BCTG • AVOCATS

RENDEZ-VOUS DU NUMÉRIQUE

SEPTEMBRE 2017

10 QUESTIONS SUR LE REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES ("RGPD"), par François-Xavier Boulin

A quelle date le Règlement sera-t-il applicable ?

Le Règlement sera "obligatoire dans tous ses éléments et directement applicable dans tout État membre", dont la France, le 25 mai 2018.

Puisqu'il s'agit d'un règlement, celui-ci entrera directement en vigueur, sans nécessiter de législation de transposition.

Néanmoins, dans de nombreux cas, le RGPD permet aux États membres de légiférer sur des problématiques relatives à la protection des données : traitement nécessaire au respect d'une obligation légale, démarche d'intérêt public, ou effectué par une autorité publique.

Le Règlement prévoit également que certaines de ses dispositions pourront être précisées ou restreintes par le droit des États membres, par exemple en matière de données personnelles des salariés.

Quelles sont les données concernées ?

Le Règlement ne s'applique qu'aux "données à caractère personnel" définies comme "toute information se rapportant à une personne physique identifiée ou identifiable".

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, physio logique, génétique, psychique, économique, culturelle ou sociale.

Quelles sont les activités et données concernées par le nouveau Règlement ?

Le Règlement s'applique aux traitements de données à caractère personnel, automatisés en tout ou partie, et aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans un fichier.

Constitue un traitement "toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensemble de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction".

Le RGPD ne s'applique cependant pas à certaines activités, parmi lesquelles les traitements couverts par la Directive relative à la protection des données personnelles traitées à des fins répressives ayant pour finalité la sécurité nationale et les traitements effectués par les personnes physiques dans le cadre d'activités exclusivement personnelles ou domestiques.

Quelles sont les entités concernées par le Règlement ?

Le RGPD s'applique aux responsables de traitement mais également aux sous-traitants disposant d'établissements dans l'Union Européenne, dès lors que des données à caractère personnel sont traitées dans le cadre des activités de tels établissements.

Il s'applique également aux organisations non établies dans l'Union Européenne et "ciblant" ou effectuant un "suivi" des personnes concernées dans l'Union Européenne, dans le cadre d'une "offre de biens ou services" (sans qu'il y ait nécessairement lieu à paiement) ou d'un "suivi" de leur comportement à l'intérieur de l'Union.

La simple accessibilité à un site internet à partir de l'UE ne devrait pas être suffisante ; la possibilité de passer des commandes, de payer en euros, etc, pourra suffire.

Qelles sont les sanctions prévues par le Règlement ?

Les sanctions prévues par le Règlement sont significatives :

- avertissement, mise en demeure, limitation temporaire ou définitive du traitement, suspension des flux de données, obligation de rectifier, limiter ou effacer, ...

- amendes administratives pouvant s'élever, selon la catégorie de l'infraction, à 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu.

Quels sont les nouveaux principes fixés par le Règlement ?

Le Règlement expose en détail les principes relatifs au traitement des données à caractère personnel (article 5) et les conditions de licéité des traitements (article 6).

Le principe essentiel animant le Règlement est celui d'accountability, c'est-à-dire de responsabilisation des opérateurs : afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment (= documenter la conformité).

Tout au long du processus de traitement des données, le responsable du traitement devra non seulement garantir mais aussi être en mesure de démontrer qu'il respecte les droits des personnes au regard des finalités du traitement et des risques inhérents au traitement.

Quelles sont les conséquences concrètes de ces nouvelles règles ?

L'une des conséquences de cette responsabilisation des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.

S'agissant des traitements actuellement soumis à une autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

Par ailleurs, le responsable de traitement (ou le sous-traitant) devra :

- Désigner un représentant basé dans l'Union Européenne ;

- Notifier les failles de sécurité aux autorités et personnes concernées ;

- Désigner un Délégué à la Protection des Données (DPO / Data Protection Officer) s'il appartient au secteur public, si ses activités principales l'amènent à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter (toujours à grande échelle) des données sensibles ou relatives à des condamnations pénales et infractions

- Mener des analyses d'impact sur la vie privée ;

- Tenir un registre des activités de traitements mis en œuvre (article 30), s'il compte plus de 250 employés ou si le traitement effectué est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il n'est pas occasionnel ou s'il porte notamment sur des données sensibles ou relatives à des condamnations pénales et infractions.

Qu'est-ce que le « Privacy by Design » ?

Ce principe nouveau est prévu à l'article 25 du Règlement.

Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.

Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (principe dit de "minimisation").

Seules les données nécessaires au regard de la finalité définie devront être traitées, ce qui impliquera que le responsable de traitement définisse avant toute traitement la "quantité" de données collectées, l'étendue du traitement, la durée de conservation ainsi que les modalités d'accessibilité aux données.

Quels sont les droits des personnes concernées ?

Le consentement des personnes concernées est soumis à des conditions supplémentaires : il doit s'agir de "toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement".

Le responsable du traitement doit être en mesure de prouver que la personne concernée a donné son consentement (article 7).

La personne a par ailleurs le droit de retirer son consentement à tout moment ; le consentement doit être aussi simple à retirer qu'à donner.

Si le consentement est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples.

Le Règlement reprend par ailleurs les droits "fondamentaux" des personnes concernées que nous connaissons déjà en droit français (droit d'information sur le traitement des données et les finalités, droit d'accès et de rectification et droit d'opposition) et en ajoute des nouveaux : droit à la limitation du traitement (article 18), droit à la portabilité des données (article 20), droit d'opposition au profilage (article 21), et droit à l'effacement ou au déréférencement (droit à l'oubli) (article 17).

Le Règlement contient par ailleurs des dispositions spécifiques sur le consentement des mineurs (par ex. : articles 8(2), 12, 38, 75).

Quelles actions sont à mettre en œuvre aujourd'hui pour assurer la mise en conformité des pratiques avec les nouvelles règles ?

Il importe d'auditer dès aujourd'hui les pratiques internes des différents services de l'entreprise (marketing, RH, IT...), mais également celles de ses partenaires.

Une étude des outils contractuels en place est également nécessaire, s'agissant en particulier des contrats avec les prestataires, des chartes internes, CGU, mentions d'information lors de la collecte des données..., pour s'assurer de leur pertinence.

Une fois cet audit réalisé, les actions de mise en conformité seront identifiées et pourront être initiées : mise en place d'un registre, désignation d'un DPO, modification des contrats ou clauses contractuelles, sécurisation des traitements, refonte des CGU et formules d'information, etc.

Une cartographie des traitements et la mise au point d'un référentiel des finalités et des traitements permettront de comprendre l'état des pratiques, d'alimenter le suivi des formalités et les évolutions nécessaires, et d'établir l'existence de pratiques conformes et à jour au regard du RGPD en cas de contrôle des autorités.