RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES TOUR D'HORIZON DES NOUVELLES OBLIGATIONS

Pierre-Yves THOUMSIN
Avocat au barreau de Bruxelles spécialisé en droit de la propriété intellectuelle et Assistant à l'Université libre de Bruxelles (ULB)

■ Les données à caractère personnel sont devenues un véritable enjeu pour ceux qui y donnent accès, comme pour ceux qui les utilisent. Le nouveau "Règlement général sur la protection des données" (RGPD), qui est entré en vigueur en mai 2016, laisse aux entreprises et aux organisations jusqu'au 25 mai 2018 pour se plier aux nouvelles exigences. Il importe de prendre des dispositions afin de faciliter la transition vers la nouvelle réglementation. Cet article propose de prendre connaissance des concepts de base relatifs au traitement de données à caractère personnel, puis des nouveaux droits et obligations introduits par le RGPD. Quelles sont les conséquences pour le traitement des données à caractère personnel ? Comment gérer au quotidien les contraintes juridiques ? Comment mettre son organisation en conformité ?

■ Persoonsgegevens zijn een uitdaging geworden zowel voor wie ze ter beschikking stelt als voor de gebruiker. De nieuwe "Algemene Verordening Gegevensbescherming" (AVG), van kracht sinds mei 2016, laat aan bedrijven en organisaties tot 25 mei 2018 de tijd om aan de nieuwe eisen te voldoen. Vanaf nu dienen dan ook de nodige maatregelen getroffen te worden om de overgang naar de nieuwe regeling vlot te laten verlopen. Het artikel biedt een voorstel om kennis te nemen van de basisbegrippen van de verwerking van persoonsgegevens, en van de nieuwe rechten en plichten ingevoerd door de AVG. Wat zijn de gevolgen voor de verwerking van persoonsgegevens? Hoe dient dagdagelijks omgegaan te worden met de juridische vereisten? Hoe de regelgeving naleven?

RGPD. L'acronyme désigne le Règlement Général sur la Protection des Données[1], applicable à compter du 25 mai 2018.

Depuis plusieurs mois, ces quatre lettres sont sur toutes les lèvres et tous les écrans : le droit de la protection des données à caractère personnel change et il faut être prêt ! Pourtant, parler d'une révolution serait trompeur.

La protection des données à caractère personnel fait déjà l'objet d'une règlementation étendue en Belgique, notamment par le biais de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Depuis 1995, la matière est également harmonisée au niveau européen par le biais d'une directive[2]. Cette directive sert de substrat au RGPD, qui la met au goût du jour et l'étoffe considérablement[3].

Le RGPD remplace ainsi une constellation de législations nationales par une réglementation unique et unifiée, avec pour objectif une plus grande harmonisation de la protection des données à caractère personnel en Europe.

Résumer en quelques pages les lignes de force d'un règlement de cette ampleur est une gageure. Dans le cadre de cette note synthétique, nous rappellerons d'abord les concepts de base du traitement de données à caractère personnel. Nous aborderons ensuite les droits étendus des personnes concernées par le traitement. Nous terminerons par les obligations corrélatives des responsables du traitement et les sanctions qui s'attachent à leur respect.

Le traitement de données à caractère personnel : notions de base

La notion de "traitement de données à caractère personnel" est particulièrement large, en sorte que tout organisme est potentiellement soumis aux obligations du RGPD.

La notion de "traitement" vise en effet toutes (ou tout ensemble d') opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données[4]. Le RGPD est applicable à tout traitement automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données contenues ou appelées à figurer dans un fichier[5].

Les "données à caractère personnel" sont toute information se rapportant à une personne physique identifiée ou identifiable, telle qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ainsi que tout élément propre à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou encore sociale[6]. On parle de "personne concernée".

Un certain nombre de données dites sensibles bénéficient d'un statut particulier et d'un degré élevé de protection, il s'agit des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses, à la santé et aux orientations sexuelles[7]. Signe des temps, le RGPD ajoute à la liste des données sensibles les données génétiques et biométriques utilisées aux fins d'identifier une personne physique de manière unique.

