Nouveau règlement européen en matière de protection des données

Cruquenaire, Alexandre

Published in:
Bulletin juridique et social

Publication date:
2016

Document Version
le PDF de l'éditeur

Nouveau règlement européen en matière de protection des données

La protection des données à caractère personnel est devenue une préoccupation majeure à la suite de l'essor des nouvelles technologies.

Conscients de ce phénomène et de la nécessité de mettre à jour la législation en vigueur sous l'actuelle directive 95/46/CE[16], le Parlement européen et le Conseil ont adopté un règlement (UE) 2016/679[17] relatif à la protection des données à caractère personnel. Publiées le 4 mai dernier au *Journal officiel de l'Union européenne*, les dispositions de ce règlement seront directement applicables dans tous les États membres à partir du 25 mai 2018.

Les changements majeurs introduits par le règlement ont pour conséquence de faire de la question de la protection des données à caractère personnel un enjeu prioritaire pour toute entreprise ou tout groupe d'entreprises amené(e) à traiter dans le cadre de ses activités, de quelque manière que ce soit, des données à caractère personnel.

---

16 *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, J.O.U.E., n° L 281 du 23 novembre 1995, p. 31.*

17 *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, J.O.U.E., n° L 119 du 4 mai 1995, p. 1.*

Par donnée à caractère personnel est visée toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée identifiable toute personne physique pouvant être, directement ou indirectement, identifiée. Constituent donc des données à caractère personnel, notamment, le nom patronymique, l'adresse, le numéro de registre national, l'adresse e-mail, des données de localisation, l'adresse IP, ou encore des éléments propres à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale d'une personne. Dès lors, tout traitement, à savoir toute opération effectuée, de manière automatisée ou non, sur ces données, telle que la collecte, l'enregistrement ou encore l'utilisation de ces données, bénéficie de la protection instaurée par le règlement.

Considérations préliminaires

Avant toute chose, le champ d'application territorial de la protection se trouve élargi puisque le règlement s'appliquera tant aux entreprises qui sont établies au sein de l'Union européenne qu'aux entreprises situées hors de l'Union européenne mais dont l'activité principale consiste à offrir des produits et services aux citoyens européens ou à observer le comportement de citoyens européens.

Par ailleurs, le législateur européen a opéré une harmonisation de l'application du règlement dans les vingt-huit États membres en prévoyant que lorsqu'une entreprise exerce ses activités dans différents pays membres, l'autorité nationale de contrôle de l'établissement principal de cette entreprise sera compétente pour agir en tant qu'autorité-chef de file concernant les traitements de données transfrontières effectués. Il sera donc mis fin aux divergences d'appréciation et de délais de traitement entre les différentes autorités nationales de contrôle, ce qui assurera une plus grande sécurité juridique aux entreprises et groupes d'entreprises.

Plus concrètement, le règlement ainsi adopté poursuit le principal objectif d'accroître la sécurité des données détenues par des entreprises en renforçant les droits des personnes auxquelles ces données font référence et en responsabilisant davantage les responsables de traitement.

Renforcement des droits des personnes concernées

Outre l'obligation pour le responsable du traitement de fournir aux personnes concernées toutes les informations concernant le traitement de leurs données (finalités, catégories de destinataires, durée de conservation…) de manière concise, transparente, compréhensible et aisément accessible (en particulier pour toute information destinée spécifiquement à un enfant), les conditions d'obtention du consentement de ces personnes à ce que leurs données soient traitées seront, à l'avenir, plus strictes. En effet, lorsque le responsable de traitement devra recueillir le consentement écrit de la personne concernée par ledit traitement, la demande de consentement devra être formulée en des termes clairs et simples et être présentée sous une forme qui la distingue clairement des autres questions. Il ne sera donc plus possible pour le responsable du traitement d'opter pour un consentement tacite ou passif ou recueilli au moyen de cases cochées par défaut.

Les personnes concernées auront d'autre part un droit d'accès aux données traitées les concernant et pourront en demander la rectification auprès du responsable du traitement en cas de données incomplètes ou inexactes.

