RGPD : la protection des données à caractère personnel

5e édition

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

20 fiches pour réussir et maintenir votre conformité

DROIT EN POCHE

Aurélie Banck

Gualino un savoir-faire de Lextenso

RGPD : la protection des données à caractère personnel

5e édition

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

20 fiches pour réussir et maintenir votre conformité

DROIT
EN POCHE

Aurélie Banck

Gualino un savoir-faire de Lextenso

DROIT
EN POCHE

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

© 2023, Gualino, Lextenso
1, Parvis de La Défense
92044 Paris La Défense Cedex
EAN 9782297224437
ISSN 2276-2809

Cet ouvrage a été achevé d'imprimer
dans les ateliers de Leitzaran (Espagne)
Numéro d'impression : 801 – Dépôt légal : Mars 2023

PEFC
PEFC/14-38-00338

SOMMAIRE

PRÉSENTATION

Le Règlement général sur la protection des données adopté le 27 avril 2016 (Règlement 2016/679) – RGPD – applicable depuis le 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 pour 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 « Informatique et Libertés » du 6 janvier 1978.

L'année 2022 aura été marquée par les 4 ans d'application du RGPD, plusieurs dizaines de sanctions prononcées pour un montant de plus de 830 millions d'euros, à l'encontre de géants du web (Meta, Microsoft...) mais également à l'égard de plus petits acteurs (comme des médecins libéraux ou des particuliers), la publication d'une dizaine de lignes directrices de la part du CEPD et de nouvelles décisions contraignantes visant à régler des conflits entre différentes autorités de contrôle. Alors même que les autorités de protection des données se sont engagées dans le cadre de la déclaration de Vienne en avril 2022 à renforcer leur coopération et que les débats sur leur efficacité à faire appliquer le RGPD enflent, la Commission européenne, dans le cadre de la stratégie digitale de l'UE, multiplie les textes visant à réguler les données (on peut notamment citer le projet de règlement sur la donnée « Data Act », celui sur l'intelligence artificielle « Intelligence Artificial Act » ou le règlement sur la gouvernance des données « Data Gouvernance Act » adopté à l'été 2022).

Par ailleurs, les juridictions civiles se saisissent d'une manière anachronique de la question de 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 6 janvier 2023.

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

FICHE 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** permettant **d'identifier des personnes de manière directe** comme le nom et le prénom **ou indirecte** 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.

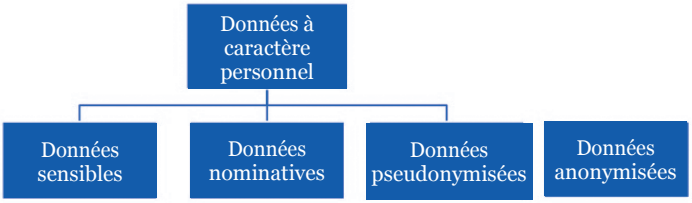
L'exception d'usage privé

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 individus, 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 relevé 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).

Ce critère a été illustrée par la CNIL dans le cadre de l'affaire Clearview AI (délibération n° SAN-2022-019 du 17-10-2022). Clearview aspire des photographies figurant sur des sites internet afin de mettre à la disposition de ces clients une base de données d'images permettant de rechercher un individu sur la base de sa photographie. En l'espèce, la CNIL a considéré que « le traitement [...] permett[ait] la création de profil comportemental et [leur] mise à disposition des personnes effectuant des requêtes dans le moteur de recherche de la société [devait] être qualifié de suivi sur internet ». La société a donc été sanctionnée, bien que n'étant pas établis au sein de l'UE (2 autres autorités de protection des données européennes ont également prononcé des sanctions à l'égard de cette société en 2022 pour des faits similaires).

Inversement dans une décision en date du 20 décembre 2022 (délibération n°SAN-2022-024), la CNIL a considéré que la société Lusha Systems INC. n'était pas soumise au RGPD dans la mesure où le service proposé par cette dernière, en l'occurrence, le rapprochement entre des données de contacts professionnels avec l'identité des personnes dont le profil est visité sur LinkedIn afin d'en vérifier la véracité, ne vise pas à analyser ou prédire un comportement, les préférences ou les déplacements, etc.

Focus sur le champ d'application territoriale des spécificités locales

Le RGPD prévoit la possibilité pour les États membres d'adopter des spécificités locales aussi appelées marges de manoeuvre. 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.

FICHE 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.

À noter que si **un sous-traitant** « détermine les finalités et les moyens du traitement, il est **considéré comme un responsable du traitement** » pour ce qui le concerne (art. 28, 10). Ainsi, dans l'hypothèse où un sous-traitant réutiliserait des données communiquées par un responsable du traitement en violation du contrat qui les lie, il serait responsable de cette réutilisation.