Le "responsable du traitement" est l'organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement[8].

Les personnes concernées bénéficient de droits et les responsables du traitement se voient corrélativement imposer des obligations.

Le traitement des données à caractère personnel doit ainsi être conforme à six principes de base[9] :

- les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (principes de licéité, loyauté et transparence) ;
- la collecte de données doit être effectuée pour des finalités déterminées, explicites et légitimes et tout traitement ultérieur doit être compatible avec celles- ci (principe de limitation des finalités) ;
- il y a lieu de limiter les données à ce qui est adéquat, pertinent et nécessaire au regard des finalités (principe de minimisation des données) ;
- les données doivent être exactes et, si nécessaire, tenues à jour et à défaut effacées ou rectifiées (principe d'exactitude) ;
- la durée de conservation des données ne doit pas excéder ce qui est nécessaire au regard des finalités (principe de limitation de la conservation) ;
- le responsable du traitement est tenu de garantir une sécurité appropriée des données à caractère personnel, au moyen de mesures techniques et organisationnelles adéquates (principe d'intégrité et de confidentialité).

À ces principes s'ajoute désormais un principe général de responsabilité, au sens où le responsable du traitement est responsable du respect des principes précités et doit être en mesure de démontrer leur respect. Ce principe de responsabilité constitue le fil rouge du RGPD et des nouvelles obligations qu'il impose.

Des droits accrus pour les personnes concernées

Le RGPD étend considérablement les droits de la personne concernée.

Une information plus claire et plus complète

Premier changement notable : le renforcement du droit à l'information. La liste des informations à fournir à la personne concernée afin de recueillir son consentement est considérablement allongée et inclut désormais notamment les coordonnées du délégué à la protection des données, l'exposé des intérêts légitimes du responsable (lorsqu'ils servent de fondement au traitement), la mention de l'existence des droits d'effacement, de limitation, d'opposition et de portabilité des données, la mention de l'existence du droit de retirer son consentement à tout moment, ou encore l'existence du droit d'introduire une réclamation auprès d'une autorité de contrôle[10].

Afin de "rendre à l'utilisateur le contrôle de ses données", il est requis que ces informations lui soient communiquées sous une forme concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

Le RGPD instaure ainsi un "droit à la compréhension", visant à garantir un consentement éclairé de la personne concernée.

La consécration du droit à l'oubli

Dans la foulée de l'arrêt Google Spain de la Cour de justice de l'Union européenne[11], le RGPD consacre expressément le "droit à l'oubli", compris comme le droit à l'effacement de données qui ne sont plus nécessaires au regard des finalités, ou pour lesquelles le consentement a été retiré et pour lesquelles il n'existe plus d'autre fondement juridique[12]. Si l'arrêt précité concernait spécifiquement le traitement effectué par les moteurs de recherche, le droit à l'effacement consacré par le RGPD s'étend potentiellement à tout type de traitement.

Émergence du droit à la portabilité des données

La personne concernée a désormais le droit d'exiger que le responsable du traitement lui fournisse une copie de ses données dans un format structuré, couramment utilisé et lisible par machine. La personne concernée peut en outre exiger que ces données soient transmises à un autre responsable de traitement. Ce droit naît dès que le traitement est fondé sur le consentement de la personne concernée et qu'il est effectué à l'aide de procédés automatisés[13].

Le profilage en ligne de mire

Le RGPD aborde une forme de traitement des données de plus en plus courante à l'heure des big data : le profilage. La notion vise "toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements pour cette personne physique"[14].

Le profilage n'est ainsi autorisé que moyennant le consentement explicite de la personne concernée

ou dans le cadre de la conclusion ou de l'exécution d'un contrat, lequel requiert par hypothèse un consentement. Le profilage est toutefois autorisé lorsque la législation de l'État membre l'autorise et que des mesures appropriées ont été prises pour la sauvegarde des droits et libertés individuels[15].

