efcse.eu

OUTIL / Règlement Général de la Protection des Données [RGPD]

Auteur : Olivier de Maison Rouge, Vice-President EFCSE, Avocat
Mai 2018

Rappel des textes

24 octobre 1995 : Le Parlement européen et le Conseil adoptent la directive européenne 95/46 relative à la protection des données personnelles. Cette directive crée le premier cadre européen en la matière, mais les Etats membres ont une certaine souplesse dans transposition des règles de cette directive dans leur droit interne.

14 avril 2016 : Le règlement européen en matière de protection des données personnelles, initié en 2012, est adopté. Ce règlement apporte des changements importants dans les grands principes de la protection des données personnelles. Le règlement est directement applicable dans tous les pays de l'Union européenne.

RGPD : enjeux

À l'ère du big data (cloud, data mining, smart intelligence, blockchain, …) et sous l'impulsion soudaine des GAFAM (Google, Apple, Facebook, Amazon, Microsoft) et NATU (Netflix, Airbnb, Tesla, Uber), la donnée est devenue le pétrole du 21ème siècle. Son traitement, par algorithme, est devenu le moteur de la nouvelle économie digitale.

Dans ce contexte, le RGPD se substitue à la directive de 1995 le 25 mai 2018). Il a été adopté pour donner aux citoyens davantage de contrôles sur les informations privées les concernant.

Définition de la donnée à caractère personnel

Article 4 du RGPD : « 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. »

Tels que des adresses IP[1], des témoins de connexion sur internet, dits « cookies », des identifiants liés à l'appareil utilisé

Responsable du traitement

Le fait d'agir sur une donnée personnelle est dans tous les cas considéré comme un traitement de données personnelles.

1 Adresse IP (Internet Protocole) : c'est la base du système d'acheminement des données sur internet, il correspond au numéro d'identification qui est attribué de façon permanente ou provisoire à chaque branchement à un réseau informatique utilisant l'Internet Protocole.

Le responsable de traitement est l'entité à l'initiative du traitement, qui décide l'objectif de celui-ci et exploite effectivement les données ainsi que les moyens pour le réaliser.

Il peut exister plusieurs responsables pour un même traitement de données personnelles. Dans ce cas-là, les coresponsables de traitement sont conjointement tenus de respecter les obligations relatives au traitement.

Le responsable de traitement peut déléguer certaines opérations à un sous-traitant. Dans ce cas, il est toujours responsable au premier chef et doit veiller à ce que le sous-traitant respecte également les obligations qui lui incombent.

La règlementation s'applique même lorsque le sous-traitant est établi en dehors de l'Union européenne ; seule la localisation du responsable de traitement est prise en compte pour déterminer l'applicabilité de la loi.

Le traitement

Le règlement ne modifie pas de manière fondamentale le champ d'application matériel du droit de la protection des données.

Les traitements concernés par le règlement sont ceux comportant des informations ou données relatives aux personnes physiques.

Il résulte de l'article 2 du RGPD, que le « règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier ».

Les acteurs du traitement

Tout acteur économique susceptible de traiter des données à caractère personnel, qu'il soit responsable du traitement ou sous-traitant, doit se conformer aux dispositions du règlement : « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

Le destinataire

Le règlement apporte également un éclairage sur les notions de destinataire du traitement et de personne concernée.

Ainsi, le destinataire est : « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement ».

L'application territoriale

Les réseaux de communication et la circulation des données à caractère personnel s'effectuent par-delà les frontières. Dans un tel environnement, il n'est pas surprenant que le règlement affiche clairement une visée extraterritoriale.

Ainsi, les sociétés dont le siège social est situé dans un Etat non membre de l'Union européenne mais qui pèsent sur le marché européen ont vocation à être soumises aux mêmes règles que les sociétés de l'Union européenne. A bien des égards, une telle position apparaît de bon sens lorsque l'on songe à la difficulté pour localiser des données dans une société numérique.

L'article 3 du règlement étend son application aux responsables du traitement et sous-traitants établis sur le territoire de l'Union européenne ainsi qu'à ceux qui ne sont pas établis sur le territoire de l'Union européenne si leurs activités de traitement sont liées soit à l'offre de biens ou de services à des personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; soit 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.

