Les dispositions du RGPD illustrées avec les principales positions des autorités de contrôles

RGPD : la protection des données à caractère personnel

20 fiches pour réussir et maintenir votre conformité

Aurélie Banck

4e édition

Gualino un savoir-faire de Lextenso

Aurélie Banck est juriste, DPO et Responsable pédagogique du DU DPO Evry Val d'Essonne. Elle est également professeur associé à l'Université d'Evry.

Suivez-nous sur www.gualino.fr

Contactez-nous gualino@lextenso.fr

1, Parvis de La Défense
92044 Paris La Défense Cedex
ISBN 978-2-297-13225-1

Sommaire

1	Le champ d'application des règles relatives à la protection des données	6
2	Les acteurs de la protection des données	10
3	Les principes fondamentaux de la protection des données	14
4	Le data protection officer	18
5	Le consentement des personnes concernées	22
6	Les données « sensibles »	26
7	L'Accountability	30
8	L'analyse d'impact relative à la protection des données	34
9	Les transferts de données hors Union européenne	38
10	L'obligation d'assurer la sécurité et la confidentialité des données	43
11	La notification des violations de données à caractère personnel	46
12	La sous-traitance	50
13	Les droits des personnes	54
14	Le profilage et la prise de décision automatisée	59
15	Les codes de conduite et les certifications	62
16	Les autorités de contrôle	65
17	Le Comité européen de la protection des données	69
18	Les recours et les sanctions	73
19	Les cookies et traceurs	78
20	Le maintien de la conformité au RGPD	84

PRÉSENTATION

Le Règlement général sur la protection des données adopté le 27 avril 2016 (Règlement 2016/679) – RGPD – applicable à compter du 25 mai 2018 est une réforme majeure du droit de la protection des données en Europe. Avec la Directive Prévention et détection des infractions pénales (2016/680), il compose le « **paquet data** » qui vise à harmoniser les règles de protection des données, renforcer les droits des personnes concernées et leur rendre le contrôle de leurs données, et à diffuser la conception européenne de la protection des données via son effet extraterritorial.

En France, cette réforme entraîne un basculement d'un régime administratif de formalités préalables à un régime de conformité globale dans le cadre duquel les entreprises et les organismes traitant des données doivent être en mesure de démontrer à tout moment qu'ils respectent les principes du Règlement. Le RGPD prévoit également la possibilité d'adopter des spécificités locales (une cinquantaine), ce qui lui donne un caractère hybride, entre un règlement et une directive.

Afin d'adopter ces spécificités et de transposer en droit français cette directive, le législateur a procédé à une modification de la loi du 6 janvier 1978.

L'année 2020 aura été marquée par les 2 ans de l'entrée en application du RGPD, plusieurs dizaines de sanctions prononcées dont certaines à l'encontre des géants du web (Google, Amazon, Twitter) mais également à l'encontre de plus petits acteurs (comme des médecins libéraux en France ou des particuliers à l'étranger), la première décision contraignante du CEPD visant à régler un conflit entre différentes autorités de contrôle et les premières décisions des juridictions civiles sur l'indemnisation du préjudice subi par des personnes concernées en matière de protection des données personnelles.

Cet ouvrage présente de manière synthétique les principales dispositions du RGPD, illustrées avec les principales positions des autorités de contrôles. Il s'organise en **19 fiches** permettant d'avoir une vision globale des règles relatives à la protection des données personnelles pour vous mettre en conformité et **1 fiche** pour la maintenir. Ces dispositions ont été complétées avec les spécificités françaises.

Ouvrage achevé de rédiger le 15 février 2021.

Repères

Les principaux textes applicables en matière de protection des données personnelles

6 janvier 1978	Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés, dite Loi *Informatique et Libertés*
28 janvier 1981	Convention pour la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, dite « Convention 108 »
24 octobre 1995	Directive 95/46/CE relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
18 décembre 2000	Charte des droits fondamentaux de l'Union européenne
8 novembre 2001	Protocole additionnel à la Convention 108 concernant les autorités de contrôle et les flux transfrontières de données
12 juillet 2002	Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, dite Directive « E-privacy »
6 août 2004	Loi n° 2004-801 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 (transposition de la Directive 95/46/CE en droit français)
27 avril 2016	Règlement 2016/679 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 (RGPD) Directive 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données
7 octobre 2016	Loi n° 2016-1321 pour une République numérique
10 janvier 2017	Projet de règlement européen E-privacy
25 mai 2018	Entrée en application du RGPD
20 juin 2018	Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles modifiant la loi *Informatique et Libertés*
12 décembre 2018	Ordonnance n°2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n°2018-493 du 20 juin 2018
29 mai 2019	Décret n° 2019-536 pris pour l'application de la nouvelle loi Informatique et Libertés

1 Le champ d'application des règles relatives à la protection des données

Pour relever du champ d'application de la Réglementation relative à la protection des données à caractère personnel, un organisme doit procéder à un traitement de données à caractère personnel dans un périmètre géographique déterminé.

