Fiche 3 - RGPD

Avec l'avènement et l'intensification du recours aux moyens technologiques est apparue une utilisation exponentielle des données à caractère personnel. Cela a nécessité la révision de la réglementation européenne en matière de protection des données à caractère personnel. C'est ainsi que le règlement général pour la protection des données à caractère personnel (ou RGPD[1]), en application depuis mai 2018, est né. Il n'est pas en soi une révolution, mais plutôt une évolution des règles relatives à la protection des données à caractère personnel.

Ces moyens technologiques ont aussi permis l'organisation de ce qu'on appelle l'e-gouvernement, tel qu'il est actuellement organisé en Belgique[2]. L'e-gouvernement ou le gouvernement électronique est "*une manière intégrée et continue de fournir des services publics, grâce à l'utilisation optimale des technologies de l'information et de la communication*"[3]. Il se matérialise notamment par l'introduction d'une demande d'un citoyen de manière électronique auprès d'une administration locale ou par l'accès de la commune à des données détenues par une autre autorité et ce, parfois de manière complètement intégrée, directement dans le logiciel métier.

Le développement de l'e-gouvernement au sein des et par les pouvoirs locaux est étroitement lié au respect de la protection des données à caractère personnel, même s'il ne lui est pas propre. Le respect du RGPD doit être considéré comme un enjeu primordial dans la digitalisation des pouvoirs locaux.
De plus, compte tenu des nombreuses initiatives prises par l'Union européenne en matière digitale (notamment en matière d'open data, de cybersécurité, d'interopérabilité, de single digital gateway) et compte tenu des développements récents technologiques (intelligence artificielle entre autres), il est impératif que les pouvoirs locaux s'organisent et veillent à protéger et gérer les données, qu'elles soient à caractère personnel ou pas, d'ailleurs.

Une certaine maturation en matière de protection des données doit s'acquérir auprès de tous, qu'il s'agisse d'autorités publiques locales, fédérales ou régionales ou d'entreprises privées. Voici quelques idées-clés pour y tendre.

1. Les principes du RGPD en quelques mots

En un mot comme en cent, le RGPD peut se résumer en l'application de quelques principes clés[4] :

a. Finalité : il s'agit de vérifier que les données traitées vont être utilisées pour des raisons légitimes;
b. Licéité : ce principe impose de disposer d'une raison autorisant de traiter les données; si l'on a beaucoup parlé du fait de devoir obtenir le consentement des personnes dont on traite les données, en ce qui concerne les autorités publiques, c'est surtout des textes réglementaires qui leur permettent ou leur imposent de traiter des données. En effet, on ne demande pas aux citoyens leur consentement pour établir des impôts les concernant ou instruire un dossier d'urbanisme qu'ils ont initié. Les autorités publiques traitent des données essentiellement parce qu'elles en ont l'obligation légale ou exercent une mission d'intérêt public.
c. Proportionnalité : selon ce principe, les responsables de traitement ne peuvent traiter que les données à caractère personnel strictement nécessaires, durant le temps strictement nécessaire et que par l'intermédiaire des agents ayant été strictement autorisés.

[1] Règl./UE 2016/679 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, ci-après le RGPD.
[2] Voyez la Fiche e-Gouvernement.
[3] https://economie.fgov.be/fr/themes/line/la-notion-de-gouvernement.
[4] RGPD, art. 5.

d. Responsabilité : chaque responsable de traitement doit respecter le RGPD et doit pouvoir démontrer son respect.

2. Le RGPD est une porte d'entrée vers l'e-gouvernement et le management des données

La notion de données à caractère personnel s'apprécie de manière extrêmement large,[5] et ce, afin de protéger les personnes dont on traite les données. La notion comprend toutes les informations directement identifiantes (noms, coordonnées…), mais aussi celles ne permettant pas directement l'identification des personnes physiques (adresse d'un bien, salaire, objet d'une demande, situation précise). Elle englobe toutes les informations, quelle que soit sa nature (intime, amicale, professionnelle ou politique, etc.).
Il est donc clairement plus probable que le RGPD s'applique que l'inverse. Il est aussi plus simple et efficace d'appréhender les deux ensembles de données de manière globale que de les distinguer.
Par ailleurs, les données sont partout et existent pour tout. Si elles permettent de simplifier les démarches des citoyens et des entreprises, elles contribuent également à simplifier le travail des administrations, spécialement lorsqu'elles sont complètement intégrées au sein des logiciels utilisés par celles-ci. Les données permettent aussi d'évaluer et de contrôler le travail de l'administration[6]. La publication de certaines données favorise certainement ainsi la transparence administrative.