Renforcement des obligations des responsables de traitement

Conformément au nouveau principe de responsabilité, le RGDP impose au responsable du traitement des obligations renforcées, tant au stade de la prévention du risque que de sa gestion, lorsqu'il se matérialise. On attend ainsi du responsable de traitement qu'il prenne les mesures techniques et organisationnelles appropriées afin de garantir les droits des personnes concernées et la sécurité des données qui lui sont confiées.

Un consentement de qualité

Plus que jamais, le consentement au traitement de données à caractère personnel doit être éclairé.

Dès lors, s'il fait l'objet d'une déclaration écrite, il est désormais requis qu'il soit demandé de manière claire et distincte des autres questions, sous une forme compréhensible et aisément accessible, et en des termes clairs et simples[16]. S'il ne doit pas nécessairement être écrit, le consentement doit résulter d'un acte positif clair. Sont exclus le simple silence ou l'inactivité de la personne concernée, ou le recours à des cases cochées par défaut.

Dans ce contexte, il est important de vérifier le contenu des formulaires de consentement existants, de les compléter et le cas échéant de les clarifier.

Concernant spécialement les enfants, le traitement de leurs données à caractère personnel n'est licite que lorsque l'enfant est âgé d'au moins 16 ans. En-dessous de cet âge, le traitement n'est licite que si le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant[17]. Il est toutefois loisible aux États membres de prévoir un âge inférieur, pour autant qu'il ne soit pas en-dessous de 13 ans.

La déclaration à la Commission de la protection de la vie privée remplacée par un registre des activités de traitement

Alors qu'auparavant les responsables de traitement étaient tenus de déclarer leurs activités à la Commission de la protection de la vie privée, ils doivent désormais tenir un registre à produire en cas de contrôle[18].

Ce registre mentionnera notamment :

- le nom et les coordonnées du responsable de traitement et du délégué à la protection des données ;
- les finalités du traitement ;
- les catégories de personnes concernées et les catégories de données ;
- les catégories de destinataires ;
- l'éventuel transfert vers un pays tiers ;
- le délai d'effacement pour les différentes catégories ;
- une description générale des mesures de sécurité techniques et organisationnelles.

L'obligation de tenir un registre ne concerne en principe que les entreprises de plus de 250 employés. Toutefois, elle s'applique à toute entreprise qui opère un traitement de manière non occasionnelle, ou dont le traitement est risqué pour les droits et libertés de la personne concernée, ou porte sur des données sensibles ou des données relatives aux condamnations et infractions.

La Commission de la protection de la vie privée a publié sur son site un canevas de registre[19].

Analyse d'impact

Lorsque le traitement présente un risque élevé pour les droits et libertés, notamment en raison du recours à de nouvelles technologies et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, le responsable est tenu d'établir préalablement une analyse d'impact[20]. Après avoir décrit les opérations envisagées et leurs finalités, l'analyse procèdera à l'évaluation de leur nécessité et de leur proportionnalité, des risques que le traitement présente pour les droits et libertés, ainsi que des mesures envisagées pour y faire face.

Si l'analyse d'impact révèle des risques élevés, le responsable sera tenu de consulter préalablement l'autorité de contrôle.

Le délégué à la protection des données

Le processus de responsabilisation passe également par une nouvelle figure : le délégué à la protection des données.

Sa désignation est obligatoire au sein des autorités et organismes publics, au sein d'organisations dont les activités exigent un suivi régulier et systématique à grande échelle des personnes concernées, et lorsque le traitement porte sur des données sensibles ou des condamnations pénales. En dehors de ces hypothèses, sa désignation est facultative[21].

Le délégué à la protection des données est appelé à devenir le point de contact de l'organisation pour toute question relative à la protection des données, tant en interne en tant qu'organe consultatif que vis-à-vis de l'extérieur en tant que relais auprès des personnes concernées[22].