Le champ d'application matériel

Une donnée à caractère personnel faisant l'objet d'un traitement

Les règles relatives à la protection des données sont applicables aux traitements de données à caractère personnel. On entend par « 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 » (RGPD, art. 4, 1). Il s'agit donc de données relatives à des personnes physiques (dites « personnes concernées ») ce qui exclut les informations relatives à des personnes morales (sauf dans l'hypothèse où elle permettrait d'identifier une personne physique).

La notion de données à caractère personnel est très large, incluant des **données directement nominatives** comme le nom et le prénom **ou indirectement** comme des identifiants, des données biométriques, un numéro de carte bancaire ou des données de localisation et bien entendu une adresse IP.

Ces données doivent faire l'objet d'un traitement, c'est-à-dire d'une opération ou d'un ensemble d'opération manuelle ou automatisée les concernant, « tel (...) 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 » (RGPD, art. 4, 2). Cette notion couvre toute opération relative à des données personnelles, qu'elle soit automatisée ou manuelle (ce qui inclut les fichiers papiers).

Données anonymisées/pseudonymisées

Les **données anonymisées** sont **exclues du champ d'application** de cette réglementation (RGPD, considérant 26). Il s'agit de données ne concernant pas une personne physique ou de données personnelles ayant été rendues anonymes de manière irréversible, c'est-à-dire via un processus permettant de garantir que la personne concernée ne pourra pas être réidentifiée par la suite.

Cette catégorie de donnée doit être distinguée des **données pseudonymisées**. Celles-ci restent qualifiées de données à caractère personnel car elles restent attachées à la personne concernée, par exemple à l'aide d'un identifiant. Les données sont dites pseudonymes lorsqu'elles ne peuvent « plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires ». Ces données supplémentaires doivent, en outre, être « **conservées séparément et soumises à des mesures techniques et organisationnelles** » afin de garantir qu'une information ne soit pas attribuée à une personne physique. L'utilisation de données pseudonymes permet cependant de réduire le risque pour les personnes concernées (RGPD, considérant 28). En effet, en cas de perte ou de vol, l'identité de l'individu n'est pas directement exposée. Il est, en effet, nécessaire pour identifier cette personne de disposer de la table reliant les identifiants à son identité.

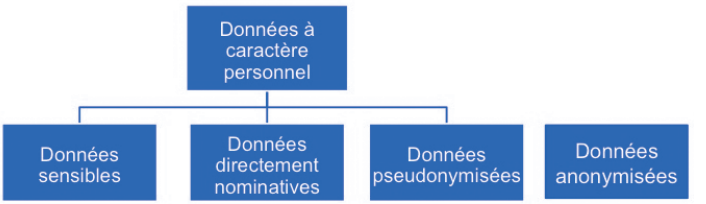
L'exception d'usage privé

Les activités purement personnelles ou domestiques sont exclues du champ d'application de cette réglementation. Nos **activités quotidiennes** peuvent justifier de collecter des données personnelles (par exemple la tenue d'un fichier d'adresses, ou d'une liste de contacts, l'utilisation de réseaux sociaux, etc.). Pour autant, si ce traitement est utilisé à des fins uniquement personnelles et « **sans lien avec une activité professionnelle ou commerciale** » (considérant 18), il n'est **pas soumis au respect du RGPD**.

À noter cependant que les responsables du traitement et les sous-traitants proposant des outils ou des solutions technologiques pour procéder à ces traitements doivent respecter le RGPD (considérant 18). Ainsi, le fabricant d'un bracelet électronique utilisé à des fins purement personnelles par ses utilisateurs sera tenu de mettre en œuvre le principe de ***Privacy by design*** et ***Privacy by default*** (v. Fiche 7).

Le RGPD n'est pas non plus applicable aux activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne et aux traitements de prévention et de détection des infractions pénales, d'enquêtes et de poursuite qui font l'objet de la Directive 2016/680 du 27 avril 2016.

Synthèse sur les données



Le champ d'application géographique

Le RGPD est **applicable aux organismes établis en Europe mais pas seulement**. Afin de garantir aux européens, un niveau de protection des données équivalent quel que soit le lieu de traitement de leurs données, le législateur a doté le RGPD d'un **effet extraterritorial** (art. 3).

Les organismes établis sur le territoire de l'Union européenne

Le RGPD « 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** ». Le considérant 22 précise que « l'établissement suppose l'exercice effectif et réel d'une activité au moyen d'un dispositif stable. La forme juridique retenue (...) qu'il s'agisse d'une succursale ou d'une filiale ayant la personnalité juridique n'est pas déterminante à cet égard ».

Les dispositions du RGPD sont cohérentes avec la décision de la Cour de justice de l'Union européenne du 1er octobre 2015 (Weltimmo c/ NAIH, n° C-230/14) qui, à cette occasion, avait retenu une définition souple de la notion d'établissement et relever qu'elle s'étend à toute activité réelle et effective, même minime exercée au moyen d'une installation stable. Elle n'est donc pas liée à un éventuel enregistrement administratif.

