

Mai 2018

Données à caractère personnel : votre conformité

Règlement Général sur la
Protection des Données

Loi de modernisation de la
justice du XXIème siècle

Loi relative à la protection
des données personnelles



Ce document est la propriété du Cabinet d'Avocats Mathias. Toute reproduction et représentation est soumise à l'autorisation préalable du Cabinet d'Avocats Mathias et au respect des dispositions du Code de la Propriété Intellectuelle.

SOMMAIRE

INTRODUCTION	05
HISTORIQUE	06
LES NOTIONS ESSENTIELLES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL	08
LES ACTEURS DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL	09
LES GRANDS PRINCIPES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL	10
L'APPLICATION TERRITORIALE	12
LE PRINCIPE D'ACCOUNTABILITY	14
L'ANALYSE D'IMPACT	19
LA GESTION DE CRISE RENFORCEE	25

LE DPO AU CŒUR DE LA DEMARCHE DE CONFORMITE	27
LES OBLIGATIONS DES SOUS-TRAITANTS	34
LA RESPONSABILITE CONJOINTE DE TRAITEMENTS	38
LE RENFORCEMENT DES DROITS DES PERSONNES ET LA CONSECRATION DE NOUVEAUX DROITS	40
LES TRANSFERTS DE DONNEES A CARACTERE PERSONNEL	46
LE RÔLE DES AUTORITES DE CONTRÔLE APRES LA SUPPRESSION DE FORMALITES PREALABLES	48
LE CARACTERE DISSUASIF DES SANCTIONS	52
L'ACTION DE GROUPE	54

INTRODUCTION

Le 25 mai 2018, date d'entrée en application du Règlement général sur la protection des données, devient une réalité pour tous les acteurs (administrations, grands comptes, startup, etc.).

Ce texte s'appliquera au sein des 28 Etats membres de l'Union européenne ainsi qu'à tous traitements de données à caractère personnel visant à fournir des biens et des services aux résidents européens ou à les « cibler ».

Indépendamment du montant conséquent des sanctions en cas de manquements, les données à caractère personnel sont au cœur de l'économie avec de nouveaux usages exponentiels (l'intelligence artificielle, data mining, etc.).

Le RGPD (ou GDPR, en anglais) loin d'être un frein, a comme volonté de permettre à, chaque acteur, de mettre en œuvre sa conformité en définissant ses propres mesures, procédures grâce notamment à une cartographie des données, des flux entre les différents prestataires ainsi qu'une sécurisation des contrats (responsabilisation des acteurs).

Cette conformité doit être « gagnant - gagnant » tant pour les usagers (« nous tous ») avec ce besoin de confiance, de transparence renforcée, que pour les professionnels en renforçant leur crédibilité. N'oublions pas que dans cette économie digitale, les données à caractère personnel sont des actifs immatériels ayant une valeur

économique certaine.

Des outils de conformité, de gouvernance sont d'ores et déjà mis à disposition des acteurs afin de leur permettre d'avoir leur propre gestion du risque comme le registre, les PIA ou encore le fait de se préparer à désigner un Délégué à la Protection des Données (DPO, véritable clef de la voûte de la conformité).

En outre, en France, la culture « protection des données à caractère personnel » est mise en œuvre depuis 1978. Certains acteurs ont désigné un Correspondant Informatique et Libertés depuis 2005. Il est donc possible de s'appuyer sur un existant. Le projet de loi modifiant la loi n°78-17 relative à l'informatique, aux fichiers et aux libertés intégrant certains aspects du RGDP s'inscrit dans cette continuité.

En tant que Conseil, nous sommes confrontés quotidiennement à la gestion des enjeux stratégiques, nous accompagnons les acteurs dans leur conformité juridique et leur transformation numérique.

Nous vous souhaitons une bonne lecture, en espérant sincèrement que les lignes qui suivent pourront vous être utiles dans vos projets.

Restant à votre écoute,

Garance Mathias

Avocat à la Cour

Fiche 1 - Un rappel de l'historique

2016 a été l'année de la protection des données à caractère personnel. Après quatre années de débats, la Commission européenne, le Parlement européen et le Conseil de l'Union ont abouti à un texte de compromis le 15 décembre 2015.

Le RGPD a été formellement approuvé par les institutions et publié au Journal Officiel de l'Union européenne le 4 mai 2016. La singularité réside dans le fait que le RGPD n'est entré en application que deux ans à compter de la date de son entrée en vigueur, soit le 25 mai 2018. Ce délai de deux ans a été utilisé par de nombreux organismes pour s'engager dans un processus de mise en conformité afin d'intégrer les nouvelles exigences du Règlement. Cette période de transition a également été mise à profit par les institutions nationales des Etats membres et les autorités de contrôle.

Rappelons que l'ancienne réglementation résulte de la [directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données](#) ; chaque Etat membre de l'Union européenne ayant ensuite transposé cette directive dans son droit national. Cette directive a été abrogée par l'applicabilité du RGPD, au 25 mai 2018.

Le RGPD poursuit notamment un objectif d'harmonisation des législations européennes puisqu'il sera directe-

ment applicable dans chaque Etat membre sans qu'aucune transposition ne soit nécessaire.

Toutefois, le RGPD renvoie sur certains points à la loi nationale des Etats membres. Aussi, certains pays – à l'instar de l'Allemagne et de la France – ont adopté une loi intégrant les exigences du RGPD. En France, il s'agit de la [loi relative à la protection des données personnelles, adoptée le 14 mai 2018 par le Parlement](#). Cette loi modifie la loi n°78-17 du 6 janvier 1978 pour l'adapter au RGPD et pour transposer la directive du 27 avril 2017 relative aux traitements de données à caractère personnel par les autorités dans le cadre des enquêtes et procédures judiciaires [Directive (UE) 2016/680 du Parlement européen et du conseil du 27 avril 2016 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, et abrogeant la [décision-cadre 2008/977/JAI du Conseil](#)].

Les autorités de contrôle ont également été actives collectivement et individuellement. Le Groupe de l'Article 29 a, en effet, adopté et publié des [lignes directrices](#) sur certaines thématiques (autorité de contrôle, délégué à la protection des données, portabilité, analyse d'impact...). Certaines autorités

ont également mis des outils à disposition des acteurs. Par exemple, l'autorité de contrôle belge a publié un modèle de registre des activités de traitement. La Commission nationale de l'informatique et des libertés a par ailleurs créé un [outil d'aide à la réalisation et à la formalisation des analyses d'impact](#).

Rappelons enfin qu'un autre règlement européen devrait intervenir dans le courant du 1er semestre 2018, à savoir le règlement « ePrivacy » relatif aux communications électroniques. Il aura notamment un impact sur le traitement des métadonnées et l'utilisation des cookies.

LES DONNÉES PERSONNELLES EN FRANCE ET DANS L'UE



FICHE 2 - LES NOTIONS ESSENTIELLES DE LA PROTECTION DES DONNÉES

Avant de procéder à l'analyse proprement dite du RGPD, nous vous proposons un rappel terminologique des notions clefs de la protection des données enrichi des apports du Règlement.

DONNÉE À CARACTÈRE PERSONNEL

Toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement par référence à un identifiant tel que le nom, un numéro d'identification, une donnée de localisation, un identifiant en ligne, etc.

TRAITEMENT DE DONNÉES

Toute opération ou ensemble d'opérations effectués sur des données à caractère personnel que le procédé soit automatisé ou non. Constituent notamment un traitement la collecte, l'enregistrement, l'organisation, le stockage, l'extraction, l'adaptation ou la modification, la consultation, l'utilisation, la communication par transmission, la diffusion, l'effacement ou la destruction, le verrouillage, etc.

FICHE 3 - LES ACTEURS DE LA PROTECTION DES DONNÉES PERSONNELLES

Voici un rappel des acteurs clefs de la protection des données à caractère personnel.

TIERS Personne physique ou morale, autorité publique, service ou tout autre organisme distinct de la personne concernée, du responsable de traitement, du sous-traitant et des personnes qui, sous l'autorité directe du responsable de traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel.	RESPONSABLE DE TRAITEMENT Personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel.
PERSONNE CONCERNÉE Personne physique identifiée ou identifiable dont les données à caractère personnel sont traitées.	DESTINATAIRE Personne physique ou morale, autorité publique, service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.
CO-RESPONSABLE DE TRAITEMENT Responsable de traitement qui détermine conjointement avec d'autres les finalités et les moyens du traitement de données à caractère personnel.	SOUS-TRAITANT Personne physique ou morale, autorité publique, service ou tout autre organisme qui traite les données à caractère personnel pour le compte du responsable de traitement.

Fiche 4 - Les principes de la protection des données personnelles réaffirmés

Les principes, clés de voûte de la protection des données

Licéité, loyauté, limitation des finalités, minimisation des données, exactitude des données, conservation limitée des données et sécurité des données, tels sont les principes de la protection des données qui figurent à l'article 5 du RGPD. Si certaines dénominations ont changé, ces principes ne sont pas inconnus des responsables de traitement.

La licéité du traitement fait référence à son fondement juridique tandis que la loyauté du traitement désigne les modalités selon lesquelles les données sont collectées (lien avec la transparence et l'information des personnes).

A l'instar de la situation antérieure, les responsables de traitement doivent toujours justifier, à compter de l'entrée en vigueur du RGPD, d'une finalité déterminée, explicite et légitime pour tout traitement de données à caractère personnel mis en œuvre.

Ils doivent ainsi définir au préalable le but poursuivi préalablement et ce de manière claire, afin que les finalités arrêtées puissent être facilement comprises par les personnes concernées. Cette étape revêt une importance particulière puisqu'elle limitera par la suite les éventuelles réutilisations des données à caractère personnel.

Qu'est-ce que la minimisation des données ? Ce principe désigne la proportionnalité entre les données à caractère personnel traitées et la finalité

du traitement (caractère adéquat, pertinent et non excessif des données traitées).

La qualité des données à caractère personnel compte également parmi les principes de la protection des données. Celles-ci doivent être exactes et si nécessaire mises à jour. Ainsi, les données inexactes doivent-elles être rectifiées ou supprimées. Ce principe revêt une importance particulière dans le cadre notamment des fichiers d'exclusion.

La durée de conservation limitée des données est un enjeu important pour le responsable de traitement car elle doit désormais figurer dans la mention d'information délivrée aux personnes concernées. Dès lors, ces dernières seront en mesure de vérifier si l'organisme responsable de traitement respecte la durée qu'il a lui-même déterminée.

Enfin, la sécurité des données demeure au cœur de la protection des données. En pratique, une grille de lecture reprenant chacun de ces principes pourra être élaborée afin de déterminer s'ils sont bien pris en compte dans le cadre de la mise en œuvre des traitements.

La notion de consentement précisée et renforcée

Les conditions de la licéité d'un traitement sont définies par l'article 6 du RGPD. En tant que responsable de traitement, un organisme pourra fon-

der la légitimité du traitement sur l'un des critères suivants :

- consentement de la personne concernée,
- exécution d'un contrat,
- respect d'une obligation légale,
- sauvegarde des intérêts vitaux de la personne,
- exécution d'une mission d'intérêt public,
- poursuite d'intérêts légitimes (intérêt économique, commercial, respect de l'objet social d'une association, sécurité des personnes et des biens, etc.).

Le consentement des personnes concernées est défini par le 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 » (article 4 du RGPD). Cette définition complète celle consacrée par la directive 95/46/CE en ce qu'elle prévoit expressément que le consentement résulte d'un acte positif univoque. Afin de rapporter la preuve du consentement recueilli, un responsable de traitement devra utiliser des solutions de traçabilité. De manière pratique, rappelons toutefois que la case à cocher ou encore la poursuite de la navigation en matière de cookies caractérisent ces actes positifs.