Le délégué a pour mission d'informer et de conseiller le responsable de traitement, en portant un regard critique sur ses activités au regard du RGPD (notamment dans le cadre d'analyses d'impact). Il est le point de contact de l'autorité de contrôle, avec laquelle il coopère[23].

Gestion du risque lorsqu'il se produit

En cas de fuite de données, le responsable du traitement est désormais tenu d'en avertir l'autorité de contrôle dans les 72 heures, sauf si cette violation n'est pas susceptible de porter atteinte aux droits et libertés des personnes physiques concernées[24]. La personne concernée doit également en être avertie, sauf si cela est disproportionné ou si des mesures utiles ont été prises en amont ou en aval[25].

Des sanctions véritablement dissuasives

Les autorités de contrôle – en Belgique la Commission de la protection de la vie privée – voient leurs pouvoirs considérablement renforcés. À cet égard, la réforme la plus notable est la capacité d'imposer des amendes administrative pouvant s'élever jusqu'à 20.000.000 EUR ou, dans le cas d'une entreprise, 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent[26].

Conclusion

Sans révolutionner les principes relatifs au traitement de données à caractère personnel, le RGPD contraint les responsables du traitement à réexaminer leurs pratiques et à les mettre à jour.

Il est vrai que certaines figures nouvelles (délégué à la protection des données ou analyse d'impact) ne concerneront vraisemblablement que les organisations de grande taille, ou qui effectuent des traitements à grande échelle. Néanmoins, dès lors que des obligations de base sont également renforcées – principalement celles relatives au consentement –, tout responsable de traitement est tenu de s'interroger sur la conformité des traitements qu'il effectue, même s'ils sont plus limités.

Dans ce cadre, il est recommandé de consulter régulièrement les sites de la Commission de la protection de la vie privée[27] et du groupe de travail article 29[28], dont on attend qu'ils publient progressivement des lignes directrices et conseils relatifs à la mise en œuvre du RGPD.

Pierre-Yves Thoumsin
JVM Avocats
Place Stéphanie 6
1050 Bruxelles
Tél. : 02-289 00 20
Fax : 02-289 00 21
http://www.jvm.be
pierre-yves.thoumsin@jvm.be

Octobre 2017

NDLR : Pierre-Yves Thoumsin a présenté une partie du Doc'Moment du 18 septembre 2017 sur la protection des données. Les dias de sa présentation et de celle de Caroline de Geest (Commission de protection de la vie privée) sont disponibles sur le site de l'ABD-BVD.

Notes

1. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif 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.
<http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:32016R0679> [en ligne] (consulté le 26/10/2017)
2. Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
<http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex%3A31995L0046> [en ligne] (consulté le 26/10/2017)
3. Alors que la directive contenait 34 articles, le règlement en compte désormais 99.
4. Art. 4, 2) du Règlement.
5. Art. 2, § 1.
6. Art. 4, 1).
7. Art. 9.
8. Art. 4, 7).

9. Art. 6.
10. Art. 13 et 14.
11. CJUE, 13 mai 2014, Google Spain, aff. C-131/12. <http://eur-lex.europa.eu/legal-content/FR/TXT/?qid=1509048351799&uri=CELEX:62012CJ0131> [en ligne] (consulté le 26/10/2017)
12. Art. 17.
13. Art. 20.
14. Art. 22.
15. Art. 22.
16. Art. 7.
17. Art. 8.
18. Art. 30.
19. Modèle de Registre des activités de traitement. Commission de la protection de la vie privée. <https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement> [en ligne] (consulté le 26/10/2017)
20. Art. 35.
21. Art. 37.
22. Art. 38.
23. Art. 39.
24. Art. 33.
25. Art. 34.
26. Art. 83.
27. Commission de la protection de la vie privée. <http://www.privacycommission.be> [en ligne] (consulté le 26/10/2017)
28. Article 29 Working Party. European Commission - Justice and Consumers. <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> [en ligne] (consulté le 26/10/2017)