



# Application du RGPD aux sociétés établies hors de l'Union Européenne

publié le **02/06/2018**, vu **5207 fois**, Auteur : [Maître Naciri-Bennani Zineb](#)

**Le RGPD (le Règlement (UE) n°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 » (Règlement Général sur la Protection des Données) est paru au journal officiel de l'Union européenne entrera en application le 25 mai 2018. Ce texte vient mettre en conformité la réglementation applicable aux nouvelles réalités du numérique. Les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.**

Le RGPD (le Règlement (UE) n°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* » (Règlement Général sur la Protection des Données) est paru au journal officiel de l'Union européenne entrera en application le 25 mai 2018. Ce texte vient mettre en conformité la réglementation applicable aux nouvelles réalités du numérique. Les traitements déjà mis en œuvre à cette date devront d'ici là être mis en conformité avec les dispositions du règlement.

Il s'agit de renforcer la protection des droits des personnes, de responsabiliser les acteurs amenés à effectuer un traitement des données et de crédibiliser la régulation par une meilleure coopération entre les autorités chargées de la protection des données, les sanctions étant renforcées.

Le texte adopté est un règlement européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différents États membres.

Toutefois, le RGPD s'applique également au-delà des frontières de l'Union Européenne, ce dont résultent des obligations et un risque de sanction à l'encontre des sociétés hors UE devant se conformer aux dispositions du nouveau texte.

## Définition du traitement de données à caractère personnel

Aux fins du règlement, on entend par :

1- « *données à caractère personnel* » : 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, physiologique, génétique, psychique, économique, culturelle ou sociale ;

2- « *traitement* » : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles 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.

## **Application du RGPD au-delà du territoire de l'Union Européenne**

Le règlement s'applique dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union européenne ou que le responsable de traitement ou le sous-traitant met en œuvre des traitements visant à fournir des biens et des services aux résidents européens ou à les « cibler » (en anglais monitor).

En pratique, le droit européen s'appliquera donc chaque fois qu'un résident européen sera directement visé par un traitement de données, y compris par Internet.

Ainsi, selon l'article 3 du RGPD :

« 1. *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un **responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.***

2. *Le présent règlement s'applique au traitement des données à caractère personnel relatives à des **personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union**, lorsque les activités de traitement sont liées :*

a) *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou*

b) *au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.*

3. *Le présent règlement s'applique au traitement de données à caractère personnel par un **responsable du traitement qui n'est pas établi dans l'Union mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public.*** »

Autrement dit, le règlement s'applique dès qu'un résident européen sera visé par un traitement de données quelque soit le lieu d'implantation du responsable de traitements ou du sous-traitant.

Alors que le droit de la protection des données personnel antérieur au RGPD concerne principalement les responsables de traitements, le règlement étend aux sous-traitants une large partie des obligations imposées y prévues.

## **Conséquences de l'application du RGPD au-delà du territoire de l'Union Européenne**

Le RGPD impose la mise à disposition d'une information claire et aisément accessible aux personnes concernées par le traitement de données qui doivent exprimer un consentement explicite et positif au traitement en question.

### **Les droits des personnes concernées**

Le RGPD impose un consentement explicite et positif de la part de la personne concernée par le traitement des données. Ce consentement doit être éclairé en raison de l'obligation d'information préalable. La charge de la preuve repose sur le responsable de traitement (article 7 du RGPD).

«consentement» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement;

« Si le consentement de la personne concernée 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 ».

Pour la première fois, la législation européenne comporte des dispositions spécifiques pour les mineurs de moins de 16 ans. Dans un tel cas, l'information doit être rédigée en des termes clairs et simples que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale.

Par ailleurs, la personne concernée a le droit de retirer son consentement à tout moment et d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant (droit à l'oubli).

Le RGPD reconnaît un nouveau droit, le droit à la portabilité des données, qui permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable (« *dans un format structuré, couramment utilisé et lisible par la machine* »), et, le cas échéant, de les transférer à un tiers. Il s'agit de redonner aux personnes la maîtrise de leurs données.

Les associations actives dans le domaine de la protection des droits et libertés des personnes en matière de protection des données auront la possibilité d'introduire des recours collectifs en matière de protection des données personnelles. Les responsables du traitement et sous-traitants seront ainsi tenu, en vertu d'actions individuelles ou collectives, à la réparation de tout préjudice matériel ou moral subi par toute personne du fait de la violation du RGPD.

### ***Les nouvelles obligations***

Le RGPD prévoit de nouvelles obligations à la charge du responsable du traitement ou du sous-traitant centrées sur la responsabilisation des acteurs en allégeant les obligations déclaratives et en imposant de nouveaux outils visant à garantir le respect du règlement.

- *Protection des données dès la conception* : le règlement impose aux sociétés de prendre en compte les exigences relatives à la protection des données personnelles et ce, dès la conception des produits, services et systèmes exploitant des données à caractère personnel (« *Privacy by design* »).
- *Un allègement des formalités administratives et une responsabilisation des acteurs* : 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 (*accountability*). D'où la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes.
- *la tenue d'un registre des traitements mis en œuvre*
- *la notification de failles de sécurité (aux autorités et personnes concernées)*
- *la certification de traitements*
- *l'adhésion à des codes de conduites*
- *Les études d'impact sur la vie privée* : lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, le responsable du traitement doit effectuer, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la

protection des données.

- *La nomination d'un « Data Protection Officer »* ou délégué à la protection des données : lorsque le traitement est effectué par une autorité publique ou un organisme public (à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle), lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ou en un traitement à grande échelle de catégories particulières de données.
- *Notification en cas de violation des données à caractère personnel* : le responsable du traitement doit notifier la violation en question à l'autorité de contrôle compétente 72 heures au plus tard après en avoir pris connaissance.

## **Les sanctions de la violation du RGPD**

En plus de la réparation du préjudice subi par la personne concernée par le traitement, les responsables de traitement et les sous-traitants soumis au RGPD peuvent faire l'objet d'une panoplie de sanctions administratives selon la gravité des infractions : avertissement, mise en demeure, limitation des traitements, suspension des flux de données, ordre de rectifier, limiter ou effacer les données, amende ou encore retrait de la certification délivrée.

L'amende administrative s'élève à :

- 10 millions d'euros (ou 2% du chiffre d'affaires mondial annuel s'il s'agit d'une personne morale), notamment en cas de violations aux obligations relatives au consentement des enfants, violations relatives à la sécurité des données personnelles, etc ;
- 20 millions d'euros (ou 4% du chiffre d'affaires), notamment en cas de violation des dispositions relatives à la portabilité des données, violation des principes de base, violation des dispositions relatives au consentement et non-respect d'une injonction émise par l'autorité de contrôle.