Un statut spécifique pour les mineurs

Le RGPD prévoit un régime spécifique aux traitements de données à caractère personnel mis en œuvre dans le cadre de l'offre de services aux mineurs (réseaux sociaux, etc.) de moins de 16 ans ou de 13 ans, en fonction de la législation nationale. En France, cet âge a été fixé à 15 ans par la loi relative à la protection des données personnelles.

En effet, le consentement des personnes dépositaires de l'autorité parentale doit être recueilli si la personne concernée a moins de 15 ans. Dès lors, de manière pratique, un responsable de traitement devra le cas échéant d'une part s'assurer que le consentement est valablement recueilli mais également vérifier que la personne qui donne son consentement est bien majeure ou titulaire de l'autorité parentale. Une double traçabilité devra donc être prévue.

Fiche 5 - L'application territoriale

Les institutions européennes ont souhaité que la protection des données à caractère personnel des citoyens européens s'applique de manière étendue.

C'est la raison pour laquelle l'article 3 du RGPD prévoit une application territoriale large à tout traitement de données à caractère personnel, mis en œuvre par un responsable de traitement, même s'il n'est pas établi sur le territoire de l'Union européenne (UE) dès lors qu'il s'agit d'activités liées à l'offre de biens ou de services, proposées à des personnes se trouvant au sein de l'UE et à l'observation du comportement des personnes situées au sein de l'UE.

Plus précisément, une entreprise établie aux États-Unis qui commercialise ses produits directement à des résidents de l'Union européenne, sans être physiquement présente sur le territoire de l'Union, est soumise aux exigences du RGPD.

Notons qu'en application de l'article 4 de la directive 95/46/CE relatif au droit national applicable, l'application de la loi nationale d'un Etat membre de l'Union européenne à un responsable de traitement qui n'y était pas établi supposait qu'il ait recours « (...) à des moyens, automatisés ou non, situés sur le territoire dudit Etat membre (...) ». Cette notion était entendue de manière large afin de soumettre une large partie des responsables de traitement à la loi de protection d'un Etat membre. Aussi les moyens de traite-

ment pouvaient-ils être caractérisés par les logiciels de collecte utilisés, les formulaires de collecte, les serveurs informatiques ou encore le recours à des cookies.

Aussi, même si cette appréhension large de l'application territoriale de la réglementation n'est pas foncièrement nouvelle, ces aspects sont plus précisément définis. Ceci n'est pas sans conséquences pour un organisme non établi dans l'Union européenne. Ce dernier doit en effet désigner un représentant au sein de l'UE, c'est-à-dire une personne physique ou morale établie sur le territoire de l'Union européenne désignée par le responsable de traitement de données à caractère personnel afin de le représenter.



DIRECTIVE VS RÈGLEMENT

ART. 4 DIRECTIVE 95/46/CE

Opérateurs économiques établis sur le territoire de l'Union Européenne



Moyens, automatisés ou non, de traitement situés sur le territoire de l'Union européenne

Désignation d'un représentant

ART. 3 RÈGLEMENT EUROPÉEN

Opérateurs économiques non établis sur le territoire de l'Union européenne



Offre de biens ou de services à des personnes se trouvant au sein de l'Union européenne ou observation du comportement de ces dernières

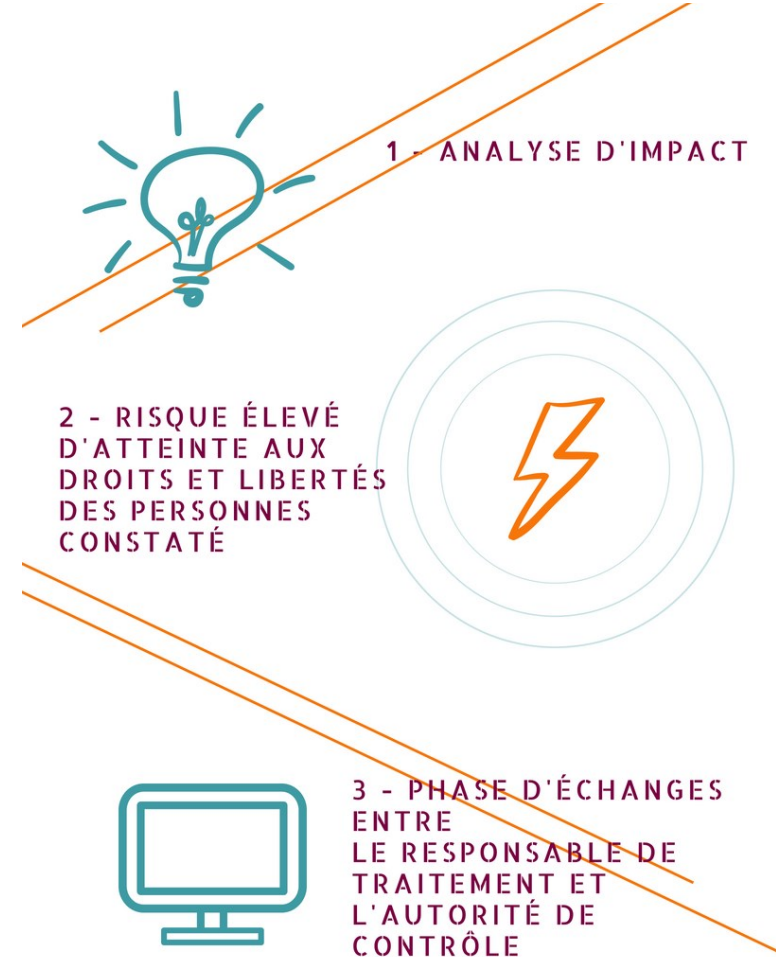
Désignation d'un représentant

Fiche 6 - Le principe d'accountability

Au système déclaratif actuel, le RGPD substitue une démarche responsable (« *accountability* ») selon laquelle un organisme responsable de traitement doit être en mesure de démontrer à son autorité de contrôle qu'il se conforme à ses obligations en matière de protection des données.

Le responsable de traitement n'est plus soumis au système de formalités préalables à la mise en œuvre des traitements tel qu'il figurait dans la loi du 6 janvier 1978 modifiée. Toutefois, l'article 36 du RGPD européen prévoit un régime de consultations préalables de l'autorité de contrôle comme illustré ci-contre.

Cet article prévoit par ailleurs que, dans des domaines spécifiques, la loi des Etats membres puisse prévoir un régime de consultation et d'autorisation préalables à la mise en œuvre des traitements. C'est le cas en France à la suite de la loi relative à la protection




des données personnelles. Les traitements mis en œuvre par un responsable de traitement dans le cadre d'une mission de service public ou encore dans le cadre de la protection sociale et de la santé publique seront notamment concernés. Le législateur a cependant prévu la possibilité pour la Commission nationale de l'informatique et des libertés d'établir des réfé-



1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement des données à caractère personnel est effectué conformément au présent Règlement. Ces mesures sont réexaminées et actualisées si nécessaire.

2. Lorsque cela est proportionné aux activités de traitement de données, les mesures visées au paragraphe 1 comprennent la mise en œuvre de politiques appropriées en matière de protection des données par le responsable du traitement.

3. L'application d'un code de conduite approuvé comme le prévoit l'article 40 ou de mécanismes de certification approuvés comme le prévoit l'article 42 peut servir d'éléments pour démontrer le respect des obligations incombant au responsable de traitement.



rentiels et règlements types s'appliquant aux traitements concernés. Ces traitements pourront alors être mis en œuvre sans que la procédure d'autorisation préalable ne soit suivie, si le responsable du traitement adresse au préalable à la Cnil une déclaration de conformité.

En pratique, le principe de responsabilité implique que le responsable d'un traitement de données à caractère personnel adopte des mesures techniques et organisationnelles garantissant le respect de la réglementation.

Des mesures adaptées

Ces mesures devront être adaptées en tenant compte de plusieurs éléments factuels tels que la nature du traitement de données mis en œuvre, le contexte, la portée et les finalités du traitement.

Les risques pour les droits et libertés des personnes doivent également être identifiés ainsi que leur probabilité de survenance et gravité évaluées. Les mesures ne sont donc pas les mêmes pour tous les organismes. Les études d'impact et analyses de risques doivent être privilégiées.

La politique de protection des données à caractère personnel adoptée au sein d'un organisme est ainsi redigée sur-mesure.

Des mesures diversifiées

Les mesures techniques et organisationnelles mises en place par le responsable de traitement sont de nature diverse. De manière générale, elles sont matérialisées par toutes les dispositions prises par l'entreprise pour respecter les obligations qui lui incombent en application du RGPD (principes du privacy by design et by default, respect des droits des personnes, analyses d'impact le cas échéant, sécurité et confidentialité des données, notification des failles, tenue du registre, etc.).

Surtout, la prise en compte des [principes de protection des données à caractère personnel par défaut et dès la conception](#) fait désormais partie intégrante de l'évaluation de la conformité d'un organisme responsable de traitement (traduits de l'anglais « privacy by default » et « privacy by design »).

La protection des données à caractère personnel doit être intégrée dès la conception des systèmes et des technologies mis en place. Le RGPD précise que ce principe doit être décliné tant en phase de détermination des moyens du traitement qu'au moment de sa mise en œuvre. Cette exigence présente un lien étroit avec le principe de minimisation des données à caractère personnel, principe en vertu duquel les données à caractère personnel doivent être « [adéquates, pertinentes et limitées à ce qui est néces-](#)

saire au regard des finalités pour lesquelles elles sont traitées ».

Ce principe connu des responsables de traitement, puisqu'il figurait déjà dans la directive 95/46/CE et dans la loi Informatique et Libertés, postule de ne collecter que les données strictement nécessaires à la réalisation de la finalité définie. Dès lors, une analyse précise du traitement envisagé s'impose pour déterminer ses caractéristiques et vérifier qu'elles sont en adéquation avec les règles de protection des données (durée de conservation limitée, données strictement nécessaires, etc.).

Notons que le RGPD prévoit expressément que les données à caractère personnel ne doivent pas être rendues accessibles à « *un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée* ». Il convient donc de laisser une marge de manœuvre doit aux personnes dont les données sont traitées. De ce point de vue, la personne retrouve la maîtrise de ses données à caractère personnel puisqu'il lui appartient de modifier les paramètres.

L'important est de démontrer les engagements pris par le responsable de traitement en faveur de la protection effective des données personnelles.

La protection des données personnelles peut prendre de nombreuses formes.

ET EN PRATIQUE ?

- 1** Procédure interne de gestion des réclamations et des demandes d'exercice des droits
- 2** Politique en matière de sous-traitance des traitements
- 3** Règles internes d'entreprise ("Binding Corporate Rules") définissant la politique d'un groupe en matière de transfert de données personnelles
- 4** Labels délivrés par la CNIL
- 5** Désactivation par défaut de la géolocalisation des personnes et absence de partage de données par défaut
- 6** Techniques de pseudonymisation

Le registre de traitements pour tous, une mesure pertinente

La [généralisation de la tenue d'un registre des traitements](#) mis en œuvre participe également de la démarche de responsabilité des organismes. Le RGPD rappelle l'importance de ce registre en précisant que « Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement mises en œuvre ».

Les entreprises de moins de 250 salariés ne sont pas soumises à cette obligation. Cette exception sera toutefois écartée si le traitement mis en œuvre par un tel organisme responsable de traitement est générateur de risque pour les droits et libertés des personnes, s'il est récurrent ou s'il porte sur des données à caractère personnel sensibles ou relatives à des condamnations et infractions pénales.