Enfin, tout prestataire de service n'a pas la qualité de sous-traitant au sens du RGPD. Un prestataire autonome dans la définition des finalités et des moyens d'un traitement de données sera qualifié de responsable du traitement.

Le Data Protection Officer ou Délégué à la Protection des Données

Le **Data Protection Officer** (DPO) ou le Délégué à la Protection des Données (DPD) qui succède au Correspondant à la protection des données (CIL) est un **acteur central de la conformité au Règlement** (v. Fiche 4).

À noter que les responsables du traitement ou sous-traitants non établis en Europe mais rentrant dans le champ d'application du Règlement doivent désigner un représentant sur le territoire de l'Union européenne (v. Fiche 1). L'article 27 précise que cette désignation doit être effectuée par écrit et qu'elle doit être assortie d'un mandat faisant du représentant le point de contact des autorités de contrôle et des personnes concernées (art. 27, 4). La désignation de ce représentant est cependant assortie d'exceptions.

Les lignes directrices du CEPD sur le champ d'application territoriale du RGPD précisent les obligations et responsabilités de cet acteur.

Le destinataire

L'article 4, 9° définit le destinataire comme « 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** ». Le destinataire d'un traitement de données est donc la personne, le service, la direction (etc.) qui de manière habituelle reçoit communication des données. Il a été préalablement autorisé par le responsable du traitement à prendre connaissance de ces données, habilitation reposant sur le principe du moindre privilège (prévoyant une limitation des accès des utilisateurs aux seules données strictement nécessaires à l'exercice de leurs missions) et formalisée dans une politique de gestion d'accès.

Les autorités publiques qui reçoivent communication de données dans le cadre d'une mission d'enquête particulière ne sont pas considérées comme des destinataires. En droit français, elles sont qualifiées de tiers autorisés.

Les tiers autorisés

L'article 4, 10° précise ainsi qu'un tiers est « une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, **placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel** ».

Des dispositions législatives et réglementaires spécifiques permettent à certaines administrations et autorités publiques de se faire communiquer, sous certaines conditions et dans le cadre de leur mission, des données à caractère personnel ou d'exercer un droit de communication. Ainsi, les autorités judiciaires ou l'administration fiscale peuvent solliciter un responsable du traitement pour que celui-ci leur communique des données à caractère personnel concernant ses clients ou ses employés. Elles recevront donc ces informations sans pour autant en être un destinataire habituel. Elles sont alors qualifiées de tiers autorisé. La CNIL a publié en juillet 2020 un guide des tiers autorisés.

Les autorités de contrôle (autorité chef de file, autorité de contrôle concernée, etc.)

Le Règlement européen introduit la possibilité pour un Groupe de sociétés établi dans plusieurs États membres de désigner une autorité de contrôle dite « autorité chef de file » qui sera compétente pour contrôler certains traitements (v. Fiche 16). **L'autorité chef de file** est définie comme « **l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant** » (art. 56, 1).

L'introduction de cette nouvelle autorité n'a pas pour autant pour effet de priver l'autorité de contrôle sur le territoire de laquelle le dommage serait survenu de toutes prérogatives, l'autorité est alors dite « concernée ».

Une autorité est dite « concernée » dans les hypothèses suivantes (art. 4, 22) :

- le responsable du traitement ou le sous-traitant en cause est établi sur le territoire de l'État membre dont cette autorité de contrôle relève ;
- des personnes concernées résidant dans l'État membre de cette autorité de contrôle sont sensiblement affectées par le traitement ou sont susceptibles de l'être ;
- une réclamation a été introduite auprès de cette autorité.

Cette distinction entre autorité chef de file et autorité concernée applicable dans les cas où un organisme aura désigné une autorité chef de file. Elle n'est donc pas applicable à toutes les situations, ce qui a conduit le législateur européen à utiliser d'une manière générique la notion d'« **autorité compétente** », à charge pour le lecteur de déterminer celle-ci.

À noter enfin que les éditeurs de logiciel et les fournisseurs de produits ne sont pas *stricto sensu* soumis aux dispositions du RGPD, s'ils ne traitent pas de données à caractère personnel. Toutefois, les produits et services qu'ils développent et mettent à la disposition de leurs clients influencent la capacité de ces derniers à respecter leurs obligations au titre du RGPD. Dès lors, on peut imaginer que le marché sera une source de régulation de ces acteurs.

Les personnes concernées

Il s'agit des personnes dont on traite les données (clients, prospects, etc.).

Le RGPD prévoit également des dispositions spécifiques pour les enfants et le CEPD a créé une catégorie de personnes dites vulnérables dont font notamment partie les salariés.

