Isabelle DUBOIS

Avocate de formation et ancienne juge cantonale, Isabelle Dubois a été la première préposée à la protection des données et à la transparence du canton de Genève. Elle met depuis janvier 2014 son expertise en la matière à disposition des organisations comme indépendante à l'enseigne d'AD HOC RESOLUTION, et délivre expertises et accompagnements en la matière.

Le Règlement général sur la protection des données de l'Union européenne

Pixel a pris connaissance du Règlement général sur la protection des données de l'Union européenne. C'est un très gros document, Pour commencer, pourriez-vous dire à nos lecteurs s'il faut impérativement le lire dans son intégralité ?

Il est vrai que ce document est long puisqu'il contient en tout 88 pages. Mais il est constitué de deux parties, dont la première est une sorte d'exposé des motifs sous forme de préambule. Le texte de loi proprement dit commence à la page 33, et comprend 99 articles en tout. Pour connaître les dispositions légales auxquelles nous serons tenus, la deuxième partie est suffisante. Si l'on souhaite comprendre les motivations du législateur et déterminer quelle était sa volonté, la première partie constitue un éclairage très intéressant. Le texte légal lui-même est structuré en dix grands chapitres, qui prévoient successivement les dispositions générales, les principes applicables, les droits de la personne concernée, la question du responsable du traitement et du sous-traitant, le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales, les autorités de contrôle indépendante, les règles de coopération et de cohérence, les voies de recours, responsabilités et sanctions, les dispositions relatives à des situations particulières de traitement des données, les actes délégués et les actes d'exécution, enfin les dispositions finales. On peut donc lire ce document de différentes façons en fonction de ses besoins. Les lecteurs trouveront par ailleurs sur mon site une table

des matières du règlement qui peut s'avérer utile (http://adhocresolution.ch/2016/12/20/reglement-general-de-lunion-europeenne-protection-donnees/).

Pourquoi l'union européenne s'est-elle dotée d'un règlement général en la matière ?

L'objectif du règlement est de renforcer les droits des personnes physiques en matière de protection des données, et de faciliter la libre circulation des données à caractère personnel dans le marché unique numérique, notamment par une réduction de la charge administrative. Il a une force d'application plus grande que la directive actuelle, car il s'applique de plein droit sur tout le territoire de l'Union européenne. Il permet d'uniformiser les droits et obligations et d'organiser de manière cohérente le traitement des litiges par les autorités de surveillance.

Son fondement est le respect de tous les droits fondamentaux et principes reconnus par la Charte des droits fondamentaux de l'Union européenne, consacrés par les traités, et en particulier le droit au respect de la vie privée et familiale, du domicile et des communications, le droit à la protection des données à caractère personnel, et le droit à la liberté d'expression et d'information.

Il part d'un constat : l'évolution technologique et la mondialisation requièrent « un cadre de protection des données plus solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur ».

Pourriez-vous nous expliquer à qui et à quoi ce règlement s'appliquera ou au contraire ne s'appliquera pas ?

Sur le plan matériel, le règlement s'applique aux traitements de données à caractère personnel automatisés ainsi qu'aux traitements manuels si les données sont contenues ou destinées à être contenues dans un fichier (structuré). Il ne s'appliquera pas au traitement par une personne physique pour l'exercice d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale, mais bien aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques. Sur un plan territorial, il s'appliquera à tout traitement de données à caractère personnel intervenant dans le cadre des activités d'un établissement (exercice effectif et réel d'une activité), d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement lui-même ait lieu ou non dans l'Union ; il s'appliquera aussi au traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est, lui, pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non. Idem lorsque ledit traitement est lié à l'observation du comportement de ces personnes, dans la mesure où il s'agit de leur comportement au sein de l'Union européenne. Il s'appliquera aux citoyennes et citoyens, en tant que personne concernée, indépendamment

de leur nationalité ou de leur lieu de résidence, dans le cadre du traitement de leurs données à caractère personnel. C'est le traitement de données à caractère personnel qui compte, pas la technologie utilisée. Certains traitements spécifiques font l'objet d'autres règlements, comme le traitement par un organe étatique ou le traitement à des fins de prévention et de détection des infractions pénales.

Est-il exact que la notion de données personnelles ou de données à caractère personnel doit être comprise de manière large et non restrictive ?

On peut dire cela, en effet, car le règlement s'appliquera à toute information concernant une personne physique, qu'elle soit identifiée ou identifiable, y compris les données qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires, par « des moyens raisonnablement susceptibles d'être mis en œuvre ». Il ne s'appliquera pas aux données anonymes, traitées notamment à des fins statistiques ou de recherche.