Le registre devra préciser :

- le nom et les coordonnées des différents acteurs (responsable de traitement, co-responsable, représentant de l'organisme et le cas échéant, délégué à la protection des données) ;
- les finalités du traitement ;
- la description des catégories de personnes concernées, des catégories de données et des catégories de destinataires des données à caractère personnel ;

- les transferts de données à caractère personnel avec identification des pays de destination et des garanties utilisées pour encadrer cette opération (BCR, clauses contractuelles types, etc.) ;
- la description des mesures de sécurité adoptées ;
- les délais prévus pour l'effacement des différentes catégories de données.

La loi relative à la protection des données personnelles ajoute deux éléments, pour les registres des traitements de données à caractère personnel à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ou d'exécution de sanctions pénales. Ces registres devront en sus comprendre la mention de la base juridique des opérations de traitement et le cas échéant du recours au profilage.

Comment faire face à ces exigences ?

Afin de vous mettre en conformité avec le RGPD, il est recommandé d'identifier et de passer en revue les différentes politiques internes en lien avec la protection des données à caractère personnel. Un audit des traitements mis en œuvre peut également être réalisé avec l'assistance d'experts techniques et juridiques. La Cnil a publié une [infographie](#) détaillant les démarches à prendre et les principes

clés, ainsi qu'un guide [pratique adapté aux TPE/PME](#).

D'autres autorités de contrôle ont également pris des mesures afin d'aider les responsables du traitement. Par exemple, le Préposé fédéral à la pro-

tection des données et à l'information de la confédération suisse fournit un [questionnaire](#) qui permet au responsable du traitement d'anticiper les risques dès le début du développement de son projet.



Fiche 7 - L'analyse d'impact

L'une des nouveautés issues du RGPD est l'obligation de réaliser, avant la mise en œuvre de certains traitements, une analyse d'impact relative à la protection des données à caractère personnel (en anglais, Data Protection Impact Assessment ou DPIA), d'après le considérant 84 et l'article 35 du Règlement.

Il s'agit d'un instrument aux objectifs multiples dans la mesure où une analyse d'impact permet d'identifier les risques sur la vie privée des personnes concernées (origine, nature, gravité du risque...), d'identifier les mesures adéquates de la protection des données à caractère personnel et de démontrer que le traitement mis en œuvre est conforme au RGPD (l'analyse d'impact donnant lieu à l'élaboration d'une documentation). À ce titre, l'analyse d'impact participe à la démarche de responsabilisation adoptée par le RGPD.

La Cnil a publié une [infographie](#) et des [études de cas](#) afin d'aider les professionnels à définir dans quel cas une analyse d'impact est obligatoire et les accompagner dans sa réalisation. La Cnil a également mis à disposition du public, un [outil d'aide à la réalisation de ces analyses d'impact](#).

L'analyse d'impact est-elle obligatoire ?

Une analyse d'impact n'est pas obligatoire pour l'ensemble des traitements

mis en œuvre. Certains organismes peuvent toutefois opter pour une analyse d'impact systématique, en fonction de la politique interne définie.


Une analyse d'impact doit être effectuée lorsqu'un type de traitement « est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques », selon l'article 35§1 du RGPD. Ceci sera notamment le cas pour le traitement à grande échelle de données relative à la santé.

Une analyse d'impact peut porter sur un type de traitement ou plusieurs types de traitement similaires. Le risque sera évalué compte tenu de la nature, la portée, du contexte et des finalités du traitement.

Le paragraphe 3 de l'article 35 du RGPD identifie trois cas non-exhaustifs dans lesquels une analyse d'impact est également requise. Afin de préciser les cas énoncés, le G29 a publié des [recommandations](#) relatives à l'analyse d'impact, révisée le 4 octobre 2017.

⇒ « L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard de cette personne ou l'affectant de manière significative de façon similaire. ».

Cette situation concerne toute évaluation, y compris le profilage, ou nota-



tion d'une personne physique l'affectant de manière significative (ex : refus d'un prêt en raison de la référence de crédit).

Un traitement est systématique s'il répond à l'un ou plusieurs des critères suivants : il est mis en œuvre selon un système prédéfini, organisé et méthodique, la collecte de données est réalisée dans le cadre d'un plan général et/ou réalisée dans le cadre d'une stratégie. Rappelons que cette définition est issue des lignes directrices du G29 relatives au DPO (Guidelines on Data Protection Officers (DPOs), G29, 5 April 2017).

⇒ « *Le traitement à grande échelle de catégories particulières de données, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions.* ».

En raison de l'absence de définition de ce que constitue un traitement à grande échelle dans le RGPD, le G29 a identifié plusieurs facteurs non exhaustifs à prendre en compte : le volume des données traitées, l'étendue géographique du traitement, le nombre de personnes concernées et la durée du traitement.

En outre, cette hypothèse sera applicable au traitement de catégories particulières de données au sens de l'article 9 du RGPD (données de santé, opinions politiques, données biométriques, génétiques...) et de l'article 10 du même texte (données relatives à

des condamnations pénales, à des infractions ou encore des mesures de sûreté).


⇒ « *La surveillance systématique à grande échelle d'une zone accessible au public.* »

A cet égard, le G29 a pu préciser que le traitement mis en œuvre permet d'observer, de surveiller ou de contrôler les personnes concernées, en ce compris sur les réseaux de communication. Etant précisé que cette situation intègre les cas dans lesquelles les personnes concernées seraient dans l'impossibilité de se soustraire au traitement (surveillance dans l'espace public, par exemple).

Quand l'analyse d'impact doit-elle être réalisée ?

L'analyse d'impact doit être réalisée avant la mise en œuvre du traitement afin de pouvoir mettre en place des mesures rectificatives si nécessaires. Elle devrait être effectuée le plus tôt possible, même si l'ensemble des opérations de traitement n'est pas encore clairement défini.

L'analyse d'impact doit en outre évoluer avec le traitement de données à caractère personnel qui en a fait l'objet. Ainsi, lorsque les conditions de la mise en œuvre du traitement changent (changement de la nature des données à caractère personnel collectées, de la période de conservation des données...) et que ce changement



présente un risque pour les droits et libertés des personnes concernées, l'analyse d'impact doit être modifiée. De cette manière, le responsable du traitement s'assure que les mesures de protection définies sont toujours en adéquation avec les risques présentés par le traitement.

Quels acteurs interviennent dans la réalisation de l'analyse d'impact ?

En vertu de l'article 35 du RGPD, la réalisation de l'analyse d'impact pèse sur le responsable du traitement. En pratique, les équipes métiers auront un rôle prépondérant puisqu'elles con-


ANALYSE D'IMPACT OBLIGATOIRE

Traitement qui figure sur la liste établie par l'autorité de contrôle

Évaluation systématique et approfondie d'aspects personnels relatifs aux personnes physiques (y compris le profilage) permettant notamment la prise de décision

Surveillance systématique à grande échelle d'une zone accessible au public

Traitement à grande échelle de données à caractère personnel particulières (données de santé, données biométriques, etc.) ou de données relatives à des condamnations pénales et à des infractions



naissent les caractéristiques du traitement projeté. Ainsi pourront-elles notamment décrire le contexte dans lequel le traitement sera mis en œuvre, ses finalités ainsi que les catégories de données, évaluer le volume de personnes concernées ou encore identifier les durées de conservation à appliquer...

Les équipes métiers devront sans doute s'appuyer sur l'expertise technique ou juridique d'autres collaborateurs afin de rassembler l'ensemble des informations nécessaires à l'analyse d'impact.

L'implication du DPO pourra varier selon les organismes, le niveau de prise en compte du RGPD et de ses enjeux ainsi que selon le niveau de sensibilisation des métiers. Aussi, le DPO peut avoir un rôle de guide des équipes métiers. L'analyse d'impact lui permettant aussi de sensibiliser les opérationnels.

Le DPO s'assurera ainsi de l'existence d'une analyse d'impact de qualité, en formulant le cas échéant des demandes de complément et/ou de modification. Le DPO peut au contraire être plus en retrait si les enjeux de protection des données sont intégrés par les métiers. Notons qu'en tout état de cause, le G29 recommande de documenter l'avis formulé par le DPO dans le cadre de l'analyse d'impact (article 39 §1. c) du RGPD).

En outre, le sous-traitant doit aider le responsable du traitement et lui fournir les informations à sa disposition

lors de la réalisation d'une analyse d'impact (article 28 §3. f) du RGPD).

Le responsable du traitement peut également demander l'avis des personnes concernées ou de leurs représentants (article 35§9 du RGPD). Le G29 recommande de documenter la décision de concerter ces dernières ou de l'absence de concertation.

Enfin, le responsable est libre de consulter toute personne susceptible de l'accompagner (avocats, experts en informatique ou en sécurité, déontologue en fonction de son secteur d'activité, etc.).

Que contient une analyse d'impact ?

Selon l'article 35 §7 du RGPD, l'analyse d'impact doit *a minima* contenir :

- une description systématique des opérations de traitement envisagées et des finalités du traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à

caractère personnel et à apporter la preuve du respect du RGPD.

Chaque étape de la réalisation de l'analyse d'impact doit être documentée afin d'être en mesure de démontrer la prise en compte de la protection des données. Dans ce cadre, le respect par le responsable du traitement ou le sous-traitant de code(s) de conduite sera pris en compte lors de l'évaluation de l'impact des opérations de traitement. Seront également pris en compte les mécanismes de certification et les labels en matière de protection des données. Les règles d'entreprise contraignantes (en anglais, Binding Corporate Rules, BCR) pourraient également être prises en compte. Concernant les mécanismes de certification définis par le RGPD, l'European Union Agency for Network and Information Security (ENISA) a publié, le 27 novembre 2017, des [recommandations](#).

Le G29 souligne que la publication de l'analyse d'impact est de nature à susciter la confiance des personnes concernées. Il convient toutefois de souligner que le RGPD n'impose aucune obligation de publication de l'analyse d'impact. Au regard de son contenu, une majorité de responsables du traitement pourrait toutefois opter pour la confidentialité des analyses d'impact.


Quel est le rôle de l'autorité de contrôle lors de la réalisation d'une analyse d'impact ?

L'autorité de contrôle peut intervenir en amont en dressant et en publiant une liste des types d'opération de traitement pour lesquelles une analyse d'impact est requise et/ou une liste des traitements non soumis à une telle analyse (article 35 § 4 et 5 du RGPD).

Selon l'article 36 du RGPD, elle peut également intervenir après la réalisation d'une analyse d'impact mais aussi préalablement à la mise en œuvre du traitement lorsque l'analyse révèle qu'il existe un risque résiduel élevé pour les droits et libertés des personnes concernées (licenciement, difficultés financières par exemple).

Dans ce contexte, le responsable du traitement doit lui communiquer plusieurs éléments notamment l'analyse d'impact ainsi que les mesures et garanties prévues afin de protéger les droits et libertés des personnes concernées. L'autorité de contrôle participe ainsi à l'élaboration des mesures techniques et organisationnelles du responsable du traitement.

Si le traitement envisagé par le responsable du traitement est susceptible de constituer une violation du RGPD, l'autorité de contrôle rendra un avis écrit et pourra exercer ses pouvoirs propres (enquête, mesures correctrices...).



Cas spécifique : l'analyse d'impact réalisée au cours de l'adoption d'un texte européen ou national.

L'article 35§10 du RGPD prévoit un cas particulier pour lequel le responsable du traitement n'aura pas à réaliser d'analyse d'impact.

Toutefois, les conditions suivantes doivent être réunies :

- le traitement de données à caractère personnel mis en œuvre a pour fondement le respect d'une obligation légale ou l'exécution d'une mission d'intérêt public ;
- le traitement mis en œuvre est encadré par le droit de l'Union européenne ou le droit national ;
- une analyse d'impact relative à la protection des données a été réalisée dans le cadre de l'adoption de la réglementation encadrant le traitement.

Soulignons toutefois que le RGPD laisse une marge d'appréciation aux Etats membres qui peuvent prévoir que même en pareil cas, une analyse d'impact est tout de même exigée.