La mise en conformité au RGPD est donc plus qu'une mise en conformité réglementaire : elle est nécessaire pour entrer et se maintenir dans l'e-gouvernement et dans le management des données. Elle doit donc être considérée comme indispensable pour gérer plus équitablement et plus efficacement les nombreuses missions de service public incombant aux communes.

Le RGPD est aussi intimement lié à la question de la sécurité des systèmes d'information et à la sécurité informatique au sein de toute organisation. La question de la sécurité informatique est plus que jamais d'actualité.

3. Désignation d'un délégué à la protection des données

Le RGPD prévoit explicitement l'obligation pour les autorités publiques ou pour les organismes publics de désigner un délégué à la protection des données[7]. Les communes doivent donc en disposer d'un, que ce soit en interne ou en externe, le cas échéant mutualisé avec d'autres communes et/ou CPAS.

Ses missions sont[8]:

- d'informer et de conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur leurs obligations ;
- de contrôler le respect du RGPD et notamment les règles internes du responsable du traitement, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel et les audits;
- de dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci;
- de coopérer avec l'autorité de contrôle;

[5] RGPD, art. 4, 1) : "toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale".
[6] Voyez notamment l'initiative e-comptes : http://ecomptes.wallonie.be/ecomptes/index.php.
[7] RGPD, art. 37.1, a).
[8] RGPD, art. 39.

- de faire office de point de contact pour l'autorité de contrôle.

L'on dit souvent que le délégué à la protection des données est un mouton à cinq pattes: il est à la fois technicien en matière informatique, connaisseur des métiers de l'administration tout en s'intéressant aux questions juridiques, mais aussi en étant bon pédagogue et diplomate. Bref, il n'est guère aisé de trouver et de garder l'élu au sein de l'administration. Aussi, il faut le soutenir dans ses démarches et veiller à sa formation pour qu'il maintienne ses connaissances à jour.

La désignation d'un délégué à la protection des données est en outre indispensable pour permettre aux administrations d'accéder à certaines "sources authentiques", c'est-à-dire les bases de données officielles, notamment gérées par les autorités publiques au sens strict[9]. Une notification de sa désignation auprès de l'Autorité de Protection des Données ainsi qu'auprès d'autorités publiques est d'ailleurs imposée réglementairement ou contractuellement.

Enfin, la présence d'un délégué à la protection des données est indispensable pour guider l'administration en sa qualité de responsable de traitement, de sous-traitant ou de responsable de traitement conjoint, parmi les démarches de mise en conformité et de maintien en conformité avec le RGPD et toutes les réglementations qui découlent.

4. Etablissement et mise à jour du registre des activités de traitement

Le registre des activités de traitement est une nouveauté issue du RGPD. L'on pourrait le résumer comme étant un document synthétisant les traitements effectués par un responsable de traitement (ou le cas échéant un sous-traitant). Il n'est pas une base de données ni une reproduction des données traitées par l'administration. Il est une vue globale sur les traitements. Il contient aussi des indications précises sur chacun de ses traitements (quelles données, quelle durée de conservation, quelle(s) finalités, etc.). Il peut ainsi servir de référentiel en matière de management de données et surtout, il sera le premier outil de documentation servant à justifier l'état de mise en conformité de l'administration au RGPD.

Cet outil sera continuellement remis à jour (nouveaux traitements ou traitements à supprimer ou mises en conformité).

5. Adoption de plans de mise en conformité au RGPD définissant les priorités, de plans de protection/management des données et de plans de gestion des incidents

Pour débuter ou maintenir le travail de mise en conformité au RGPD et aux règlements connexes, l'administration sera bien inspirée d'adopter et de mettre à jour un plan déterminant les priorités de mise en conformité. En effet, la tâche est de longue haleine et l'on sait à quel point rares sont les organismes qui seraient parfaitement en ordre (s'ils existent). Aussi, aidée de son délégué à la protection des données, l'administration établira, le cas échéant en lien avec son PST, un plan de mise en conformité au RGPD.

De même, la gestion des incidents (informatique et lié à la protection des données, les deux étant liés) doit faire l'objet d'une procédure écrite, précieusement conservée et communiquée aux intervenants concernés. Ce plan de gestion comprendra notamment l'obligation d'éventuellement notifier à l'Autorité de Protection des Données voire aux personnes concernées des violations de données[10].

[9] Voyez la fiche à propos de l'e-Gouvernement.
[10] RGPD, art. 33 et 34.