Le Contrôleur Européen de la Protection des Données (CEPD ou EDPS)

Il s'agit de l'organe de contrôle des institutions européennes en matière de protection des données (en anglais *European Data Protection Supervisor* – EDPS). Il est donc **compétent pour contrôler les pratiques** de ces institutions **en matière de protection des données**. Le Règlement l'investit également de nouvelles missions. **Il devient, en effet, le secrétariat du Comité Européen de la Protection des Données** (CEPD) (v. Fiche 17).

Le Comité Européen de la Protection des Données (CEPD ou EDPB)

Le Comité Européen de la Protection des Données (CEPD - en anglais *European Data Protection Board* - EDPB) est l'héritier du Groupe de l'article 29 ou G29. Ce groupe créé par l'article 29 de la Directive 95/46/CE dont il tire son nom, était un organe consultatif et indépendant regroupant l'ensemble des autorités de contrôle, le Contrôleur Européen de la Protection des Données et la Commission européenne. Il émettait des avis et des recommandations.

Suite à l'entrée en application du RGPD, il est devenu le **Comité Européen de la Protection des Données** (v. Fiche 17).

FICHE 3

Les principes fondamentaux de la protection des données

Tout traitement de données à caractère personnel doit respecter les principes fondamentaux énoncés à l'article 6 du RGPD. Ces derniers s'inscrivent dans la continuité de la Directive 95/46/CE et de la loi *Informatique et Libertés*.

Il convient donc d'analyser l'ensemble des traitements à la lumière de ces principes avant toute collecte de données. Cette analyse devra être documentée afin de répondre aux exigences d'« **Accountability** » (v. Fiche 7).

Le principe de limitation des finalités

Les données sont « collectées pour des **finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ». **La finalité correspond à l'objectif poursuivi par le responsable du traitement** dans le cadre de la mise en œuvre d'un outil ou d'un logiciel (par exemple la gestion de la paie, la mise en place d'un programme de fidélité, etc.). Une **même collecte** de données peut répondre à **plusieurs objectifs distincts**.

La ou les **finalités doivent être** :

- « **déterminées** » préalablement, ce qui exclut toute collecte de données au hasard ou à des fins préventives ;
- « **explicites** », c'est-à-dire communiquées à la personne concernée (v. Fiche 13 sur les droits des personnes concernées) ;
- et « **légitimes** » par rapport à l'activité de l'organisme mettant en œuvre le traitement (ainsi, une société de droit privé ne peut pas prétendre tenir un casier judiciaire).

Un traitement ultérieur pour une autre finalité peut être possible sous certaines conditions ; en particulier, sous réserve que cette finalité ultérieure soit considérée comme compatible avec la finalité initiale du traitement (RGPD, art. 6, 4). Une réutilisation des données « à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques » effectuée conformément à l'article 89 du RGPD, sera présumée compatible avec les finalités initiales.

En cas de réutilisation des données pour une autre finalité, l'organisme est susceptible de voir sa responsabilité engagée pour détournement de finalité. La CNIL a, ainsi, déjà mis en demeure des sociétés d'assurance pour avoir utilisées des données personnelles collectées exclusivement pour le versement des allocations de retraite à des fins de prospection commerciale (délibérations n°MED-2018-034 du 25-9-2018 et n°2018-333 du 11-10-2018) ou prononcé un rappel à l'ordre à l'encontre d'une députée et d'un rectorat suite à l'utilisation du fichier OCEAN, utilisé

habituellement à des fins de gestion des examens et concours nationaux pour adresser des courriers de félicitations aux bacheliers (délibérations SAN-2020-005 et SAN-2020-006 du 3-09-2020). L'autorité belge de protection des données a prononcé une sanction de 5 000 euros à l'encontre d'un bourgmestre pour avoir utilisé des données collectées dans le cadre de sa fonction afin d'adresser un courrier à des fins de campagne électoral (décision quant au fond 10/2019 du 25/11/2019).

Dans une décision du 20/10/2022 (C-77/21), la Cour de justice de l'UE a identifié cinq critères permettant de qualifier une finalité de « compatible » :

- l'existence d'un lien éventuel entre la finalité initiale et la ou les finalités ultérieures ;
- le contexte de la collecte des données en particulier s'il existe une relation entre les personnes concernées et le responsable de traitement ;
- la nature des données ;
- les conséquences possibles du traitement pour les personnes concernées ;
- l'existence de garanties appropriées dans le cadre du traitement initial et du traitement ultérieur.

Le principe de licéité, de loyauté et de transparence

Les données doivent être « **traitées de manière licite, loyale et transparente au regard de la personne concernée** ».