ANALYSE D'IMPACT NON EXIGÉE PAR LE RGPD

Traitement qui figure sur la liste établie par l'autorité de contrôle

Traitement non susceptible de générer un risque élevé pour les droits et libertés des personnes concernées

Traitement mis en œuvre sur le fondement du respect d'une obligation légale ou de l'exécution d'une mission d'intérêt public, pour lequel une analyse d'impact relative à la protection des données a été réalisée dans le cadre de l'adoption de la réglementation encadrant le traitement

Fiche 8 - La gestion de crise **renforcée**

La sécurité des données à caractère personnel est depuis toujours un enjeu technique et juridique de la protection des données à caractère personnel. Technique car les mesures mises en œuvre doivent être adaptées à la nature des données et aux risques présentés par le traitement mis en œuvre. Juridique ensuite parce que, d'une part, cette exigence de sécurité a une influence sur les différents contrats conclus avec les prestataires et d'autre part, les manquements sont susceptibles de sanctions administratives par la Cnil et de sanctions pénales.

La sécurité des données renforcée – en amont

Il convient de constater que la sécurité des données à caractère personnel doit être assurée, en application du RGPD, tant par le responsable de traitement que par le sous-traitant. En effet, l'article 32 du RGPD impose à ces deux acteurs de prendre en compte différents facteurs de sécurité, tels que ceux présentés ci-contre.

Notons que les mesures de sécurité doivent avoir pour objectif notamment d'assurer la confidentialité, l'intégrité et la disponibilité du système de traitement des données ainsi que l'accès à celles-ci. Bien entendu, ces mesures ne peuvent être déterminées qu'après identification des risques. Dès lors, les analyses de risques classiquement utilisées demeurent un précieux outil.

QUELS FACTEURS PRENDRE EN COMPTE ?

- 1 Etat de l'art, portée, contexte et finalités du traitement mis en œuvre
- 2 Conséquences pour les personnes concernées en cas de destruction ou d'accès aux données par des tiers
- 3 Risques pour les droits et libertés des personnes concernées

Par ailleurs, le RGPD introduit la notion nouvelle de « *résilience constante des systèmes et des services de traitement* ». Selon le glossaire de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la résilience se dit, en informatique, de la « *capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident* ». Les solutions de sauvegarde et le système de redondance doivent donc être renforcés.

L'ensemble de ces mesures doit être décrit dans une politique de sécurité afin de documenter le respect par le responsable de traitement de son obligation d'assurer la sécurité des données à caractère personnel, conformément au principe de responsabilité. En outre, l'exigence d'adaptation des mesures de sécurité impose d'évaluer

SÉCURITÉ DES DONNÉES

Comment faire ?

Identification / Authentification

Audit

Chiffrement des transmissions

Traçabilité des accès

Localisation des données

Pseudonymisation

Politique de sécurité

Sensibiliser les salariés / agents

Gestion des droits d'accès / Habilitation

l'efficacité des mesures prises pour les réajuster le cas échéant.

La notification des violations de sécurité généralisée – en aval

Les responsables de traitement doivent impérativement être proactifs lorsqu'il s'agit de notifier à la Cnil les violations de données à caractère personnel.

Le RGPD généralise l'obligation de notifier ces violations. La [violation de données à caractère personnel](#) se définit comme la violation de sécurité entraînant la destruction, la perte, l'altération, la divulgation des données à caractère personnel traitées.

La notification devra être effectuée auprès de la Cnil dans un délai de 72 heures au plus tard après la prise de connaissance de la violation. Notons que la notification peut être effectuée à partir du site de la Cnil au moyen d'un [formulaire en ligne](#).

En cas de sous-traitance du traitement des données, une collaboration avec les prestataires est organisée par le RGPD. En effet, [l'article 33 du texte](#) prévoit que le sous-traitant doit notifier au responsable de traitement toute violation dont il a connaissance dans les meilleurs délais. Dans ce contexte, le responsable de traitement doit s'enquérir auprès de ses prestataires des délais dans lesquels ils sont en capacité de lui notifier toute violation de sécurité.

Fiche 9 - Le DPO au coeur de la démarche de mise en conformité

Les institutions européennes ont placé le DPO au centre de la démarche de conformité des organismes ([Garance Mathias, Amandine Kashani-Poor et Aline Alfer, Le Délégué à la protection des données \(DPO\), Les essentiels de la banque et de la finance, Revue Banque, 2017](#)).

C'est la raison pour laquelle le DPO doit, dans les conditions prévues par le RGPD, être désigné non seulement par les responsables de traitement mais aussi par les sous-traitants.

Les institutions européennes ont, du fait des compétences exigées du DPO et les missions qui lui seront confiées, institué un nouveau métier de la protection des données à caractère personnel.

Ce nouvel acteur suscite de nombreuses questions. Afin de tenter d'y répondre, le Groupe de l'Article 29 a publié des [lignes directrices](#) sur le délégué à la protection des données. Elles ont été révisées le 5 avril 2017.

Une désignation quasi-systématique du DPO ?

Au cours des discussions sur le RGPD, les institutions européennes ont pu marquer leur désaccord sur le caractère obligatoire de la désignation du DPO. La Commission européenne et le Parlement européen se sont positionnés pour le caractère obligatoire de la désignation dans des cas limitativement énumérés.

Au contraire, le Conseil de l'Union européenne laissait à la législation de chaque Etat membre le soin de déterminer le caractère obligatoire ou facultatif de la désignation du DPO.

Finalement, une position de compromis a été trouvée. Trois catégories d'entités devront systématiquement désigner un DPO.

En dehors de ces hypothèses, l'article 35 du RGPD prévoit que les organismes pourront désigner un DPO à moins que la loi nationale de l'Etat membre dans lequel ils sont établis ne rende cette désignation obligatoire. En France, le législateur a choisi de ne pas rendre obligatoire la désignation du DPO. Le G29 encourage cependant les entités à désigner volontairement un DPO.

Notons par ailleurs que la procédure de désignation du DPO est plus souple que celle concernant le Correspondant Informatique et Libertés, disparu au 25 mai 2018 (absence d'information des institutions représentatives du personnel, absence d'engagement écrit de la personne désignée, etc.). La Cnil a mis en place un [téléservice](#) afin de permettre aux entités de lui signaler les DPO désignés.

Comment déterminer si votre organisme est soumis à l'obligation de désigner un DPO ?

Indépendamment des autorités et organismes publics, deux catégories

d'entité devront systématiquement désigner un DPO.

DÉSIGNATION	
Délégué à la Protection des Données (DPO)	
DÉSIGNATION SYSTÉMATIQUE Organismes publics Organismes traitant des données sensibles (origine raciale, données génétiques, etc.) / condamnations / infractions Organismes procédant à de la surveillance à grande échelle (profilage, etc.)	GROUPE DE SOCIÉTÉS 1 DPO pour le Groupe Coordonnées du DPO aisément accessibles dans chacune des sociétés du Groupe Communication du DPO adaptée notamment aux personnes concernées et aux équipes mettant en oeuvre les traitements (langue utilisée) Allocation des ressources nécessaires afin que le DPO unique puisse exercer ses missions
ORGANISMES CONCERNÉS Responsable de traitement Sous-traitant	CHOIX DU DPO DPO interne DPO externe

Pour rappel, il s'agit des responsables du traitement et des sous-traitants dont :

- « les activités de base (...) consistent en des opérations de traite-

ment 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 » ;

- « les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».

Toutefois, qu'est-ce qu'une activité de base ? Qu'est-ce qu'un suivi régulier et systématique à grande échelle ? Qu'est-ce qu'un traitement à grande échelle ? En effet, ces notions ne sont pas définies par le RGPD alors même qu'elles déterminent la désignation obligatoire ou non d'un DPO.

Selon le considérant 97 du RGPD, les activités de base d'une entreprise évoluant dans le secteur privé « *ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité accessoire.* ».

Les lignes directrices du Groupe de l'Article 29 en la matière indiquent que la notion d'activité de base ne devrait pas être exclue lorsque l'activité d'une entité consiste intrinsèquement à traiter des données à caractère personnel.

Ainsi, le Groupe de l'Article 29 considère par exemple qu'une société de surveillance chargée d'assurer la sécurité d'un centre commercial ou de tout lieu ouvert au public devra désigner un délégué à la protection des données dans la mesure où son activité de surveillance implique un traitement de données à caractère personnel.

Concernant les opérations de traitement à échelle, le considérant 91 du RGPD relatif à l'analyse d'impact apporte des éclaircissements.

D'une part, le considérant 91 définit la notion a contrario en indiquant que « *Le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel.* ».

Ainsi, le traitement de données à caractère personnel réalisé par un avocat ou un médecin exerçant son activité à titre individuel ne serait pas constitutif d'un traitement à grande échelle imposant la désignation d'un DPO.

D'autre part, selon ce considérant, les opérations de traitement à grande échelle seraient celles qui « *visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernées*


et qui sont susceptibles d'engendrer un risque élevé (...). »

Dans ce contexte, le Groupe de l'Article 29 préconise de nombre en compte plusieurs critères parmi lesquelles le nombre de personnes concernées, le volume de données traitées, la durée des opérations de traitement ou encore l'étendue géographique des opérations de traitement.

A titre d'illustration, le traitement de données à caractère personnel relatif aux déplacements des usagers d'un service de transport serait considéré comme un traitement à grande échelle.

Notons que le Groupe de l'Article 29 n'exclut pas de publier des seuils relatifs à la désignation d'un DPO.

Enfin, concernant le suivi régulier et systématique des personnes. Il convient de noter que le considérant 24 du RGPD fait référence à la notion de « *suivi* » dans le cadre de la définition du champ d'application territorial : « *Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comporte-*



ments et ses dispositions d'esprit. ». Le suivi du comportement des personnes au sein de l'Union est par ailleurs un critère d'application du règlement précité (article 3§2 du RGPD).

Soulignons que le suivi peut être réalisé tant sur le réseau Internet qu'en dehors. Ensuite, le Groupe de l'Article 29 fait une interprétation large de la notion de suivi régulier et systématique des personnes de sorte qu'elle désigne toutes les formes de suivi et de profilage dont la publicité comportementale.

A titre d'illustration, le suivi de la position géographique des personnes dans le cadre de l'utilisation d'applications mobiles, les programmes de fidélité ou encore la surveillance et l'enregistrement de données dites de bien-être et d'état de forme à partir d'objets connectés seraient considérés comme un suivi régulier et systématique des personnes.

Un positionnement fort du DPO

Le DPO doit directement faire rapport « *au niveau le plus élevé du responsable du traitement ou du sous-traitant* ». Il doit donc pouvoir accéder aux instances décisionnaires de son organisme (comité exécutif, secrétariat général, direction générale, etc.). Preuve du positionnement fort du DPO, ce dernier peut avoir accès aux données à caractère personnel et aux traitements de données à caractère personnel. Il peut donc apprécier con-

crètement les conditions dans lesquelles les traitements sont mis en œuvre.


Le positionnement du DPO doit, en tout état de cause, lui permettre d'être informé et consulté sur tous les sujets ayant trait à la conformité de l'organisme au RGPD.

La consultation du DPO, qu'il soit interne ou externe à l'organisme, doit intervenir suffisamment en amont afin de lui permettre de formuler ses recommandations. Notons également que ces dernières doivent être prises en compte. En cas de désaccord, le Groupe de l'Article 29 recommande que les raisons pour lesquelles les recommandations du DPO n'ont pas été suivies soient documentées.

En outre, compte tenu de son positionnement, le DPO doit être consulté dans le cadre d'une violation de données ou de tout autre incident de sécurité, ce qui n'est pas sans lien avec le profil du DPO.

