Union des Villes et Communes de Wallonie asbl

LEGISLATION

RGPD – NOUVEAU REGLEMENT EUROPEEN EN MATIERE DE PROTECTION DE LA VIE PRIVEE EN QUELQUES MOTS

Marie-Laure Van Rillaer, Conseiller

A été signé, le 27 avril 2016, le nouveau règlement européen relatif à la protection des données à caractère personnel[1] destiné à remplacer la directive 95/46/CE[2]. 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.
Nous vous livrons ici une synthèse des nouveautés, qui mettent l'accent sur la sécurité et l'intégrité des données et qui renforcent les obligations des responsables de traitement de ces données.

A l'heure d'écrire ces lignes, n'est pas encore connue la manière dont la ou les autorité(s) compétente(s) implémentera(ont) ce nouveau règlement dans le droit belge. Même si ce nouveau règlement ne nécessite en théorie pas de transposition, il est clair que la loi[3] qui régit la matière devra être revue.

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[4] identifiée ou identifiable ; est réputée être une personne physique identifiable, une personne physique qui peut être identifiée, directement ou indirectement, notamment via un nom, un numéro d'identification, des données de localisation, un identifiant ou un élément spécifique se rapportant à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[5] ; 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 appliquée à des données, telles que la collecte, l'enregistrement, la conservation, la consultation, la communication par transmission, la diffusion ou la mise à disposition[6].
- La notion de *responsable de traitement* : il s'agit de la personne, physique ou morale, l'autorité publique qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[7].

[1] 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 directive 95/46/CE, *J.O.U.E.*, 4.5.2016.
[2] 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.
[3] 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] Ni les personnes morales, ni les personnes décédées ne sont protégées par cette réglementation.
[5] Règl./CE, art. 4, 1).
[6] Règl./CE, art. 4, 2).
[7] Règl./CE, Art. 4.7).

1. Première nouveauté : renforcement des exigences relatives au consentement 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, une des hypothèses de traitement licite est celle du consentement donné par la personne dont on traite les données à caractère personnel. Le règlement renforce les exigences liées à ce consentement puisqu'il le définit comme étant la 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[8]. La personne concernée pourra également retirer son consentement[9].

2. Deuxième nouveauté : élargissement de la notion de données sensibles

Le règlement distingue différentes catégories de données à caractère personnel dont certaines sont plus sensibles, telles que les données qui révèlent l'origine raciale, les opinions politiques, les convictions religieuses ou philosophiques, les données de santé ou l'orientation sexuelle. Une nouvelle catégorie de données sensibles s'est explicitement ajoutée aux précédentes : les données génétiques et biométriques[10].

Le traitement de ces données sensibles est en principe interdit, sauf exceptions, et est soumis à des règles particulières[11].

3. Troisième nouveauté : évolution des droits de la personne concernée

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. Parmi ces droits, notons que les droits à l'effacement (ou « droit à l'oubli ») et à la portabilité des données sont neufs et impacteront certainement la manière de traiter les données. Le premier droit permet à la personne concernée de faire effacer ses données lorsque, par exemple, elle retire son consentement au traitement des données ou lorsque les données ne sont plus nécessaires au regard des finalités[12]. Le droit à la portabilité des données est quant à lui le droit de la personne concernée de recevoir ou de faire suivre les données à caractère personnel qui la concernent dans un format structuré, couramment utilisé et lisible par machine[13]. Il s'agit donc pour la personne concernée de retrouver la maîtrise de ses données.

4. Quatrième nouveauté : responsabilisation accrue des acteurs et protection des données dès la conception 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[14]. Il doit donc mettre en place une politique proactive de

[8] Règl./CE, art. 4.11).
[9] Règl./CE, art. 7.3.
[10] Règl./CE, art. 9.
[11] Règl./CE, art. 9.
[12] Règl./CE, art. 17.
[13] Règl./CE, art. 20.
[14] Règl./CE, art. 5.2.

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[15].

5. Cinquième nouveauté : tenue d'un registre des traitements

Le règlement impose désormais l'obligation pour le responsable du traitement de tenir un registre des activités de traitements[16]. Cette obligation remplace l'obligation de notification préalable des traitements prévue par la loi du 8 décembre 1992[17].

6. Sixième nouveauté : réalisation d'une étude d'impact

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* »[18]. Cette étude doit également être établie lorsque, notamment, il y a traitement à grande échelle de catégories particulières de données sensibles.

7. Septième nouveauté : désignation d'un délégué à la protection des données

Les responsables de traitement qui sont des autorités publiques ou des organismes publics doivent désigner un délégué à la protection des données en fonction de certaines conditions[19]. Il est, entre autres, chargé d'informer et de 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.

Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille[20].

