Le nouveau règlement général de protection des données à caractère personnel (RGPD)[1]

Le 27 avril 2016, a été signé le nouveau règlement européen relatif à la protection des données à caractère personnel[2], destiné à remplacer la directive 95/46/CE[3]. La matière de la protection des données à caractère personnel, qui constitue un pan de la protection de la vie privée, est aussi dense que complexe. Les domaines touchés par les données à caractère personnel dans les Pouvoirs locaux sont vastes : données à caractère fiscal, données issues du registre national ou de la banque-carrefour de la sécurité sociale, données issues du développement économique local ou encore les données relatives au personnel employé par le pouvoir local quel qu'il soit.

Ce règlement, entré en vigueur le 24 mai 2016, doit être mis en œuvre dans les États membres depuis le 25 mai 2018. L'on notera principalement que c'est la loi du 30 juillet 2018, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, qui est venue compléter ce règlement européen et qui est directement applicable en droit belge, sans acte de transposition.

Après un rappel des notions élémentaires, nous passerons en revue quelques évolutions réglementaires issues du RGPD.

Au titre de prémisse, il convient de rappeler les éléments suivants, qui constituent les notions triangulaires de la réglementation :
- la notion de *donnée à caractère personnel* : toute information se rapportant à une personne physique identifiée ou identifiable, telle que le nom ou un numéro d'identification ; la personne concernée est la personne dont on effectue le traitement de données à caractère personnel ;
- la notion de *traitement de données* à caractère personnel : toute opération ou ensemble d'opérations appliquées à des données, telle que la collecte ou la transmission[4] ;
- la notion de *responsable de traitement* : il s'agit de la personne, physique ou morale, l'autorité publique qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[5].

1. Évolution de la protection et des droits de la personne concernée

Les données à caractère personnel ne peuvent être utilisées, c'est-à-dire traitées, de manière libre puisqu'elles constituent un aspect de la vie privée des personnes physiques que cette réglementation tend à protéger.

Pour répondre au principe de licéité des traitements des données à caractère personnel, l'une des hypothèses de traitement licite est celle du consentement donné par la personne dont on traite les données à caractère personnel. Ce consentement est défini comme étant la manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration

---

1 Fiche rédigée par M.-L. Van Rillaer, Conseiller UVCW.

2 Ci-après, le règlement ; règl./CE 2016/679 du Parlement européen et du Conseil du 27.4.2016 rel. 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 dir. 95/46/CE, *J.O.U.E.*, 4.5.2016.

3 Dir. 95/46/CE du Parlement européen et du Conseil du 24.10.1995 rel. à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.U.E.*, 23.11.1995, transposée en droit belge par la L. 8.12.1992 rel. à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18.3.1993.

4 Règl./CE, art. 4, 2).

5 Règl./CE, art. 4.7).

ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement[6].

Le nouveau règlement augmente les droits de la personne dont on traite les données à caractère personnel. L'on dénombre les six droits suivants : droit d'accès, droit à la rectification, droit à l'effacement, droit à la limitation, droit à la portabilité des données et droit de ne pas faire l'objet d'un profilage.

L'on rappellera utilement que les autorités publiques légitimisent plutôt rarement les traitements de données par le consentement, car elles agissent dans le cadre de leurs missions cadrées réglementairement et traitent donc, dans la majorité des cas, des données à caractère personnel, soit en vertu d'une obligation légale qui leur incombe, soit en raison de l'exécution d'une mission d'intérêt public ou de l'exercice de leur autorité publique[7].

2. Responsabilisation accrue des acteurs et protection des données, dès la conception et par défaut

Le règlement institue un principe de responsabilité accrue puisque le responsable de traitement se voit désormais contraint non seulement de respecter la réglementation, mais aussi de démontrer ce respect[8]. Il doit donc mettre en place une politique proactive de protection des données par la mise en œuvre de mesures techniques et organisationnelles, compte tenu de l'état des connaissances, des coûts de mise en œuvre, de la nature, de la portée, du contexte, des finalités du traitement, ainsi que des risques pour les droits et libertés des personnes physiques[9].

Suite logique du principe de proportionnalité, celui de protection des données dès la conception, et par défaut, est désormais formellement inscrit dans le règlement[10]. Il exige que la protection des données soit intégrée dès la conception d'un projet impliquant le traitement de données à caractère personnel, et que le responsable de traitement garantisse, par défaut, que seules les données à caractère personnel, qui sont nécessaires au regard de chaque finalité spécifique du traitement, soient traitées. Autrement dit, la protection des données à caractère personnel n'est pas une « couche à rajouter », mais fait partie intégrante de la manière dont un projet doit être mené.

Le responsable de traitement a, du fait du nouveau règlement, l'obligation de tenir un registre des activités de traitement[11], et ce en lieu et place de l'obligation de notification préalable des traitements (jugée inefficace) à l'autorité de contrôle[12]. Ce registre est un outil précieux permettant à la fois de connaître les traitements effectués et leurs composantes, de vérifier la légalité et la proportionnalité de ceux-ci, de garantir les droits des personnes concernées et d'améliorer la gouvernance des données.

Le règlement prévoit la réalisation d'une étude d'impact « *lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques* »[13]. Cette étude doit également être établie lorsque, notamment, il y a traitement à grande échelle de catégories particulières de données sensibles.

Les responsables de traitement qui sont des autorités publiques ou des organismes publics doivent désigner un délégué à la protection des données[14]. Il est, entre autres, chargé d'informer et de

6 Règl./CE, art. 4.11).
7 Règl./CE, art. 6, § 1, c) et e).
8 Règl./CE, art. 5.2.
9 Règl./CE, art. 25.1.
10 Règl /CE, art. 25.
11 Règl./CE, art. 30.1.
12 L. 8.12.1992, art. 17 et ss.
13 Règl./CE, art. 35.1.
14 Règl./CE, art. 37.1 et 37.4.

conseiller le responsable de traitement, de contrôler le respect de la réglementation et de conseiller le responsable de traitement quant à la réalisation d'une analyse d'impact.

Malgré toutes les mesures qui peuvent être prises par le responsable de traitement[15], nul n'est à l'abri d'une faille de sécurité comme la perte, l'altération ou la divulgation de données. Désormais, avec le règlement, en cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente[16] dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques[17]. Par ailleurs, le règlement prévoit aussi la notification à la personne concernée de la violation de ses données à caractère personnel, lorsque la violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique[18].

15 Règl./CE, art. 5.2.
16 En Belgique, l'Autorité de protection des données.
17 Règl./CE, art. 33.1.
18 Règl./CE, art. 34.1.