des moyens permettant de les limiter.

Dans quelles hypothèses une analyse d'impact sur la protection des données est-elle obligatoire ?

L'article 35 du RGPD prévoit qu'une analyse d'impact sur la protection des données est requise lorsqu'il apparaît qu'un traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

Dès lors, la CNIL précise sur son site Internet que sont en principe concernés par une telle obligation les traitements qui remplissent au moins deux des critères suivants : évaluation/scoring (y compris le profilage), décision automatique avec effet légal ou similaire, surveillance systématique, collecte de données sensibles ; collecte de données personnelles à large échelle, croisement de données ; personnes vulnérables (patients, personnes âgées, enfants, etc.), usage innovant (utilisation d'une nouvelle technologie), exclusion du bénéfice d'un droit/contrat.

En tout état de cause et conformément au point 4 de l'article 35 du RGPD, il appartiendra à la CNIL d'établir et de publier, dans les meilleurs délais, une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données devra être effectuée.

Dans quelles hypothèses une analyse d'impact sur la protection des données n'est pas nécessaire ?

Une analyse d'impact sur la protection des données n'est pas nécessaire dans les hypothèses suivantes :

- lorsque le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées,
- lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel une analyse d'impact sur la protection des données a déjà été menée et, sous certaines conditions,
- lorsque le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public.

La CNIL s'est engagée à adopter courant 2018 la liste de ces exceptions, étant précisé qu'à l'inverse des traitements pour lesquels une analyse d'impact sur la protection des données est requise, le RGPD ne la contraint pas à publier une telle liste.

Comment devra être réalisée une analyse d'impact sur la protection des données ?

À titre liminaire, il sera rappelé que c'est au responsable de traitement qu'il incombe de diligenter l'analyse d'impact sur la protection des données (soit la personne, l'autorité publique, le service ou l'organisme qui a déterminé les finalités et les moyens du traitement). Lorsqu'un délégué à la protection des données (DPD) a été désigné, le responsable du traitement doit néanmoins solliciter ses conseils avisés dans la réalisation de cette analyse.

Concrètement, l'analyse d'impact sur la protection des données devra être menée selon une méthodologie précise, laquelle a d'ores et déjà donné lieu à l'édition d'un guide disponible sur le site de la CNIL, auquel il convient donc de se référer et décliné selon quatre étapes successives : l'étude du contexte, l'étude des principes fondamentaux, l'étude des risques liés à la sécurité des données, et enfin la validation de l'analyse d'impact.

La CNIL a également mis à disposition sur son site Internet, pour accompagner les professionnels dans leurs analyses d'impact sur la protection des données, un logiciel gratuit permettant de les réaliser plus aisément.

Quelles sont les suites à donner à la réalisation d'une analyse d'impact sur la protection des données ?

L'essence même d'une analyse d'impact sur la protection des données tient à ce que toutes les mesures susceptibles de limiter les risques sur la vie privée puissent être adoptées avant que l'opération de traitement de données soit effectivement déployée et maintenues durant toute sa durée de vie.

Ce faisant, pour exemples, parmi les mesures de sécurité adéquates ayant vocation à être mises en œuvre, pourront figurer des mesures organisationnelles (procédure de contrôle, limitation du nombre de destinataires, pseudonymisation, code de bonne conduite, etc.) et des mesures techniques (sécurisation du système d'information, authentification et contrôle des accès, sécurisation des objets nomades, etc.).

En principe, ces analyses d'impact sur la protection des données ne sont soumises à aucune formalité de publicité ou de transmission préalable à leur exécution. Cependant, dans certaines hypothèses, ces analyses devront obligatoirement être transmises à la CNIL, avant le déploiement du traitement, lorsqu'il ressort des conclusions de ces analyses que le niveau de risque résiduel reste élevé ou quand la législation d'un État membre l'exige et, après le déploiement du traitement, en cas de contrôle de la CNIL.

Quelles sont les sanctions en cas de manquement aux dispositions du RGPD relatives aux analyses d'impact sur la protection des données ?

Conformément au paragraphe 4 de l'article 83 du RGPD, en cas de violation des obligations afférentes aux analyses d'impacts sur la protection des données, le responsable de traitement encourt une amende pouvant s'élever jusqu'à 10 000 000 € ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Avant l'application d'une telle sanction, une procédure contradictoire sera néanmoins respectée et d'autres mesures moins répressives pourront être appliquées (rappel à l'ordre, injonction, interruption provisoire de la mise en œuvre du traitement, limitation du traitement de certaines données, etc.).

Pour davantage de précisions sur la procédure de sanction, il conviendra de se référer au chapitre VII de la loi n° 78-17 du 6 janvier 1978 tel que modifié par la loi relative à la protection des données personnelles.

Dans quel délai devront être réalisées ces analyses d'impact sur la protection des données ?

La CNIL a annoncé qu'elle concédait un délai de trois ans suivant l'entrée en application du RGPD aux responsables de traitement pour réaliser une analyse d'impact sur la protection des données pour tous les traitements en cours régulièrement mis en œuvre et ayant, soit fait l'objet d'une formalité préalablement auprès de la CNIL avant le 25 mai 2018, soit été consignés au registre d'un correspondant « informatique et libertés ».

En revanche, elle a rappelé expressément qu'une telle analyse devait être réalisée sans délai, dans tous les autres cas, soit dès lors qu'un traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques » et que, soit il n'a jamais fait l'objet de formalités préalables auprès de la CNIL, soit il a fait l'objet d'une modification significative depuis l'accomplissement de cette formalité, soit il est mis en œuvre après le 25 mai 2018. ●

Article 35 du RGPD

Nouveauté instituée par l'article 35 du Règlement général sur la protection des données (RGPD) n° 2016/679 du 27 avril 2016, entré en vigueur le 25 mai 2018, l'analyse d'impact sur la protection des données (aussi connue sous l'acronyme anglophone DPIA) constitue un pilier important de la logique de responsabilisation impulsée par le règlement européen, qui suscite aujourd'hui plusieurs interrogations pratiques.