De manière générale, le Groupe de l'Article 29 encourage les entités à définir des lignes directrices listant les situations dans lesquelles le DPO devra être consulté. Ces documents ne peuvent que participer à la démonstration de la conformité de l'entité.

Le RGPD tient compte du fait que tous les organismes ne peuvent pas consacrer un poste à plein temps de DPO. Dans ce contexte, le DPO désigné peut exercer d'autres missions dans l'entreprise dès lors qu'il n'est pas en situa-



tion de conflits d'intérêts. Notons que le Groupe de l'Article 29 a identifié l'existence de conflits d'intérêts entre la fonction de DPO et des fonctions managériales (direction du département marketing, direction du département des ressources humaines, etc.). En tout état de cause, l'organisme doit veiller à ce que le DPO bénéficie du temps suffisant à l'exercice de ses missions.

Le DPO ne bénéficie pas du statut de salarié protégé. En revanche, le texte prévoit expressément que le DPO ne puisse pas être sanctionné, sous quelque forme que ce soit, en raison de l'exercice de ses missions. Le G29 a confirmé cette interprétation dans les [lignes directrices révisées](#) et adoptées le 5 avril 2017.

Cela étant, la fin de mission du DPO n'est pas encadrée par le RGPD. Faut-il s'en remettre aux règles internes ? La politique de protection des données à caractère personnel interne à chaque entreprise peut-elle en effet prévoir une durée pour la mission du DPO, renouvelable ou non ?

Des compétences reconnues et des missions diversifiées

Le RGPD définit le profil du DPO plus précisément que ne le faisait la réglementation jusque-là. Les DPO doivent avoir des connaissances juridiques ou se faire accompagner par leur service

juridique et/ou un avocat. Le G29 insiste sur le fait que le DPO doit être suffisamment disponible, sa priorité étant la mise en conformité de l'entreprise au RGPD.

En interne, le DPO a pour mission principale d'informer et de délivrer des conseils dans le cadre de la mise en œuvre des traitements. C'est la raison pour laquelle il doit être associé à toutes questions en matière de protection des données à caractère personnel.

Le DPO doit également informer et conseiller les salariés dont la mission est de traiter les données à caractère personnel. A cet égard, une maîtrise du RGPD mais également des textes sectoriels impactant la protection des données à caractère personnel est requise. Le RGPD prévoit en effet que certains domaines soient laissés à l'appréciation du droit national de chaque État membre.

Des compétences juridiques sont également mobilisées lorsqu'il s'agit de contrôler la conformité de l'organisme au regard du RGPD, des règles internes de l'organisme ainsi que d'autres dispositions nationales ou européennes applicables. Le texte énumère, de manière non exhaustive, certains éléments sur lesquelles l'attention du DPO doit porter, à savoir la répartition des responsabilités (cas de la responsabilité conjointe du traitement ou de recours à un sous-traitant par



Le délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39.



exemple). La sensibilisation et la formation du personnel doit également inclure les règles spécifiques applicables en matière de protection des données à caractère personnel.

Enfin, le DPO doit vérifier que les analyses d'impact sont réalisées. Ses conseils peuvent également être sollicités dans ce cadre. A la lecture des lignes directrices du Groupe de l'Article 29, il ne s'agira pas d'une simple vérification. En effet, les autorités de contrôle recommandent que les conseils du DPO soient sollicités pour :

- déterminer notamment si une analyse d'impact est ou non nécessaire ;
- déterminer la méthodologie d'analyse à suivre ;
- définir les mesures pour atténuer les risques pour les droits et libertés des personnes.

Notons que si les recommandations du DPO ne sont pas prises en compte, le rapport d'analyse d'impact doit expressément contenir les motifs pour lesquels le responsable du traitement est passé outre.

Des compétences en matière de sécurité des données semblent donc également exigées du DPO.

La visibilité du DPO est renforcée par la publication de ses coordonnées à destination du public (site Internet institutionnel, site Internet marchand, intranet accessible aux salariés et/ou aux intervenants, documents émis par

l'organisme, etc.). A ce titre, le DPO est amené à interagir avec les personnes concernées puisqu'elles pourront s'adresser à lui pour toute question relative aux traitements les concernant et à l'exercice de leurs droits.

Le Groupe de l'Article 29 souligne que le RGPD n'exige pas que le nom du DPO soit communiqué aux personnes concernées. Toutefois, le Groupe considère que cela pourrait être une bonne pratique tout en laissant le soin au DPO et à l'organisme qui le désigne le soin de trancher cette question.

En dernier lieu, le DPO est le point de contact avec l'autorité de contrôle avec laquelle il devra collaborer. C'est la raison pour laquelle le RGPD prévoit que les coordonnées du Délégué à la protection des données soient également communiquées à l'autorité de contrôle.

Comment préparer la désignation d'un DPO ?

Afin de préparer au mieux la désignation d'un DPO, il peut être intéressant d'effectuer une sensibilisation des membres des instances décisionnelles sur le rôle et les missions de cet acteur de la protection des données. Cette présentation leur permettrait de comprendre l'étendue des exigences du RGPD à leur égard (fourniture de moyens, entretien des connaissances, etc.).

Des entretiens avec les salariés et agents des différents services pourraient également être réalisés afin de comprendre comment la protection des données à caractère personnel y est appréhendée. Cela permettrait d'identifier les points à améliorer et de dégager une politique de protection des données à la rédaction de laquelle le DPO serait associé.

Bien que les Correspondants informatique et libertés (CIL) désignés par le

passé ne sont pas nécessairement devenus DPO, leur travail de CIL peut être un point de départ utile pour le DPO. A titre d'illustration, le CIL devait tenir le registre des activités de traitement sous la loi Informatique et Libertés. Cet outil peut donner au DPO nouvellement désigné un aperçu du fonctionnement de l'entreprise et des mesures prises pour protéger les données à caractère personnel, ainsi qu'une vue d'ensemble des traitements mis en œuvre.





Fiche 10 - Le renforcement des obligations des sous-traitants

L'application du RGPD a une influence forte sur les relations entre responsable de traitement et sous-traitant. Jusque-là, seul le responsable de traitement répondait auprès de l'autorité de contrôle de protection des données à caractère personnel des manquements à la réglementation. Le sous-traitant était, de ce point de vue, à l'abri des sanctions infligées par la Cnil.

Le RGPD tend à rééquilibrer la relation entre les deux opérateurs en mettant des obligations directement à la charge des sous-traitants et en renforçant les obligations contractuelles du sous-traitant. La Cnil a notamment publié un [guide du sous-traitant](#) couvrant les points clés telles que les obligations du sous-traitant ou sa relation contractuelle avec le responsable du traitement. Le guide contient également des conseils pratiques de conformité au RGPD. Le RGPD prévoit également que les manquements d'un sous-traitant puissent être sanctionnés par les autorités de contrôle.

Les obligations directement mises à la charge du sous-traitant

Plusieurs obligations sont directement mises à la charge du sous-traitant.

D'abord, un sous-traitant non établi sur le territoire de l'Union européenne doit désigner un représentant au sein de l'Union par mandat écrit. Tel est le cas si ce sous-traitant procède au traitement des données à caractère per-

sonnel concernant des personnes situées dans l'Union européenne et que les opérations de traitement sont liées à l'offre de biens et services ou à la surveillance du comportement de ces personnes (considérant 80 et article 27 du RGPD).

Le sous-traitant doit également désigner un délégué à la protection des données (Fiche n°9 : Le DPO au cœur de la démarche de conformité).

Sans qu'il s'agisse d'une nouveauté, le sous-traitant doit en outre présenter des garanties jugées suffisantes (connaissances du domaine dans lequel il intervient, fiabilité, ressources notamment) de mise en œuvre de mesures techniques et organisationnelles pour que le traitement soit conforme au RGPD. Ces garanties constituent d'ailleurs un critère de choix que les responsables de traitement doivent prendre en compte (considérant 81 et article 28§1 du RGPD). Cette exigence peut par exemple être satisfaite lorsque le sous-traitant applique un code de conduite approuvé par une autorité de contrôle.

En outre, la généralisation du registre des activités de traitement s'étend au sous-traitant. En effet, il doit tenir un registre des traitements mis en œuvre pour le compte de responsables de traitement ([article 30§2b du RGPD](#)).

Le sous-traitant est directement soumis à l'obligation de sécurité prévue à l'article 32 du RGPD ainsi qu'à une obligation de collaboration tant avec

l'autorité de contrôle de protection des données à caractère personnel qu'avec le responsable de traitement (articles 28 et 30 du RGPD).

Compte tenu des obligations que le sous-traitant doit respecter, le RGPD prévoit expressément qu'il puisse être sanctionné en cas de manquement. Le montant maximal des sanctions encourues est identique à celui encouru par le responsable de traitement (Fiche n°15 : Le caractère dissuasif des sanctions).

Le renforcement des obligations contractuelles du sous-traitant

La clause relative à la protection des données à caractère personnel dans le contrat qui lie le responsable de traitement et le sous-traitant est considérablement enrichie par le RGPD. Notons toutefois que certaines des exigences du RGPD étaient déjà insérées dans les contrats par les praticiens.

⇒ Des stipulations sur le traitement de données à caractère personnel sous-traité

Le texte exige en effet que le contrat précise l'objet, la durée, la finalité et la nature du traitement. Les catégories de données à caractère personnel traitées ainsi que les catégories de personnes concernées doivent également figurer dans le contrat.

⇒ Des stipulations sur les missions du sous-traitant

Le responsable de traitement doit s'assurer que le contrat précise expressément que le sous-traitant ne traite les données que sur ses instructions. La nouveauté réside dans le fait que ces instructions doivent être documentées. De ce point de vue, le cahier des charges pourrait être un outil. Les instructions pourront également figurer en annexe du contrat.

Le contrat doit également prévoir que le sous-traitant veille à ce que les personnes traitant les données (salariés, consultants notamment) s'engagent à respecter la confidentialité des données ou soient soumises à une telle obligation.

Comme indiqué précédemment, le sous-traitant est tenu d'une obligation de sécurité en vertu du RGPD. Il doit donc mettre en œuvre des mesures techniques et organisationnelles de nature à protéger les données à caractère personnel qu'il traite pour le compte du responsable de traitement (chiffrement, anonymisation, etc.). Cette obligation doit néanmoins être contractualisée.

En outre, la clause relative à la protection des données à caractère personnel doit préciser qu'une autorisation écrite préalable du responsable de traitement est nécessaire pour tout recours à un prestataire de second rang. Cette autorisation peut être spécifique ou générale. Dans ce dernier

cas, une obligation d'information pèse sur le sous-traitant.

En sus, les obligations contractuelles que le responsable de traitement impose au sous-traitant de premier rang doivent être répercutées aux prestataires de second rang. Par ailleurs, le RGPD prévoit que, vis-à-vis du responsable de traitement, le sous-traitant de premier rang est responsable de la mauvaise exécution de ses obligations par le prestataire de second rang.

Le sous-traitant est également tenu d'une obligation contractuelle de collaboration puisqu'il doit aider le responsable de traitement à satisfaire aux demandes formulées par les personnes dans le cadre de l'exercice de leurs droits.