Les autorités de contrôle

Le règlement consolide les missions de contrôle, de conseil et d'information des autorités nationales de contrôle (type CNIL en France).

Il leur confie un véritable pouvoir de dissuasion, d'une part, en mettant à leur disposition des pouvoirs répressifs significatifs et d'autre part, en mettant en œuvre un mécanisme de coopération et de cohérence renforcé entre autorités.

Le RGPD supprime les formalités préalables à accomplir auprès du régulateur national (création d'un « guichet unique »).

Le consentement de la personne

L'exigence du consentement de la personne concernée comme condition de la collecte licite de données n'est pas une nouveauté du règlement.

Mais, le consentement n'est qu'une des conditions de licéité de la collecte de données puisqu'un traitement est également légitime, en l'absence de consentement, s'il repose sur l'un des critères suivants :

- l'exécution d'un contrat ;
- le respect d'une obligation légale ;
- la sauvegarde des intérêts vitaux de la personne, l'exécution d'une mission d'intérêt public ;
- la poursuite d'intérêts légitimes.

La notion de consentement de la personne concernée est définie par l'article 4 du RGPD 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 ».

Le régime de protection

L'un des objectifs du règlement consiste en un renforcement des droits des personnes sur leurs données.

Un tel renforcement n'est pas sans faire peser un certain nombre de contraintes sur les entités concernées, lesquelles devront adapter leurs procédures de collecte et de traitement de données aux nouvelles dispositions.

Le droit de la personne se traduit par la communication des informations suivantes :

- l'identité et les coordonnées du responsable du traitement et, le cas échéant, de son représentant ;
- le cas échéant, les coordonnées du délégué à la protection des données (DPO) ;
- les finalités du traitement auquel sont destinées les données à caractère personnel, sa base juridique ;
- les catégories de données à caractère personnel concernées ;
- le cas échéant, les destinataires ou les catégories de destinataires des données à caractère personnel ;
- le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à un destinataire dans un pays tiers ou une organisation internationale.

Mais aussi :

- l'indication de la durée de conservation des données à caractère personnel
- l'existence d'un droit d'accès aux données à caractère personnel

  l'existence d'un droit de rectification
- l'existence d'un droit à l'effacement de ses données ou « droit à l'oubli »
- l'existence d'un droit à la limitation du traitement relatif à la personne concernée
- l'existence du droit de s'opposer au traitement
- l'existence d'un droit à la portabilité des données
- lorsque le traitement poursuit des finalités spécifiques, l'existence du droit de retirer son consentement à tout moment.
- le droit d'introduire une réclamation auprès d'une autorité de contrôle.

Le signalement des incidents

Les articles 33 et 34 du règlement obligent les responsables du traitement et les sous-traitants à notifier les violations de sécurité en aval.

La violation de données à caractère personnel se définit comme la violation de sécurité entrainant la destruction, la perte, l'altération ou la divulgation de données à caractère personnel traitées.

La notification d'une violation de données devra être effectuée auprès de l'autorité de contrôle nationale compétente dans un délai de 72 heures au plus tard après la prise de connaissance de la violation en ce qui concerne le responsable du traitement. Toute notification hors délai devra être motivée.

La notification pourra être effectuée au moyen d'un formulaire en ligne. Cette notification devra notamment indiquer quelles données ont été piratées et dans quelle quantité. Un rapport spécifique pour chaque Etat membre concerné devra être établi. Il en résulte que d'importants moyens technologiques devront être mis en œuvre par les responsables de traitement et les sous-traitants afin que toutes les informations requises soient transmises dans le délai imparti.

L'article 34 impose corrélativement au responsable du traitement l'obligation d'informer individuellement les personnes physiques concernées par une faille de sécurité dans les meilleurs délais, sauf à ce que cela exige des « efforts disproportionnés ». En pareille hypothèse, la communication sera effectuée publiquement.

En l'absence de notification, l'autorité de contrôle pourra, au regard de la gravité de la situation, exiger du responsable du traitement qu'il y procède.

La coresponsabilité

Le responsable du traitement doit garantir la conformité du traitement réalisé avec les dispositions du règlement, y compris en matière de sécurité.

Le responsable du traitement ne sera ainsi plus soumis au système de formalités préalables à la mise en œuvre des traitements tel qu'il résulte de la loi du 6 janvier 1978.