Grande nouveauté introduite par le règlement, les personnes concernées pourront, dans certains cas limitativement énumérés, exercer un « droit à l'oubli numérique » directement auprès de la ou des personne(s) qui traite(nt) leurs données. Ainsi, lorsque la personne décidera, par exemple, de retirer son consentement sur lequel était fondé le traitement, elle pourra exiger du responsable du traitement qu'il efface, dans les meilleurs délais, les données concernées. Il sera également tenu d'informer tout tiers auquel les données auront été transférées de cette demande. Il s'agit d'un véritable droit à l'effacement des données qui est consacré par le règlement et qui va donc bien au-delà du simple droit au déréférencement consacré par l'arrêt de la Cour de justice « Google Spain » rendu le 13 mai 2014 en application de la directive 95/46/CE.

Sans aller jusqu'à l'effacement, les personnes concernées pourront se contenter de demander la limitation du traitement de leurs données au responsable du traitement. Une telle demande pourrait être formulée dans l'hypothèse où l'exactitude de ces données devrait être vérifiée par le responsable, ou encore si les données ne sont plus nécessaires aux fins du traitement énoncé mais sont toutefois toujours utiles à la personne concernée, par exemple pour la constatation, l'exercice ou la défense de droits en justice.

Enfin, le règlement consacre le droit à la portabilité des données en vertu duquel la personne concernée pourra exiger du responsable du traitement qu'il lui remette, sous un format structuré, couramment utilisé et lisible par machine, les données à caractère personnel la concernant, voire, lorsque cela est techniquement possible, exiger de celui-ci qu'il transmette directement ces données à un autre responsable de traitement.

Obligations plus strictes dans le chef du responsable du traitement et des sous-traitants

Concomitamment au renforcement des droits des personnes concernées, le règlement procède à un durcissement des obligations à charge des responsables de traitement ainsi que des sous-traitants.

De manière générale, le responsable du traitement se voit tenu de faciliter l'exercice par la personne concernée de ses droits précités et devra répondre dans les meilleurs délais (et au plus tard dans le mois) à toute demande d'information d'une personne concernant le traitement de ses données.

Le règlement introduit par ailleurs les notions de *privacy by design* et de *privacy by default*. La première implique, pour le responsable de traitement, la prise en compte tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des exigences en matière de protection des données. La seconde consiste, pour le responsable du traitement, à s'assurer que, par défaut, seules les données nécessaires au regard de chaque finalité déterminée sont traitées.

Sur sa lancée, le règlement intègre aussi le principe anglo-saxon d'*accountability*, à savoir l'obligation pour les entreprises amenées à traiter des données de pouvoir démontrer à tout moment à l'autorité de contrôle qu'elles ont mis en œuvre les moyens nécessaires pour respecter le règlement.

Autre modification substantielle introduite par le règlement : l'exigence imposée sous la directive 95/46/CE de notifier à l'autorité de contrôle nationale la mise en œuvre d'un traitement de données est abandonnée et remplacée par une obligation plus générale pour le responsable de traitement de tenir un registre détaillé des activités de traitement mises en œuvre sous sa responsabilité. Ce registre devra comprendre une identification du responsable de traitement, les finalités du traitement, une description des catégories de données traitées et des personnes concernées ainsi que des destinataires de ces données, une description des mesures techniques et organisationnelles mises en œuvre pour garantir la sécurité de ces données, dans la mesure du possible, une estimation des délais prévus pour l'effacement des différentes catégories de données…

Plus strict encore, le règlement impose, en cas de traitement de données présentant un risque élevé pour les droits et libertés des personnes physiques en raison de la nature ou de la portée des opérations envisagées, la réalisation, par le responsable du traitement, d'une analyse d'impact préalable. Ce prérequis obligatoire en cas de traitement présentant un risque particulier devra être mis en œuvre dans les hypothèses suivantes, identifiées par le législateur européen :

- l'évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques, fondée sur un traitement automatisé (notamment le profilage) et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière tout aussi significative ;
- le traitement à grande échelle de données génétiques, de données biométriques, de données concernant la santé ou la vie et l'orientation sexuelle, ou de données relatives aux condamnations ou aux infractions pénales ;
- ou encore la surveillance systématique à grande échelle d'une zone accessible au public. Cette liste n'est toutefois pas exhaustive et devra être complétée par la Commission vie privée.