Cette mission de délégué à la protection des données pourra être confiée à un agent de l'administration en interne ou pourra être externalisée à une entreprise spécialisée[21]. Il devra disposer des connaissances suffisantes pour ce faire. Il jouira d'un statut particulier puisqu'il ne pourra pas recevoir d'instructions en ce qui concerne l'exercice de ses missions et ne pourra pas être relevé de ses fonctions ou pénalisé par le responsable de traitement pour l'exercice de ses missions[22]. Ce délégué pourra exercer d'autres missions pour autant que cela n'entraîne pas de conflits d'intérêts[23].

8. Huitième nouveauté : notification des violations des données à caractère personnel

Les conditions de traitement des données à caractère personnel imposent que les données soient traitées de façon à garantir une sécurité appropriée des données à caractère personnel. Malgré toutes les mesures qui peuvent être prises par le responsable de

[15] Règl./CE, art. 25.1.
[16] Règl./CE, art. 30.1.
[17] L. 8.12.1992, art. 17 et ss.
[18] Règl./CE, art. 35.1.
[19] Règl./CE, art. 37.1 et 37.4.
[20] Règl./CE, art. 37.3.
[21] Règl./CE, art. 37.6.
[22] Règl./CE, art. 38.3.
[23] Règl./CE, art. 38.6.

traitement[24], 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[25] 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[26].

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[27].

9. Neuvième nouveauté : réorganisation de la Commission de la protection de la vie privée et nouveaux pouvoirs

Le règlement est l'occasion de revoir les missions et les pouvoirs de sanctions des autorités de contrôle des Etats membres. L'effectivité des nouvelles règles, contraignantes et protectrices, n'est possible que grâce à l'accroissement des pouvoirs de contrôle et de sanction de l'autorité de contrôle, en la personne de la Commission de protection de la vie privée. Aussi, le règlement attribue aux autorités de contrôle, notamment, des pouvoirs d'enquête et le pouvoir de prendre des mesures correctrices[28].

10. Comment l'application de ce nouveau règlement se prépare-t-elle ?

Ce nouveau règlement est entré en vigueur le 24 mai 2016 et devra être appliqué dans les Etats membres dès le 25 mai 2018. Il reste donc une année pour que la Belgique et les pouvoirs locaux wallons s'adaptent aux changements.

La Commission de protection de la vie privée a également édité une brochure « R.G.P.D. : préparez-vous en 13 étapes »[29] que nous résumons comme suit :

- Conscientisation : il s'agit de conscientiser les personnes-clés et les décideurs aux changements importants en matière de données à caractère personnel qui se dessinent pour mai 2018.
- Etablissement d'un registre de données : il est recommandé de faire un inventaire minutieux des données traitées, de noter leur provenance, les personnes avec lesquelles elles sont partagées ainsi que leur fondement légal.
- Communication : le responsable de traitement doit communiquer à chacune des personnes concernées ses droits ; cela se fait par une déclaration de confidentialité[30] qui devra être mise à jour au regard des nouvelles obligations du règlement.
- Gestion des droits de la personne concernée : il s'agit d'examiner si la façon de traiter les données respecte les (nouveaux) droits de la personne concernée.
- Gestion des demandes d'accès : la Commission conseille de réfléchir sur la manière de gérer les demandes d'accès aux données par les personnes concernées.
- Déterminer le fondement légal du traitement de données à caractère personnel.
- Evaluer la qualité du consentement lorsqu'il s'agit du fondement légal du traitement utilisé et adapter les procédures aux nouvelles obligations du règlement.
- Evaluer et adapter les procédures en offrant aux enfants une protection spécifique.

[24] Règl./CE, art. 5.2.
[25] En Belgique, la Commission de protection de la vie privée.
[26] Règl./CE, art. 33.1.
[27] Règl./CE, art. 34.1.
[28] Règl./CE, art. 58.
[29] Disponible sur le lien suivant :
https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf
[30] Voyez notamment cet exemple : http://www.belgium.be/fr/declaration_de_confidentialite

- Détection et gestion des fuites de données : il s'agit de déterminer les risques de fuites de données, leur gestion et la mise en place d'une procédure en cas de notification à l'autorité de contrôle.
- Protection des données dès la conception et analyse d'impact : veiller, dès le début, à prévoir une conception des traitements des données qui permette le respect du nouveau règlement et envisager la réalisation d'une analyse d'impact.
- Désignation d'un délégué à la protection des données : elle est obligatoire pour les autorités publiques et les organismes publics.
- Au niveau national, déterminer l'autorité de contrôle compétente et si les opérations de traitement ont un caractère national.
- En ce qui concerne les contrats existants et futurs, évaluer et mettre en conformité les relations contractuelles avec vos sous-traitants (soit généralement, les adjudicataires de marchés publics locaux).

En conclusion, l'on peut dire que ce nouveau règlement amène de nombreuses nouveautés, qui s'intègrent logiquement dans la continuité de la réglementation protégeant les données à caractère personnel tout en évoluant sur des points précis. Notre association ne manquera pas d'informer ses membres sur les mesures de mise en œuvre de ce règlement et de proposer des outils utiles en vue de l'implémentation de cette réglementation dans la vie quotidienne de nos membres.