

Le Règlement Général sur la Protection des Données (RGPD) en détail



Après quatre années d'âpres négociations, les États Membres de l'Union Européenne sont enfin convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995, laquelle datait des débuts d'Internet. Mais, contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril, par le Parlement européen, est d'application directe et s'imposera aux États Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.

Le processus d'élaboration du texte, long et émaillé de près de 4000 amendements, a mis au monde un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants. Intitulé « Règlement 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 », le texte résultant, complexe et technique, est particulièrement difficile à aborder par les entreprises et les administrations, lesquelles sont pourtant les principaux acteurs visés par le texte. Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que « 90% des entreprises des trois principales économies européennes (France, Allemagne, Royaume-Uni) ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) ». Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD » !

Les acteurs du traitement de données vont donc devoir investir considérablement pour se mettre à niveau de la nouvelle réglementation, d'autant que toutes les entreprises du monde traitent des données personnelles de citoyens européens sont concernées par le Règlement.

Nous nous proposons, à travers cet article, d'exposer les principales nouveautés du texte sous une forme compréhensible pour le non-initié. Nous dresserons au préalable un tableau général des intentions du texte (I) avant d'insister sur ses innovations principales (II).

I- Présentation générale du RGPD

Le but déclaré du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, tout en simplifiant, en l'unifiant, la réglementation pour les entreprises.

Les citoyens pourront désormais réclamer contre l'utilisation abusive de leurs données auprès d'une autorité unique, chargée de la protection des données, plutôt que de devoir le faire auprès de l'entreprise détentrice de leurs données. Les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives qui, si la loi nationale les y autorise, pourront agir de leur propre initiative.

Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées. Ainsi, des trois droits reconnus à la personne par la loi Informatique et Liberté (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), l'on passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition (notamment au profilage), etc.). D'une manière générale, la personne concernée dispose d'un droit étendu et facilité à accéder aux données à caractère personnel qui la concernent et le texte réaffirme les principes essentiels de la protection de la vie privée :

- Restriction d'utilisation ;
- Minimisation des données ;
- Précision ;
- Limitation du stockage ;
- Intégrité ;
- Confidentialité.

Les entreprises sont incitées à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection (concept de la prise en compte du respect de la vie privée dès la conception). La « pseudonymisation » consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

II- Principales mesures du RGPD

1. Réalisation d'une analyse d'impact avant la mise en place d'un traitement de données

Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'entreprise devra réaliser une analyse d'impact : « Lorsqu'un type de traitement, 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, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. » (Article 35 du Règlement)

Le RGPD introduit ainsi le concept de prise en compte du respect de la vie privée dès la conception du traitement ; les différentes obligations pesant sur la collecte des données doivent être prises en compte dès la conception du traitement de données (« privacy by design and by default »).

2. Consentement clair et explicite à la collecte des données

La directive 1995/46/CE donnait une définition du consentement à la collecte des données, laquelle a été transposée de manière très hétérogène dans les législations nationales, certaines exigeant un consentement explicite, d'autres décidant qu'un consentement implicite était suffisant. Notre loi Informatique et Liberté se contente ainsi de définir des cas dans lesquels le consentement devrait être explicite. Le Règlement vient unifier une fois pour toute cette définition au onzième point de son article 4 consacré aux définitions, en définissant le consentement comme « 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 ».

Ce consentement doit donc être expressif. Il doit résulter d'un acte positif. La personne doit réellement avoir été mise devant la nécessité de donner son accord au traitement. Ainsi, dans son considérant n°32, le Règlement précise qu'« il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité. » Plus encore, la charge de la preuve du consentement pèse sur le responsable du traitement (article 7, 1°). En outre, la personne dont les données sont collectées peut retirer son consentement à tout moment (article 7, 3°).

Malgré cela, le Règlement prévoit un certain nombre de cas pour lesquels le traitement demeure licite même sans consentement (article 6, b) à f) :

- Lorsque ce traitement est nécessaire à l'exécution d'un contrat accepté par la personne ;
- Lorsque le traitement découle d'une obligation légale ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- Tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne, en particulier s'il s'agit d'un enfant.

3. Accès facilité de la personne à ses données

Les personnes dont les données sont collectées disposent de droits à la rectification, à l'effacement des données et à l'oubli : « la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais » (Article 17), et ce pour six motifs : les données ne sont plus nécessaires, la personne concernée retire son consentement, la personne concernée s'oppose au traitement à des fins de prospection, les données ont fait l'objet d'un traitement illicite, les données doivent être effacées pour respecter une obligation légale, ou encore les données ont été collectées dans le cadre d'une offre de service à destinations de mineurs.

4. Notification des violations de données personnelles (« Data Breach Notification »)

À l'heure actuelle, les différentes directives européennes font peser sur les entreprises du secteur de la télécommunication l'obligation d'informer les autorités en cas d'accès non autorisé à des données personnelles. En clair, lors d'un piratage, le Règlement, quant à lui, généralise cette obligation de signalement à l'ensemble des responsables de traitement, et ce au plus tard 72 heures après la découverte du problème (Article 33). Bien entendu, il faut que le problème atteigne une certaine gravité pour qu'il soit nécessaire de le rapporter, et tout va donc dépendre de la détermination du seuil à partir duquel le signalement devient obligatoire. L'article 34 du Règlement indique que ce signalement devra intervenir « lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. » L'emploi du mot « élevé » laisse donc place à appréciation et donnera donc probablement lieu au développement d'une jurisprudence abondante.