Notons que si une telle analyse d'impact confirme l'existence d'un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devra consulter la Commission vie privée qui disposera alors d'un délai de huit semaines (prolongeable) pour émettre son avis. Si celui-ci est négatif ou contient des remarques, le traitement projeté devra être revu, puis à nouveau soumis à l'avis de la Commission vie privée.

Une nouveauté supplémentaire réside dans l'obligation pour les entreprises, agissant en tant que responsables du traitement ou en tant que sous-traitantes, de désigner un délégué à la protection des données lorsque leurs activités de base consistent en des opérations qui exigent un suivi régulier et systématique à grande échelle des personnes concernées, ou consistent en un traitement à grande échelle de données sensibles[18]. Il en ira de même pour les autorités publiques ou organismes publics qui effectuent des traitements de données à caractère personnel.

Les missions du délégué à la protection des données seront, entre autres, d'informer et de conseiller l'entreprise (et ses salariés) sur ses obligations, de contrôler la conformité avec le règlement, de dispenser des conseils en ce qui concerne l'analyse d'impact, de coopérer et faire office de point de contact avec l'autorité nationale de contrôle (la Commission vie privée). Ce délégué à la protection des données pourra être un membre interne à l'entreprise et combiner cette fonction avec d'autres tâches ou être quelqu'un d'externe.

L'éventualité d'une fuite des données traitées par une entreprise n'a pas échappé au législateur européen. Le règlement prévoit dès lors qu'une entreprise confrontée à ce type d'incident devra signaler la fuite de données à la Commission vie privée dans les plus brefs délais et, si possible, endéans les 72 heures de la prise de connaissance de l'incident. Le cas échéant, la personne dont les données sont concernées par la brèche de sécurité devra également en être avertie. Le responsable du traitement sera en tous les cas tenu de limiter les conséquences

18 *Données génétiques, données biométriques, données concernant la santé ou la vie et l'orientation sexuelle ou encore données relatives aux condamnations ou aux infractions pénales.*

négatives d'une telle fuite de données, par exemple en recourant au chiffrement des données.

Hypothèse de plus en plus fréquente, toute entreprise qui transfère des données à caractère personnel vers un pays tiers devra dorénavant être en mesure de démontrer que ce pays tiers dispose d'un niveau de protection adéquat de ces données ou que des garanties appropriées ont été prévues afin d'assurer la sécurité de ces données. Rappelons à cet égard que l'accord de *Safe Harbor*[19] qui régissait l'exploitation des données des citoyens européens aux États-Unis a été invalidé par la Cour de justice en date du 6 octobre 2015[20]. Un nouvel accord dénommé *Privacy Shield* est en cours de négociation entre la Commission européenne et les États-Unis. Dans l'intervalle, les autres mécanismes de protection tels que les règles d'entreprise contraignantes et les clauses contractuelles types restent une alternative applicable.

Enfin, le règlement responsabilise davantage les sous-traitants agissant pour le compte d'un responsable de traitement puisque, contrairement à la directive 95/46/CE, des obligations sont directement et spécifiquement prévues les concernant. Ceux-ci devront entre autres maintenir une documentation adéquate, mettre en œuvre toutes les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté, effectuer les analyses d'impact, désigner un délégué à la protection des données, satisfaire aux exigences requises en cas de transfert de données vers des pays tiers et coopérer avec les autorités de contrôle nationales. Ces obligations s'ajoutent aux garanties contractuelles que le règlement impose d'inclure dans la convention liant le sous-traitant au responsable du traitement. Le non-respect de ses obligations par le sous-traitant sera sanctionné de manière ferme puisque celui-ci sera soumis aux mêmes sanctions que celles applicables au responsable du traitement.