Les organismes traitant des données personnelles de personnes situées en Europe

Même dans l'hypothèse où un organisme ne serait pas établi sur le territoire de l'Union européenne, il peut être soumis aux dispositions du RGPD s'il met en œuvre des activités de traitements liées :

- « à l'offre de biens ou de services à [d]es personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ou
- 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 traitements mis en œuvre doivent donc présenter l'une de ces caractéristiques. Les entreprises ou organismes étrangers qui collectent des données sur des personnes situées en Europe (par exemple par l'intermédiaire d'un site web) rentrent donc potentiellement dans le périmètre d'application du RGPD.

Le considérant 23 précise qu'« afin de déterminer si un (...) responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, il y a lieu d'établir s'il est clair que [cet organisme] **envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union** ». Selon le législateur, la simple

accessibilité du site internet, d'une adresse électronique ou d'autres coordonnées ou « l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention ». Il convient de prendre en compte des facteurs comme « l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union ». C'est donc l'**intention du responsable du traitement** ou du sous-traitant qu'il faut établir sur la base d'un **faisceau d'indices**.

Le CEPD a publié, en octobre 2019, des lignes directrices sur l'application territoriale du RGPD détaillant des critères à prendre en compte. Il s'agit notamment de :

- la nature internationale de l'activité de l'organisme concerné (comme les activités touristiques) ;
- la mention d'itinéraires à partir d'autres États pour se rendre au lieu d'établissement de l'organisme en question ;
- l'utilisation d'une langue ou d'une monnaie autres que celles utilisées dans l'État dans lequel l'organisme est établi ;
- la mention de coordonnées téléphoniques avec l'indication d'un préfixe international ;
- l'utilisation d'un nom de domaine de premier niveau autre que celui de l'État où le commerçant est établi ;
- la mention d'une clientèle internationale composée de clients domiciliés dans des États membres, etc.

C'est la même démarche qui devra être utilisée pour déterminer si le responsable du traitement ou le sous-traitant entend suivre le comportement de personnes situées en Europe. *A priori*, ce cas vise plutôt le suivi de personnes physiques sur internet par l'intermédiaire de dispositifs de tracking (RGPD, considérant 24).

À noter que le critère d'applicabilité territoriale du RGPD n'est pas lié à une notion de citoyenneté ou de résidence mais au fait d'être sur le territoire européen (ainsi un américain à Paris bénéficiera de cette protection).

Focus sur le champ d'application territoriale des spécificités locales

Le RGPD prévoit la possibilité pour les États membres d'adopter des spécificités locales. Le législateur français a utilisé cette faculté. L'article 3, II de la loi Informatique et Libertés précise que les règles nationales « s'appliquent dès lors que la personne concernée réside en France, y compris lorsque le responsable du traitement n'est pas établi en France ». Seul le critère de résidence des personnes concernées a donc été retenu.

À noter que d'autres pays européens ont adopté des critères différents.

2 Les acteurs de la protection des données

Les règles de la protection des données font intervenir différentes catégories d'acteurs, dont les missions, les prérogatives et le niveau de responsabilité varient.

Le responsable du traitement

Le responsable du traitement est « 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** » (art. 4, 7°). Il s'agit donc de l'entreprise, de l'administration… qui décide de la mise en œuvre d'un traitement et qui de ce fait en **assume la responsabilité**.

Un texte de droit européen ou national peut également désigner un responsable du traitement (ou les critères permettant de procéder à cette désignation). En France, c'est notamment le cas du **Fichier national des incidents de remboursements des incidents des crédits aux particuliers** (FICP) qui est placé sous l'autorité de la Banque de France.

Le Règlement européen reconnaît également des cas de responsabilité conjointe, c'est-à-dire des situations dans lesquels les finalités et les moyens d'un traitement sont déterminés par deux organismes ou plus. Ces organismes sont alors qualifiés de responsables conjoints de traitement (ou de co-responsables de traitement).

Le sous-traitant

Le sous-traitant est défini à l'article 4, 8° du RGPD comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui **traite des données à caractère personnel pour le compte du responsable du traitement** ». Un prestataire qui procède à des opérations de traitement au nom et pour le compte d'un responsable du traitement a donc la qualité de sous-traitant.

Le sous-traitant doit être **distingué du destinataire des données**. En effet, il n'est pas autorisé à utiliser les données pour son propre compte ou à les communiquer à un tiers à son initiative, sauf dispositions législatives ou réglementaires le prévoyant (v. *infra*, Les tiers autorisés).

Le considérant 18 du RGPD précise également que le Règlement s'applique « aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de[s] activités personnelles ou domestiques ». Comme nous l'avons vu précédemment (v. Fiche 1), les activités purement personnelles ne sont pas soumises au RGPD. Toutefois, les solutions que les personnes concernées sont susceptibles d'utiliser à cette fin (par exemple un hébergeur ou un service de coffre-fort électronique personnel) doivent être conformes au Règlement.