Les personnes concernées par la violation des données doivent également être notifiées dans les meilleurs délais, sauf si des mesures de protection ont été mises en œuvre ou seront prises ultérieurement.

5. La création et la maintenance d'un registre des traitements devient obligatoire

Aux termes de l'article 30 du RGPD, un registre détaillé des traitements doit désormais être obligatoirement conservé non seulement par le responsable du traitement mais également par ses éventuels sous-traitants. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle.

Le texte insiste ainsi sur la responsabilité du contrôleur des données, lequel est responsable de la conformité du traitement avec le Règlement et doit être, à tout moment, en mesure de le démontrer.

Lorsque le traitement de données est délégué par le responsable du traitement à un sous-traitant, ou « data processor », même situé hors de l'Union Européenne, celui-ci a désormais les mêmes obligations que le responsable du traitement, y compris la désignation d'un délégué à la protection des données, et ce même dans le cas d'un traitement de données gratuits.

6. Création de délégués à la protection des données (Data Protection Officer)

Si notre loi Informatique et Liberté, et ses mises à jour, ont créé le Correspondant Informatique et Liberté (le « CIL »), le Règlement, quant à lui, rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPO ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont « les activités de base (-) exigent un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque « le traitement est effectué par une autorité publique ou un organisme public » (article 37), à l'exception des juridictions. Ce délégué n'est obligatoire que dans certains cas, mais il est fortement recommandé de le nommer systématiquement puisque toute entreprise ou administration doit être capable à tout moment de rendre comptes à l'autorité de contrôle de l'état de ses traitements de données.

Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance.

7. Le transfert des données est soumis à vérification et peut être demandé par la personne elle-même

Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. L'article 45 du Règlement prévoit que, dans l'idéal, le pays destinataire devra être listé par la Commission européenne. A défaut, des clauses de garantie spéciales devront être prévues dans les contrats, outre la possibilité de recourir à des codes de conduite, des certifications et autres labels. Auquel cas, il ne sera pas nécessaire d'obtenir une autorisation auprès de l'autorité nationale du pays d'origine des données.

En outre, l'article 49 du Règlement prévoit que, si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présente l'opération. Ceci, bien entendu, afin de permettre à la personne de revenir éventuellement sur son consentement.

Enfin, les personnes dont les données sont collectées disposent elles-mêmes d'un droit à demander le transfert des données les concernant (ou « droit à la portabilité des données ») vers un autre fournisseur de services : « Les personnes concernées ont 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, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle » (Article 20).

8. Restriction du profilage automatisé servant de base à une décision

L'article 21 du Règlement dispose que « la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire », sauf si ce traitement est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou bien que la décision est autorisée par le droit de l'Union européenne, ou bien encore que le consentement explicite de la personne concernée a été recueilli en amont.

9. Recours et aggravation considérable des sanctions

La directive 1995/46/CE prévoyait jusqu'ici simplement la possibilité, pour la personne dont les droits ont été violés, de recourir aux tribunaux et d'obtenir du responsable du traitement réparation de son préjudice.

Le Règlement prévoit quant à lui un « droit à un recours effectif » (articles 78 et 79) et un « droit à réparation » (article 82). Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (article 83). Or, les amendes mises en place par le Règlement sont considérables, puisqu'elles peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial ! Le risque qui pèse sur les entreprises imprudentes est donc très sérieux...[lire la suite]

Notre métier :

Nous proposons des services d'accompagnement sur plusieurs niveaux :

1/ Au niveau des utilisateurs qui, face à la résistance au changement, doivent comprendre l'intérêt des démarches de mise en conformité des traitements des données personnelles, pour favoriser leur implication et faciliter la mission du Correspondant aux Données Personnelles.

1'/ Au niveau des utilisateurs encore peu sensibilisés les utilisateurs aux différentes formes d'attaques et d'arnaques informatiques (cybercriminalité) dont les établissements sont très largement victimes.

Les services chargés de gérer les fournisseurs sont fortement incités à suivre notamment un module sur les arnaques aux FOVI et à voir leurs procédures auditées et probablement améliorées.

2/ Au niveau de l'établissement complet afin de faire un état des lieux des traitements concernés et un audit des mesures de sécurité en place et à faire évoluer pour les rendre acceptables vis à vis de la Réglementation relative aux Données Personnelles.

3/ Au niveau du futur CIL ou du futur DPO afin de lui faire découvrir ses missions, l'accompagner dans sa prise de fonction et l'accompagner au fil des changements.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Régissez-vous à cet article

Original de l'article mis en page : RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi Informatique et Liberté. Par Bernard Rineau, Avocat, et Julien Marcel, Juriste.