Pouvoirs accrus des autorités nationales de contrôle

Last but not least, les autorités nationales de contrôle se voient quant à elles attribuer des pouvoirs de contrôle et de sanction plus importants. Alors que certaines autorités de contrôle n'étaient jusqu'ici pas en mesure de sanctionner les violations de la réglementation en matière de protection des données, le règlement introduit des sanctions en cas de non-conformité aux obligations extrêmement dissuasives, telles que des amendes allant jusqu'à 20.000.000 € ou 4 % du chiffre d'affaires de l'entreprise (ou du groupe dont fait partie l'entreprise) en infraction.

Et en pratique ?

Il ne fait aucun doute que la réglementation relative à la protection des données à caractère personnel en vigueur sous la directive 95/46/CE devait faire l'objet, de la part du législateur européen, d'une actualisation importante au regard, notamment, du développement exponentiel des activités en ligne.

Qu'elles agissent en qualité de responsable de traitement ou en qualité de sous-traitant, les entreprises ont tout intérêt à anticiper la mise en exécution du règlement en procédant, dès aujourd'hui, à l'examen des moyens actuellement déployés au sein de leur organisme en matière de protection des données, ainsi qu'en procédant à l'évaluation concrète des mesures qui devront être renforcées ou instaurées dans les mois à venir afin de se conformer aux nombreuses obligations mises à leur charge.

En effet, qu'il s'agisse d'une multinationale ou d'une PME, *toute entreprise* est aujourd'hui amenée, d'une façon ou d'une autre, à collecter, consulter ou utiliser des données relatives à ses clients, à ses employés ou encore à ses fournisseurs, et se trouve, par conséquent, *directement concernée par les obligations* examinées *supra*.

Il conviendra notamment pour ces entreprises de vérifier que leur(s) police(s) vie privée respecte(nt) les critères renforcés de transparence et de licéité du consentement de la personne concernée. Elles devront, en outre, prendre des mesures visant à réduire à un minimum les traitements des données à caractère personnel qu'elles effectuent et à pseudonymiser les données à caractère personnel dès que possible. Une procédure de conservation de toutes les traces documentaires relatives aux activités de traitement réalisées devra être mise en œuvre, impliquant la tâche d'identifier et de tenir à jour une liste de tous les tiers auxquels les données sont transférées dans le cadre de leur traitement.

Chaque entreprise devra également mettre au point un modèle d'analyse d'impact et être en mesure de l'appliquer, dès le 25 mai 2018, aux traitements de données en cours. De même, chaque entreprise devra mettre en place une procédure standardisée en cas de brèche de sécurité et être apte à conserver une trace documentaire du contexte, des effets et des mesures prises en cas de fuite de données.

Il convient par ailleurs, dès aujourd'hui, d'évaluer la nécessité, voire l'opportunité pour tout responsable de traitement ou tout sous-traitant de désigner un délégué à la protection des données et d'entamer, le cas échéant, la procédure de recrutement.

La mise en conformité des entreprises amenées à traiter des données à caractère personnel au nouveau règlement en matière de protection des données nécessitera un investissement substantiel de la part de celles-ci, tant en termes de temps consacré qu'en termes de moyens déployés. Cette démarche impliquera nécessairement une analyse préalable et détaillée des traitements effectués et des types de données traitées. Chaque entreprise devra ensuite, sur la base de cette analyse, procéder à l'élaboration d'un plan d'action visant à identifier les mesures à mettre en place afin d'assurer la sécurité des données à caractère personnel, la gestion appropriée des risques encourus, la mise en œuvre efficace de la procédure en cas de fuite de données et la collaboration effective avec les autorités nationales de contrôle.

Un tel investissement permettra *in fine* à l'entreprise de ne pas considérer le règlement uniquement comme une source de contraintes, mais également comme l'opportunité de renforcer son image en tirant parti des données à caractère personnel comme de tout autre actif de la société.

Il (ne) reste, presque jour pour jour, (que) deux ans aux entreprises pour se préparer à ces changements. À vos marques, prêts ? Partez !