Cependant, l'article 34 du règlement prévoit un régime de consultations préalables de l'autorité de contrôle.

Les responsables de traitement seront tenus de mettre en place toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles.

Le règlement impose également la tenue, par les responsables de traitement, d'un registre des traitements mis en œuvre et comportant, dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles.

Le responsable du traitement n'est plus le seul à répondre auprès de l'autorité de contrôle des manquements à la réglementation. Les sous-traitants doivent présenter des garanties suffisantes de mise en œuvre de mesures techniques et organisationnelles conformes au règlement.

Les sous-traitants sont directement soumis à une obligation de sécurité et à une obligation de collaboration tant avec l'autorité de contrôle qu'avec les responsables de traitement.

Ils auront une mission d'assistance et de conseil auprès des responsables de traitement pour que ceux-ci puissent être conformes aux obligations du règlement

Le Délégué à la Protection des Données [DPO]

Aux termes de l'article 37, un DPO doit être obligatoirement désigné par les responsables de traitement et leurs sous-traitants :

- pour les traitements de données à caractère personnel mis en œuvre 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 nécessitent un suivi régulier et systématique à grande échelle des personnes concernées ;
- lorsque les activités de base du responsable de traitement ou du sous-traitant consistent à traiter à grande échelle des données sensibles.

Son rôle est :

- d'informer et conseiller les responsables de traitement et sous-traitants, ainsi que leurs employés ;
- de contrôler le respect de la réglementation sur la protection des données à caractère personnel ;
- de dispenser des conseils pour la mise en œuvre d'analyses d'impact et s'assure de leur réalisation ;
- de coopérer avec l'autorité de contrôle.
- d'exercer un rôle de sensibilisation et de communication renforcé par rapport au poste précédent (tel que le correspondant informatique et liberté [CIL] en France).

Transfert des données hors Union Européenne

Il ressort des disposions du règlement quatre modes de transfert de données à caractère personnel :

1) Les transferts fondés sur une décision d'adéquation adoptée par la Commission européenne constatant qu'un territoire ou plusieurs secteurs déterminés dans le pays ou l'organisation internationale en question assure un niveau de protection adéquat.

2) Les transferts moyennant des garanties appropriées (clauses types de protection des données adoptées par la Commission, clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission ; code de conduite assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, mécanisme de certification assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées.)

3) Les transferts dans le cadre des règles d'entreprise contraignantes (BCR[2]). Pour être conformes au règlement, les BCR devront garantir leur caractère opposable et contraignant tant aux entités qui forment le groupe qu'aux personnes concernées par les traitements ainsi que leur effectivité par la mise en œuvre de dispositifs adéquats. Le niveau de protection des données devra être validé par l'ensemble des autorités de contrôle européennes, conformément au mécanisme de contrôle de cohérence prévu à l'article 63. Le règlement supprime le mécanisme d'autorisation par la Commission Nationale de l'Informatique et des Liberté [CNIL], autorité administrative indépendante française, des transferts sur ce fondement.

4) Les transferts en vertu d'une décision d'une juridiction ou d'une autorité administrative d'un pays tiers fondée sur un accord international tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un Etat membre, sans préjudice d'autres motifs de transfert.

Pour les Etats Unis, se reporter à l'invalidation du « safe harbor » par la Cour de Justice de l'Union Européenne [CJUE] du 6 octobre 2015 et de l'adoption du « Privacy Shield » en juillet 2016.

Les sanctions

Les autorités de contrôle pourront émettre des sanctions administratives telles que :

- prononcer un avertissement ;
- mettre en demeure l'organisme défaillant ;
- limiter temporairement ou définitivement un traitement
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes ;
- ordonner la rectification, la limitation ou l'effacement des données.

Les amendes, applicables tant au responsable de traitement qu'au sous-traitant, sont déterminées en fonction du chiffre d'affaires annuel mondial.

[2] BCR [Binding Corporate Rules] : constituent les règles internes de l'entreprise, c'est un code de conduite définissant la politique de transferts des données personnelles. Elles permettent de présenter une protection adéquate aux données qui sont transférées depuis l'UE vers des pays tiers au sein d'une même entreprise ou d'un groupe.