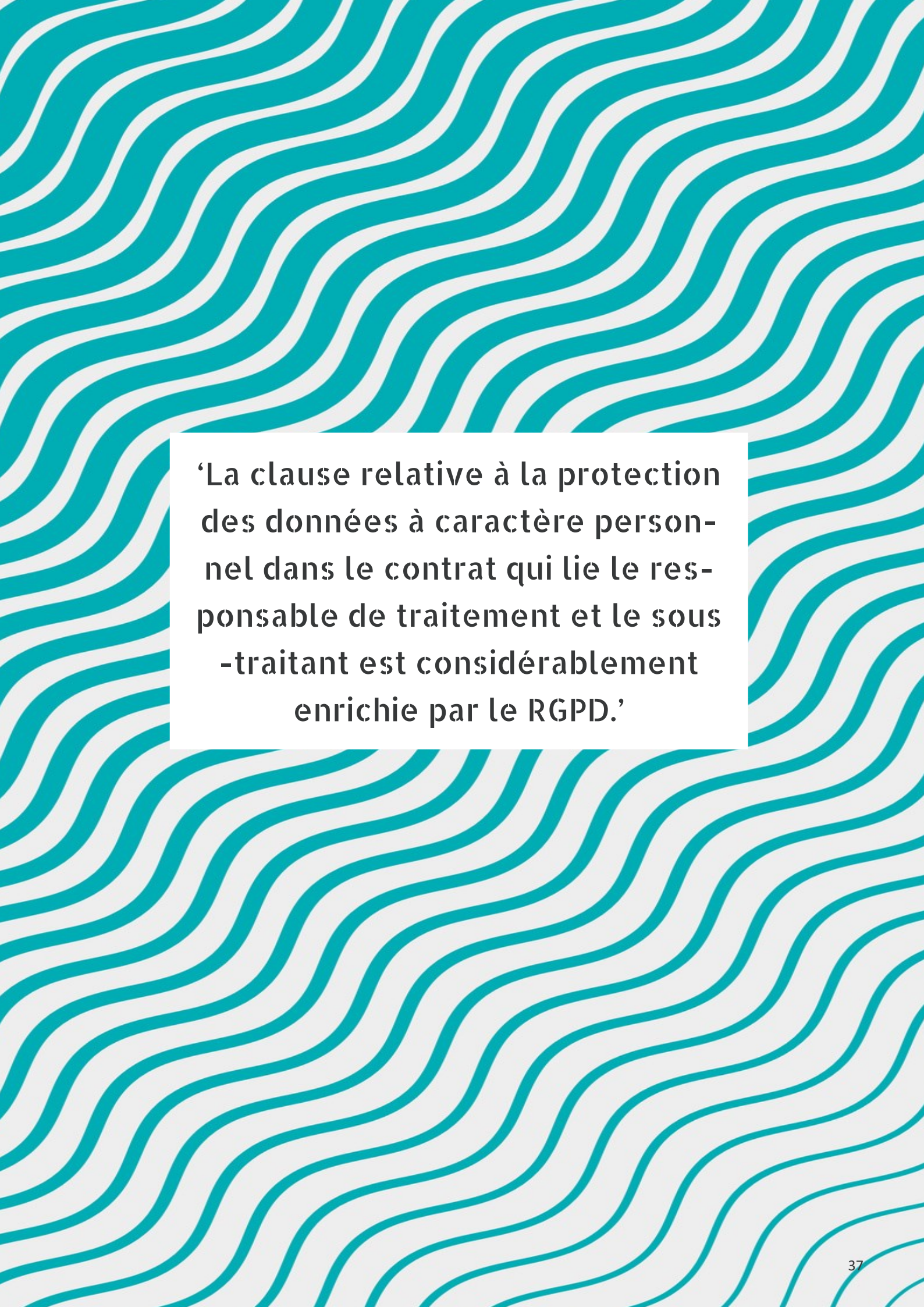
Dans la mesure où il est important que le responsable de traitement puisse vérifier que le sous-traitant respecte ses obligations contractuelles, des audits peuvent être réalisés. Le sous-traitant doit par ailleurs démontrer par tout moyen qu'il respecte ses obligations (Fiche n°6 : Le principe d'accountability).

La fin du contrat est également encadrée par le RGPD en ce qu'il prévoit que le contrat impose au sous-traitant la suppression des données à caractère personnel ainsi que celle des copies ou la restitution intégrale des données traitées, au choix du responsable du traitement.

⇒ L'utilisation par le sous-traitant des données à caractère personnel confiées

Le Règlement européen prévoit expressément que « *si, en violation [du Règlement] un sous-traitant détermine les finalités et les moyens du traitement de données, il est considéré comme un responsable de traitement pour ce traitement* » (article 28§10 du RGPD). Cette hypothèse trouve à s'appliquer lorsque le sous-traitant, en violation du contrat conclu avec le responsable de traitement, réutilise les données à caractère personnel qui lui sont confiées pour mettre en œuvre un traitement dont il est seul à définir la finalité et les moyens.

En pareil cas, le sous-traitant engage sa responsabilité vis-à-vis du responsable de traitement mais il encourt également des sanctions pénales et administratives.



‘La clause relative à la protection des données à caractère personnel dans le contrat qui lie le responsable de traitement et le sous-traitant est considérablement enrichie par le RGPD.’

Fiche 11 - La responsabilité conjointe de traitement organisée

La directive 95/46/CE avait pris en compte la responsabilité conjointe de traitement de données à caractère personnel (article 2, d) de la directive). Celle-ci était caractérisée lorsque plusieurs responsables de traitement concouraient à la définition des finalités et des moyens du traitement. Certes, cette définition était pragmatique en ce qu'elle permettait de prendre en considération des hypothèses atypiques. Toutefois, en pratique, elle aurait pu conduire à l'application concurrente de plusieurs lois de protection des données à caractère personnel en fonction du pays dans lequel les responsables de traitement étaient établis.

Cela étant, au moment de la transposition de la directive en 2004, le législateur français n'a pas consacré la responsabilité conjointe de traitement.

Notons toutefois que dans le secteur du cloud computing, la Cnil avait envisagé que la responsabilité conjointe de traitement s'applique entre le client d'un service de cloud et le prestataire notamment en présence d'offres de service standardisées faisant l'objet de contrats d'adhésion ([Cnil, Cloud computing : les 7 étapes clés pour garantir la confidentialité des données, 1er juillet 2013](#)). Il convient de préciser que si le sous-traitant peut être considéré comme disposant du contrôle des moyens du traitement, il n'est pas l'entité qui définit les finalités du recours au service du cloud computing, ni celle qui détermine la nature des données à

caractère personnel traitées ou encore la durée de conservation des données.

Le RGPD n'est donc pas novateur quant à la définition de la responsabilité conjointe de traitement ([article 26 du RGPD](#)). En revanche, il détermine le régime qui lui est applicable. Notons que le risque d'application de plusieurs lois nationales disparaît, le RGPD étant applicable sur tout le territoire de l'Union européenne.

Un accord entre les responsables conjoints de traitement

Les responsables conjoints d'un traitement de données à caractère personnel sont chacun soumis au RGPD (accountability, privacy by design, privacy by default, etc.).

La situation de responsabilité conjointe implique toutefois qu'ils définissent leurs obligations respectives. Cette répartition doit faire l'objet d'un accord entre les deux organismes, accord qui doit organiser le respect des droits des personnes et l'obligation d'information. Une pratique pourrait consister à considérer que celui des responsables du traitement qui collecte les données à caractère personnel informe les personnes concernées, organise les modalités de recueil du consentement lorsque nécessaire ou encore gère les droits des personnes.

Par ailleurs, en cas de recours à un sous-traitant, celui des responsables du traitement partie au contrat devrait

s'assurer des garanties présentées par le prestataire, s'assurer que le contrat satisfait aux exigences du RGPD...

Les responsables du traitement doivent en outre collaborer afin d'être en mesure de respecter leurs obligations (registre des activités de traitement, coopération avec l'autorité de contrôle, notification des violations de données...).

Une mise à disposition de l'accord

Le RGPD prévoit que « *les grandes lignes* » de l'accord doivent être mises à la disposition de la personne concernée par le traitement. En revanche, le texte ne précise pas les modalités de cette mise à disposition.



Fiche 12 - Le renforcement des droits des personnes et la consécration de nouveaux droits

L'économie numérique est pourvoyeuse de nouveaux services qui requièrent la collecte des données à caractère personnel des utilisateurs. Toutefois, la confiance des utilisateurs susceptibles d'utiliser ces services a pu être altérée par de nombreuses atteintes médiatisées.

Du fait de ce constat, la reconnaissance de nouveaux droits au bénéfice des personnes et le renforcement de ceux préexistants se sont imposés.

Transparence et droits des personnes

Nous soulignerons d'abord que les institutions européennes ont inséré un principe de transparence dans le RGPD (article 12). Ce principe postule que le responsable d'un traitement de données à caractère personnel délivre aux personnes une information concise, transparente, intelligible et dans une forme aisément accessible en utilisant un langage clair.



Ce principe de transparence n'est pas limité à l'information des personnes puisque qu'il impose au responsable de traitement de faciliter l'exercice par les personnes des droits qui leur sont reconnus. Les actions menées en vue du traitement de la demande formulée par la personne ainsi que, le cas échéant, les raisons pour lesquelles il n'est pas donné suite à la demande devront donner lieu à une information sans délai indu et au plus tard un mois à compter de la réception de ladite demande.

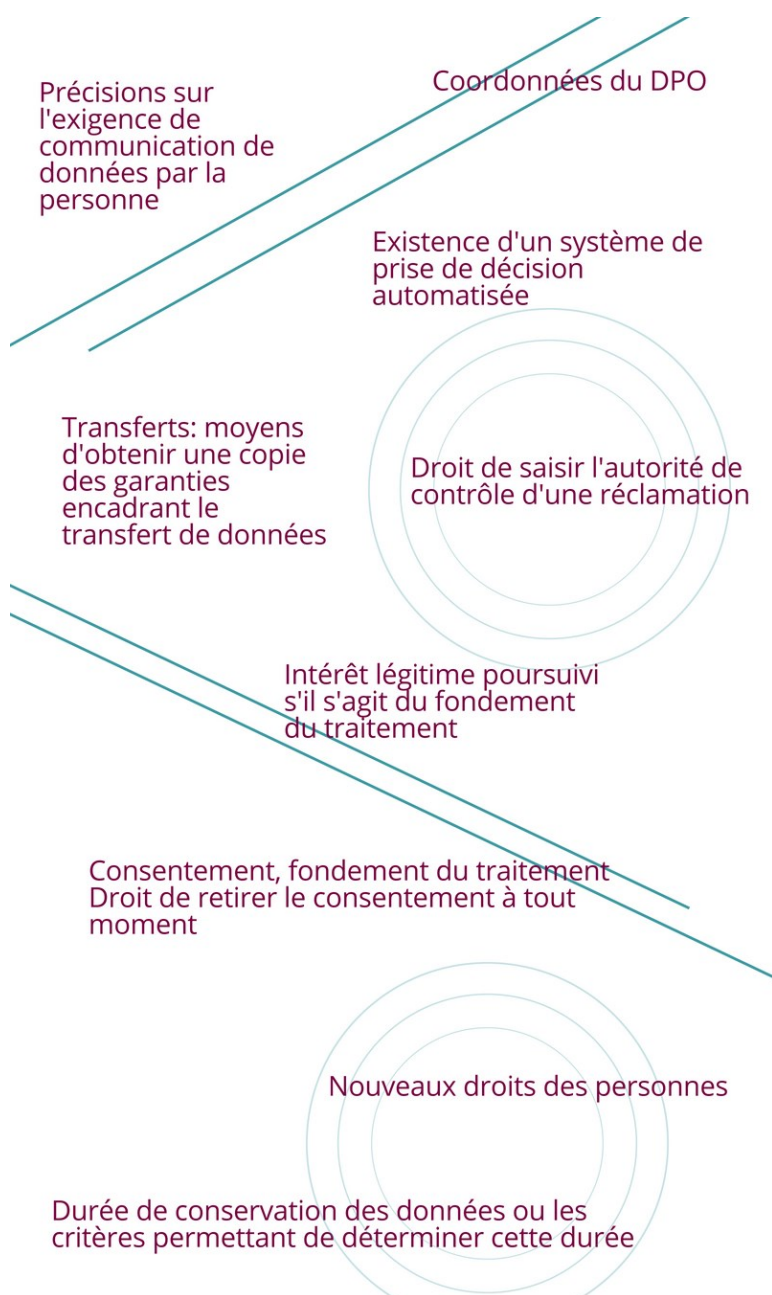
Les institutions européennes ont donc réduit le délai de réponse qui était de deux mois en application du décret d'application de la loi Informatique et Libertés.