Élodie Lecroart et Alexandre Cruquenaire

19 *Décision de la Commission 2000/520/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, J.O.U.E., n° L 215 du 25 août 2000, pp. 7-47.*

20 *CJUE (gr. ch.), 6 octobre 2015, Schrems, C-362/14.*

Urbanisme – Aménagement du territoire – Environnement

Jurisprudence

Article 112 du CWATUP – règle du comblement

Dans un arrêt récent du 5 janvier 2016[21], le Conseil d'État a été amené à préciser les conditions d'application de l'article 112 du CWATUP. Cette disposition permet d'octroyer un permis d'urbanisme dans une zone du plan de secteur dont l'affectation n'est pas compatible avec l'objet de la demande (à l'exclusion des zones naturelles, des zones de parcs et des périmètres de point de vue remarquable), à condition que :

« 1° le terrain soit situé entre deux habitations construites avant l'entrée en vigueur du plan de secteur et distantes l'une de l'autre de 100 mètres maximum ;

2° ce terrain et ces habitations soient situés *à front de voirie* et du même côté d'une voie publique suffisamment équipée en eau, électricité et égouttage, pourvue d'un revêtement solide et d'une largeur suffisante, compte tenu de la situation des lieux ;

3° les constructions transformations, agrandissements ou reconstructions s'intègrent au site bâti ou non bâti et ne compromettent pas l'aménagement de la zone » (Nous soulignons).

Dans l'arrêt précité, le Conseil d'État a pu préciser, à propos de la deuxième condition, que « l'exigence ainsi formulée concerne le terrain lui-même où viendrait s'implanter le projet ainsi que les habitations de référence existantes, qui doivent se situer "à front de voirie" ; que cette exigence, qui doit s'entendre notamment comme excluant des constructions en fond de parcelle n'est pas nécessairement synonyme d'habitation construite sur l'alignement, n'est pas formulée expressément pour l'habitation qui viendrait s'implanter entre lesdites habitations de référence ; qu'autre chose est le respect de la condition émise au 3° de ladite disposition, selon laquelle la construction doit s'intégrer au site bâti ou non bâti, excluant ainsi une construction en arrière zone ».

Il considéra donc en l'espèce « qu'un retrait de l'habitation en projet de 7 à 8 m par rapport à la voirie sur un terrain ayant un accès direct à celle-ci reste conforme à l'article 112, alinéa 1er, 2°, du CWATUPE ».

Le Conseil d'État avait par le passé pu juger qu'« il n'est pas possible de considérer qu'une habitation comme une ferme voisine, érigée à une distance mesurée par le bénéficiaire du permis d'urbanisme attaqué de 35 mètres de la voirie, est une habitation située à front de voirie »[22], et que « l'autorité peut considérer, sans commettre d'erreur manifeste d'appréciation, qu'une l'habitation sise dans le fond d'une parcelle et érigée à une distance de plus de 20 mètres de la voie publique n'est pas une habitation située à front de voirie »[23].

Détermination de la classe d'une activité classée

Dans le système d'évaluation des incidences des projets sur l'environnement, le gouvernement wallon a classé diverses activités en rubriques selon leurs nuisances potentielles exprimées en termes de capacité (d'accueil pour les salles de fêtes, de production ou de conservation pour l'industrie agroalimentaire liée aux fruits et légumes, installées de production pour la production de sel, etc.) et impose, en fonction d'un seuil déterminé, certaines formalités supplémentaires telles que la nécessité d'obtenir un permis d'environnement et, au-delà d'un certain seuil, la réalisation d'une étude d'incidences. Dans un arrêt du 28 juin 2012[24],

21 *CE, arrêt n° 233.405 du 5 janvier 2016, Roelandts.*

22 *CE, arrêt n° 203.318 du 27 avril 2010, Delpesse et consorts.*

23 *CE, arrêt n° 231.995 du 27 juillet 2015, Waterlot.*

24 *CE, arrêt n° 220.092 du 28 juin 2012, Sneessens et Jacobs.*