Alors concrètement lorsqu'en tant qu'entreprise je traite des données à caractère personnel, quels sont les principes auxquels je suis tenue ?

Les principes à respecter lors du traitement sont les suivants :

- Tout traitement doit être licite et loyal.
- Les personnes doivent être informées « en toute transparence » de la collecte, de l'utilisation, de la consultation, du traitement actuel ou futur. L'information doit être accessible, facile à comprendre, exprimée en termes simples et clairs. L'identité du responsable de traitement et la finalité doivent être connus.
- Les finalités précises du traitement doivent être explicites et légitimes, et déterminées lors de la collecte. Un traitement à d'autres fins est admissible s'il est « compatible » avec la finalité initiale (comme l'archivage).
- Les données doivent être adéquates, pertinentes, limitées à ce qui est nécessaire au vu des finalités. En particulier, la durée de conservation doit être « limitée au strict minimum », de sorte que des délais devront être fixés par les responsables de traitement. Le traitement ne doit avoir lieu que si la finalité ne peut être atteinte autrement.
- Les données inexactes doivent être rectifiées ou supprimées.
- Une sécurité et une confidentialité « appropriées » des données doit être garantie, l'accès non autorisé à ces données et à l'équipement servant à leur traitement doit être prévenu.

Quels sont les éléments nouveaux dans le règlement par rapport à la directive actuelle ?

En premier lieu, le règlement renforce certains droits et obligations : sont renforcés le droit d'accès de la personne concernée, y compris un droit à l'oubli numérique, la volonté que la personne concernée puisse se réapproprier ses données personnelles, les responsabilités de celui qui traite les données et de celui qui les sous-traite. Des dispositions spécifiques au consentement ont été adoptées : le consentement devra être donné par un acte positif ex-

plicite qui établit que la personne concernée accepte de façon libre, spécifique, informée et univoque le traitement de ses données personnelles, ce qui conduira à mon avis à faire usage de l'opt in par opposition à l'opt out sur les sites Internet. Et il devra y avoir un consentement par finalité, sauf pour le traitement des données à des fins de recherche scientifique, pour lequel un consentement par domaine de recherche ou partie d'un projet suffira. De même, l'actuel correspondant informatique et libertés est remplacé par le délégué à la protection des données (DPO), dont la mission est augmentée par rapport au premier, et acquiert un aspect stratégique. Le rôle des autorités de contrôle ainsi que les sanctions aux contrevenants sont également renforcées. Plusieurs obligations de faire sont nouvelles : l'obligation de respecter la sphère privée dès la conception, à savoir que les nouveaux traitements, applications, logiciels devront être conçus selon le principe de la privacy by design and by default ; l'évaluation d'impact, qui devra impérativement être effectuée lorsqu'un nouveau traitement envisagé est susceptible d'enfreindre les droits de la personnalité ou les droits fondamentaux des personnes concernées. Les personnes concernées ont de plus le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine (portabilité des données). Enfin, en cas de violation de données à caractère personnel, le responsable du traitement la notifie à l'autorité de contrôle compétente, dans les meilleurs délais (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.

Doit-on craindre l'entrée en application de ce règlement ? Quels conseils donneriez-vous à nos lecteurs ?

Le Règlement doit permettre d'assurer un niveau homogène de protection des personnes physiques dans l'ensemble de l'Union, et de ce point de vue je pense qu'il facilitera la vie des entreprises internationales, des groupes ayant des filiales dans divers pays. Les petites et moyennes entreprises ont des inquiétudes sur ce qui sera exigé d'elles, mais je les rassure : d'une part certaines dérogations sont prévues pour les micros, petites et moyennes entreprises ; d'autre part, les entreprises qui étaient en conformité par rapport à la directive actuelle le resteront. Je conseillerais deux choses : tout d'abord faire un état des lieux de la situation au sein de l'entreprise sur ce qui se fait actuellement et la manière dont cela se fait, pour pouvoir estimer les éventuelles mesures correctrices à apporter. La seconde chose est de nommer un délégué à la protection des données, soit de manière interne - mais attention il doit être indépendant et rattaché directement à la gouvernance - soit de manière externe pour les entreprises de petite et moyenne taille, par exemple. Car un spécialiste sachant travailler de manière transversale et s'entourer des compétences internes sera un atout précieux.

Propos recueillis par
Rémi FARGETTE - AN2V.