Une revue voire une adaptation des procédures de traitement des courriers entrant, qu'ils soient postaux ou électroniques, doit donc être mise en œuvre afin que le responsable de traitement s'assure que les délais qui lui sont impartis sont bien respectés. Une procédure de gestion de ce type de demande peut également être adoptée.

L'information des personnes étendue

Tout en reprenant les exigences de l'article 32 de la loi Informatique et Libertés, les articles 13 et 14 du RGPD étendent le périmètre de l'information à délivrer à la personne, que la collecte des données soit directe ou indirecte. Dans le cadre d'une collecte di-

recte, le responsable de traitement doit compléter son information. De plus, de nouvelles informations doivent être délivrées quant aux nouveaux droits conférés aux personnes.



Des droits nouveaux

Le RGPD conforte les droits des personnes préexistants (droit d'accès, droit de rectification, droit d'opposition, droit à la suppression). Nous avons choisi de nous intéresser aux nouveaux droits consacrés ainsi qu'à leurs conséquences pour le responsable de traitement.

Le droit à la portabilité des données (article 20 du RGPD) représente sans doute l'archétype du pouvoir que les institutions ont souhaité redonner aux personnes sur leurs données à caractère personnel. La consécration de ce droit devrait *a priori* conduire à une mise en concurrence des prestataires de services, les institutions européennes partant du postulat que les personnes se dirigeront vers les prestataires les plus engagés en matière de protection des données à caractère personnel.

L'exercice de ce droit doit permettre aux personnes de récupérer les données à caractère personnel qu'elles ont communiquées par exemple en les téléchargeant, ou de demander la transmission de ces données, par exemple via une API, du responsable de traitement vers un autre prestataire de service, qui deviendra à son tour responsable du traitement.

A titre d'illustration, l'utilisateur d'un service de messagerie devrait pouvoir obtenir dans un format numérique l'ensemble des courriels qu'il a en-

voyés et reçus ainsi que la liste des contacts qu'il a constituée.

Le G29 insiste, dans ses [lignes de conduite](#) adoptées le 13 décembre 2016 et révisées le 5 avril 2017, sur le fait que le nouveau responsable de traitement doit se conformer à son tour au RGPD, et respecter les principes de l'article 5.

Notons par ailleurs que l'exercice par la personne de son droit à la portabilité ne doit pas la priver de l'exercice des autres droits qui lui sont reconnus par le RGPD. Ainsi, le droit à la portabilité ne devra, par exemple, pas faire obstacle au droit à la suppression.

Cela étant précisé, le droit à la portabilité des données n'est pas sans limites comme le montre le schéma ci-après.


DROIT À LA PORTABILITÉ

Deux conditions cumulatives

Caractère automatisé du traitement mis en oeuvre



Traitement fondé sur le consentement ou nécessaire à l'exécution d'un contrat auquel la personne concernée est partie



Selon le guide du G29, pour que les données entrent dans le champ du droit à la portabilité, elles doivent vérifier trois conditions :

- Les données à caractère personnel doivent concerner la personne concernée : seules les données à caractère personnel entrent dans le champ de ce droit ; les données anonymes ou celles qui ne concernent pas la personne concernée ne sont pas couvertes par ce droit.
- Les données doivent être fournies par la personne concernée : sont notamment visées, les données à caractère personnel délibérément communiquées par la personne concernée (adresse électronique, nom, prénom, etc.) ainsi que les données générées par l'utilisation d'un terminal ou d'un service par cette personne (historique de recherche, données de trafic, données de localisation, etc.). Inversement, les données inférées par le responsable de traitement des données fournies par la personne concernée (par exemple, après un traitement algorithmique) ou déduites des données fournies par la personne concernée n'entrent pas dans le champ de ce droit.
- Le droit à la portabilité des données ne doit pas porter atteinte aux droits et libertés d'autres personnes : le « nouveau » res-

ponsable de traitement ne doit par exemple pas traiter les données pour une autre finalité que celle initialement prévue pour ne pas porter atteinte aux droits et libertés des tiers. Ces derniers incluent notamment le secret des affaires et la propriété intellectuelle selon le G29.

Le droit à la portabilité des données aura également des implications d'un point de vue technique. Le considérant 68 du RGPD précise à cet égard qu' « *Il y a lieu d'encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données* ». Les opérateurs doivent donc trouver des solutions afin que la restitution des données aux utilisateurs se fasse dans un format ouvert et standard. De cette manière, les données pourront être lues par tout type de matériel, de manière complète, sans que leur intégrité soit compromise. La question du coût supporté par les entreprises se pose dès lors. De plus, les responsables de traitement doivent informer les personnes concernées de leur droit à la portabilité des données, de manière claire et compréhensible.

Le droit à la limitation du traitement de données à caractère personnel est également une nouveauté (article 18 du RGPD). Il est une illustration du pouvoir redonné par le RGPD aux personnes concernées. En pratique, le RGPD limite la portée de ce droit en ce

qu'il énumère des hypothèses dans lesquelles il pourra être exercé.

DROIT À LA LIMITATION DU TRAITEMENT

Contestation de l'exactitude des données

Illicéité du traitement et préférence de la personne concernée pour la limitation des données (malgré la possibilité d'effacement)

Traitement devenu inutile mais données à caractère personnel nécessaires pour la constatation, l'exercice ou la défense d'un droit en justice

Dans l'attente de la vérification du motif légitime du responsable de traitement après exercice par la personne concernée de son droit d'opposition au traitement

Cette limitation du traitement aura pour conséquence pratique de subordonner le traitement des données au recueil du consentement de la personne notamment.

Sur le fondement du droit à l'effacement ou droit à l'oubli numérique, les personnes peuvent obtenir du responsable de traitement qu'il efface les données à caractère personnel les

concernant. En pratique, ce droit trouve à s'appliquer lorsque la personne a retiré son consentement et que ce dernier était le fondement du traitement ou encore parce que les données à caractère personnel ne s'avèrent plus nécessaires au regard des finalités poursuivies par le responsable de traitement.

Le droit à l'oubli est expressément prévu par les institutions européennes dans le RGPD. Les responsables de traitement qui auraient rendu publiques des données à caractère personnel devront en cas de demande d'exercice du droit à l'oubli prendre des mesures pour répercuter auprès de tiers une demande d'effacement des données à caractère personnel faite par la personne concernée. Ce droit n'est cependant pas absolu puisque les responsables peuvent continuer à traiter les données à caractère personnel si des raisons impérieuses et légitimes justifient la poursuite du traitement.

Face à ces exigences, comment assurer la conformité en pratique ?

En pratique, nous ne pouvons que recommander de réaliser un audit des mentions d'information utilisées. Ces mentions doivent tenir compte des nouvelles exigences européennes.

Les modalités de mise à disposition des garanties utilisées pour encadrer les éventuels transferts de données à caractère personnel doivent égale-

ment être définies. En fonction de la politique que les organismes auront choisi de mettre en place, les clauses contractuelles types peuvent par exemple être mises à disposition du public sur les sites Internet des organismes par exemple. Une copie de ces

clauses pourrait aussi être obtenue auprès du DPO dont les coordonnées sont rendues publiques.

Un moyen de retrait simple du consentement donné par les personnes doit par ailleurs être défini.



Fiche 13 - Les transferts de données à caractère personnel

Les transferts de données à caractère personnel hors de l'Union européenne et plus spécifiquement Outre-Atlantique sont au cœur de l'actualité.

Les règles actuellement en vigueur en matière de transfert de données à caractère personnel sont pour leur grande majorité reprises aux articles 44 et suivants du RGPD.

Clauses contractuelles types et BCR : deux outils confortés

Les outils de transfert antérieurs au RGPD ne sont pas remis en cause. Ainsi, les clauses contractuelles types et les BCR peuvent être utilisées sous l'empire du RGPD. A des fins de simplification, le RGPD a prévu la suppression du mécanisme d'autorisation par la Cnil des transferts encadrés par ces outils.

De nouveaux outils seront également élaborés dans les prochaines années pour encadrer les transferts tels que des mécanismes de certification et des codes de conduite.

Des contrats, *a priori* distincts des clauses contractuelles types, peuvent être conclus entre des responsables de traitement ou entre responsable de traitement et sous-traitant pour encadrer les transferts. Cependant, ces contrats sont soumis au contrôle de la Cnil. Ce mécanisme de vérification existait déjà par le passé, chaque fois que les clauses contractuelles types de la Commission européenne étaient

modifiées par un responsable de traitement.

Précisons que l'autorisation de transfert obtenue antérieurement au 25 mai 2018 de la Cnil après soumission de clauses distinctes de celles de la Commission européenne demeure valable. En revanche, les modifications sont soumises aux conditions prévues dans le RGPD.

Le responsable de traitement peut se référer à la liste des pays établie par la Cnil sur laquelle figure le niveau de protection des données à caractère personnel assuré par chacun d'eux ([Cnil, Transferts hors UE : Liste des pays et niveau de protection des données](#)).

Rappelons par ailleurs qu'au 1er janvier 2015, la Commission européenne avait adopté, sur le fondement de l'article 25§6 de la directive 95/46/CE, une décision d'adéquation concernant Andorre, l'Argentine, les Îles Féroé, Guernesey, Israël, l'Île de Man, Jersey, la Nouvelle-Zélande, la Suisse, l'Uruguay et le Canada reconnaissant leur législation comme assurant un niveau de protection adéquat. Toutefois, compte tenu de l'annulation par la Cour de justice de l'Union européenne de la décision d'adéquation de la Commission européenne sur le Safe Harbor, la liste des pays précitée est susceptible de faire l'objet de modifications à tout moment. Les décisions d'adéquation de la Commission européenne prises en application du RGPD doivent être

réexaminées tous les quatre ans afin de prendre en compte les évolutions qui auraient pu avoir lieu dans les pays tiers.

Transferts de données exigés par des autorités administratives ou judiciaires

Tout transfert de données à caractère personnel effectué sur la base d'une

décision rendue par une juridiction ou prise par une autorité administrative d'un Etat tiers à l'Union européenne sera contraire au RGPD à moins qu'un accord international le prévoie.

En pratique, les responsables de traitement doivent donc préalablement à tout transfert de données déterminer si la décision s'inscrit dans le champ d'un accord international.



Fiche 14 - Les autorités de contrôle : quel rôle à l'heure de la suppression des formalités préalables ?

Les autorités de contrôle conservent leurs missions premières de vérification de la bonne application des règles relatives à la protection des données à caractère personnel, de sensibilisation du public et d'accompagnement des responsables de traitement et des sous-traitants. Ces compétences s'exercent par principe sur le territoire de l'Etat membre dont l'autorité relève.

La Cnil, autorité nationale de contrôle pour la France

Sans surprise, la loi relative à la protection des données personnelles adoptée le 14 mai 2018 a désigné la Cnil comme autorité nationale de contrôle. La loi énumère les nouvelles missions qui lui sont confiées au titre du RGPD, et charge la Cnil de les accomplir en prenant en considération la variété des acteurs impliqués dans les traitements de données à caractère personnel.


Ainsi, la Cnil doit prendre en compte « *la situation des personnes dépourvues de compétences numériques* », mais aussi les besoins spécifiques des collectivités territoriales, des micro-entreprises, des petites et des moyennes entreprises.