Pour être licite un traitement de données doit reposer sur un fondement, c'est-à-dire répondre à l'une des conditions énoncées à l'article 6. La personne concernée doit consentir au traitement ou celui-ci doit être nécessaire :

- à l'exécution de mesures contractuelles ou précontractuelles prises à sa demande ; la personne concernée doit avoir une relation contractuelle directe avec le responsable du traitement ;
- au respect d'une obligation légale s'imposant au responsable du traitement ;
- à la sauvegarde de la vie de la personne concernée ou d'une autre personne ;
- à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; à noter qu'il doit s'agir d'une obligation légale de droit européen ou de droit national. Les obligations légales de droit étranger ne peuvent donc constituer une base légale au titre de l'obligation légale ;
- aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée.

Pour aider les responsables du traitement à définir le fondement le plus adapté, la Cnil a récemment publié des recommandations sur son site internet et le CEPD a adopté en octobre 2019 des lignes directrices relatives à l'utilisation de la base légale du contrat dans le cadre de la fourniture de services en ligne (Lignes directrices 2/2019).

Dans l'hypothèse où le responsable du traitement souhaiterait utiliser la base légale de l'intérêt légitime, il devra procéder à une balance des intérêts entre ses intérêts ou ceux du tiers le poursuivant et les droits et libertés des personnes concernées. Cette analyse devra être documentée pour chaque traitement.

L'exigence de loyauté et de transparence renvoie à l'information des personnes concernées (v. Fiche 13) et vise à éviter les traitements occultes ou cachés. Un traitement déloyal exposera son auteur à un risque de sanction.

La minimisation des données

Les données doivent être « **adéquates, pertinentes et limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ».

Également appelé **principe de proportionnalité**, il vise à garantir que l'ensemble des données collectées est strictement nécessaire par rapport à l'objectif poursuivi et à exclure toute collecte réalisée au cas où ces données se révéleraient utiles a posteriori. La CNIL a déjà sanctionné des organismes pour collecte excessive de données notamment dans le cadre de zones de texte libre.

Exemples

La société SPARTOO a été sanctionnée par la CNIL notamment pour manquement au principe de minimisation des données. Cette société enregistrait de manière intégrale et permanente les appels téléphoniques reçus par les salariés à des fins de formation (délibération n° SAN-2020-003 du 28-07-2020).

En juillet 2022, l'autorité belge de protection des données a prononcé une sanction à l'encontre d'un centre social pour avoir solliciter une enquête socio-financière dans le cadre de l'admission d'une résidente alors que l'administrateur de son patrimoine avait justifié à plusieurs reprises de ses ressources (DOS-2021-01011).

L'exactitude des données

Les données doivent être « **exactes** et, si nécessaire, **tenues à jour** ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder – doit avoir du sens par exemple pas de correction d'historiques si exactes ».

Le responsable du traitement doit donc s'assurer que les données dont il dispose sont exactes et, le cas échéant, supprimer les données obsolètes. Dans certains cas, il devra mettre en place des

mesures permettant de s'assurer que les données sont toujours d'actualité (par exemple demander régulièrement à ces clients si leurs données sont à jour, mettre en place une procédure d'actualisation de l'adresse en cas de retour de courrier avec la mention n'habite pas à l'adresse indiquée, etc.).

La limitation de la conservation

Les données sont « conservées sous une forme permettant l'identification des personnes concernées pendant une **durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées** ». Elles ne peuvent donc pas être stockées *ad vitam aeternam* mais pour une **durée déterminée, permettant de répondre à la finalité du traitement**.

Une conservation plus longue est possible sous réserve que les données soient « traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée ».

En termes de conservation, on distingue généralement :

- la conservation des données en « **base active** » lorsqu'elles sont nécessaires à la réalisation d'une tâche ou au fonctionnement d'un process ;
- l'**archivage intermédiaire** lorsque les données ne sont plus nécessaires au quotidien mais qu'elles doivent être conservées en cas de contentieux ;
- l'**archivage définitif** généralement à des fins d'archives ou historiques.

Par exemple en matière de ressources humaines les données relatives à un collaborateur seront conservées en base active pendant toute la durée de sa présence dans l'entreprise ; en cas de départ, elles seront basculées en archives intermédiaires afin de réduire le périmètre des utilisateurs susceptibles d'en prendre connaissance.

L'absence de définition et d'application d'une durée de conservation peut donner lieu à une sanction. Ainsi, la société DISCORD INC a été sanctionné en novembre 2022 pour défaut de définition d'une politique de durée de conservation, la CNIL ayant constaté lors de ses investigations que plus de 2 millions de comptes utilisateurs n'avaient pas été utilisés depuis plus de 3 ans et 58 000 depuis plus de 5 ans (délibération SAN-2022-020). Elle a également prononcé une amende d'un montant de 1,75 million d'euros à l'égard d'un assureur pour défaut d'implémentation de sa politique de conservation (délibération SAN-2021-010 du 20-07-2021). La société Carrefour a également été sanctionnée par la CNIL pour conservation excessive de données sur des clients inactifs (délibération n° SAN-2020-008 du 18-11-2020).