Le système du guichet unique

GUICHET UNIQUE AUTORITÉ CHEF DE FILE

Autorité de contrôle de protection des données située sur le territoire de l'Etat membre dans lequel le responsable de traitement ou le sous-traitant a son établissement principal ou son unique établissement

- 1** Administration centrale (siège social)
- 2** Essentiel des activités de traitement (à défaut d'administration centrale)
- 3** Autorité chef de file, seul interlocuteur
- 4** Compétence résiduelle des autres autorités (plainte)
- 5** Coopération des autorités de contrôle (échanges, assistance mutuelle, opérations conjointes, etc.)



La collaboration entre autorités de protection des données fait l'objet d'une organisation nouvelle, notamment en raison de l'instauration du mécanisme du guichet unique. Le G29 a révisé et adopté en avril 2017 les [lignes directrices](#) pour identifier l'autorité chef de file.

⇒ Dans quels cas est-il nécessaire d'identifier une autorité chef de file ?

Identifier une autorité chef de file n'est nécessaire que lorsqu'un traitement transfrontalier est mis en œuvre, c'est-à-dire un traitement effectué par un responsable de traitement ou un sous-traitant établi dans plusieurs Etats membres et/ou un traitement qui affecte sensiblement des personnes concernées dans plusieurs Etats membres. D'après les lignes directrices adoptées par le G29, l'expression « affecte sensiblement », non définie dans le RGPD, doit être interprétée au cas par cas, en prenant en compte le contexte du traitement, le type de données, l'objet du traitement et certains autres facteurs comme les possibles dommages que le traitement peut causer, les effets probables sur les droits, etc.

⇒ Comment identifier l'établissement principal du responsable de traitement ou du sous-traitant ?

Pour le responsable de traitement, l'établissement principal correspond au « *lieu de son administration centrale dans l'Union* ». Cette définition semble indiquer que l'autorité compétente est celle du pays de l'Union sur le territoire duquel le responsable de traitement a son siège social.

Toutefois, s'il s'avère que le pouvoir décisionnel relatif à la définition des finalités et des moyens d'un traitement donné est exercé dans un autre établissement, compétence est donnée à l'autorité de contrôle du pays dans lequel cet établissement se trouve, pour ce traitement. Ainsi, dans certaines hypothèses, il semblerait que plusieurs autorités chef de file puissent être identifiées.

Pour le sous-traitant, l'établissement principal est défini par référence au « *lieu de son administration centrale dans l'Union* ». A défaut d'administration centrale, cet établissement est celui où « *l'essentiel des activités de traitement* » est effectué. Le G29 nous guide quant aux critères à prendre en compte afin de déterminer ce lieu de traitement : le lieu où les décisions sont effectivement exécutées, le lieu où les décisions sont prises finalement, le lieu où la société est enregistrée, etc.

La charge de la preuve quant au lieu où le traitement est mis en œuvre pèse sur le responsable de traitement ou le sous-traitant.

- ⇒ Une fois l'établissement principal identifié, quelle sera la conséquence pratique de cette nouvelle organisation ?

L'autorité de contrôle chef de file est le seul interlocuteur du responsable de traitement ou du sous-traitant.

Toutefois, le RGPD maintient une compétence résiduelle des autres autorités de contrôle. En effet, chaque autorité de contrôle nationale demeure compétente pour connaître d'une réclamation introduite auprès d'elle si son objet ne vise qu'un établissement situé dans l'Etat membre dont elle dépend ou en cas d'infraction au RGPD si celle-ci n'affecte que les personnes concernées dans l'Etat membre dont elle dépend.

L'autorité chef de file doit être informée de cette réclamation ou infraction au RGPD et peut ensuite décider de gérer ou non le cas.

- ⇒ Comment les autorités de contrôle vont-elles coopérer ?

Le RGPD organise la coopération des autorités de contrôle en ce qu'elles doivent s'échanger des informations, et s'apporter une assistance mutuelle, voire mener des opérations conjointement (enquêtes et contrôles notamment) [articles 56, 60 et 61 du RGPD.]. Elles ont la compétence de décider discrétionnairement laquelle des autorités sera l'autorité chef de file.

La [loi relative à la protection des données personnelles](#) précise que lorsque la Commission nationale de l'informatique et des libertés (Cnil) agit en tant qu'autorité chef de file, elle est tenue de communiquer le rapport du membre rapporteur et toutes informations utiles à la procédure aux autorités de contrôle concernées.

De plus, l'autorité de contrôle d'un autre Etat membre souhaitant faire effectuer des contrôles par ses agents sur le territoire français doit demander au préalable au président de la Cnil une habilitation spécifique, qui ne lui est délivrée que si les agents présentent des garanties comparables à ceux requises pour les agents de la Cnil.

Les pouvoirs des autorités

Les pouvoirs des autorités de contrôle sont nombreux. Elles disposent d'un pouvoir d'enquête leur permettant d'obtenir la communication de toute information ou encore l'accès à toutes les données nécessaires à l'exercice de leurs missions ainsi qu'aux locaux des organismes. Elles peuvent également mener des audits auprès des organismes responsables de traitement et sous-traitants.

Elles peuvent adopter des mesures dites correctrices qui consistent par exemple à avertir un responsable de traitement de la non-conformité des traitements mis en œuvre avec le RGPD. Elles peuvent en outre ordon-

ner aux organismes de satisfaire aux demandes d'exercice par les personnes de leurs droits. Dans les cas où la consultation préalable des autorités de contrôle sera nécessaire (analyse d'impact révélant une atteinte aux droits et libertés des personnes ou si la loi nationale d'un Etat membre le prévoit), les autorités de contrôles disposent des pouvoirs consultatifs et d'autorisation le cas échéant.

La création d'un comité européen de la protection des données

Ce Comité regroupera l'ensemble des présidents des autorités de contrôle de chacun des Etats membres ainsi que le Contrôleur européen à la protection des données à caractère personnel. Ce Comité remplacera le G29 instauré par l'article 29 de la directive 95/46/CE

A l'instar de ce que fait actuellement le G29, ce Comité pourra publier de la documentation (lignes directrices, recommandations, bonnes pratiques, etc.). Il pourra également examiner des questions relatives à l'application du RGPD.

Ce Comité veillera surtout à l'application uniforme du RGPD dans l'ensemble de l'Union européenne. Ainsi devra-t-il être consulté pour avis préalablement à toute décision d'une autorité de contrôle visant à l'adoption d'une liste de traitements soumis à l'obligation d'effectuer une analyse

d'impact ou encore visant à adopter des clauses contractuelles types.

Il sera également chargé de l'analyse de toute question sur l'application générale du RGPD ou sur toute question susceptible de produire des effets dans plusieurs Etats Membres.

Ce Comité pourra également émettre des décisions contraignantes (en cas de divergences quant à la désignation de l'autorité chef de file par exemple).

Fiche 15 - Le caractère dissuasif des sanctions

Le caractère non dissuasif et disparate des sanctions prononcées par les autorités de contrôle est depuis longtemps décrié.

L'amende maximale de 150 000€ prononcée par la Cnil à l'égard de la société Google a été médiatisée sans pour autant contraindre le géant américain à infléchir sa politique en matière de protection des données à caractère personnel ou dissuader les autres GAFAs (« [La formation restreinte de la Cnil prononce une sanction pécuniaire de 150 000 € à l'encontre de la société GOOGLE Inc.](#) » relative aux règles de confidentialité ou encore « [Droit au déréférencement : la formation restreinte de la Cnil prononce une sanction de 100.000 € à l'encontre Google](#) » relative au droit au déréférencement). En témoigne la récente [mise en demeure publique de la société Facebook par la Cnil](#) en raison de nombreux manquements à la législation en vigueur.

C'est sans doute la raison pour laquelle les institutions européennes ont tenu à faire figurer dans le RGPD que les amendes prononcées en cas d'infraction aux règles applicables doivent être « *effectives, proportionnées et dissuasives* » ([article 83 du RGPD](#)).

Quels organismes sont passibles de sanction ?

En application de la réglementation française et européenne antérieures, seul le responsable de traitement en-

courrait des sanctions administratives prononcées par la Cnil. Le sous-traitant n'avait en effet pas d'autres obligations que celles fixées en matière de sécurité et de confidentialité des données à caractère personnel dans le contrat conclu avec le responsable de traitement.

Le RGPD a introduit du changement en la matière. En effet, tenu à des obligations en application du RGPD, le sous-traitant est désormais susceptible d'être sanctionné par la Cnil en cas d'infraction.

Les critères pris en compte

Le RGPD énumère une série de critères que les autorités de contrôle doivent prendre en compte pour prononcer une sanction contre un responsable de traitement ou un sous-traitant. Parmi ces derniers, figurent notamment la nature, la gravité et la durée de l'infraction, la commission délibérée ou par négligence de l'infraction.

Quelle amende pour quelle infraction ?

Les institutions européennes ont créé deux catégories de sanction.

Certaines infractions peuvent être sanctionnées d'une amende d'un montant de 10 000 000€ maximum ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent maximum

(absence de protection des données dès la conception et par défaut, défaut de sécurité des données, absence de notification des violations de données, absence de registre des traitements ou encore non-respect des règles de désignation du DPO).

D'autres infractions peuvent être sanctionnées d'une amende d'un montant

de 20 000 000€ ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent maximum (non-respect des principes de la protection des données à caractère personnel, infraction aux règles applicables au consentement ou encore infractions aux dispositions relatives aux transferts de données à caractère personnel hors de l'EEE).



Fiche 16 - L'action de groupe relative à la **protection des données à caractère personnel**

L'action de groupe, mécanisme hérité du droit américain (*class action*), connaît un processus de démocratisation en France. Ouverte initialement aux seuls domaines de l'environnement et de la santé, la loi n°2016-1547 du 18 novembre 2016 de modernisation de la justice du XXIème, complétée par le décret n°2017-888 du 6 mai 2017, ouvre l'action de groupe notamment au domaine de la protection des données à caractère personnel, pour les manquements à la loi 78-17 du 6 jan-

vier 1978 dite loi Informatique et Libertés.

La loi relative à la protection des données personnelles adoptée le 14 mai 2018 est venue compléter ce dispositif : les actions de groupe pourront désormais être fondées sur des dispositions du Règlement général sur la protection des données (RGPD). De plus, il est désormais possible d'obtenir par une action de groupe la réparation des préjudices subis.

Quelles sont les personnes concernées ?

Tribunal compétent	Juge judiciaire :	Juge administratif :
Qualité de la personne ayant manqué à ses obligations	* Tribunal de Grande Instance (TGI) du lieu de résidence du défendeur ; * TGI de Paris si le défendeur réside à l'étranger	* Tribunal administratif si les requêtes individuelles relèvent de la compétence d'une seule juridiction * Le Conseil d'État si les requêtes individuelles relèvent de plusieurs juridictions
Qualité de la personne ayant subi un dommage	Plusieurs personnes placées dans une situation similaire ayant subi un dommage causé par un responsable du traitement de données à caractère personnel ou un sous-traitant, ayant pour cause commune un manquement de même nature aux dispositions de la loi n°78-17 du 6 janvier 1978 dite « Informatique et Libertés » ou du Règlement général sur la protection des données (Règlement (UE) 2016/679 dit « RGPD »)	
Personnes ayant qualité pour agir	<ul style="list-style-type: none"> - Les associations régulièrement déclarées depuis 5 ans au moins ayant pour objet statutaire la protection de la vie privée et la protection des données à caractère personnel ; - Les associations de défense des consommateurs représentatives et agréées lorsque le traitement de données à caractère personnel affecte des consommateurs ; - Les organisations syndicales de salariés ou de fonctionnaires représentatives lorsque le traitement affecte les salariés ou les fonctionnaires. 	

Quel est l'objet de l'action de groupe ? Y a-t-il un préalable ? Quel est le rôle du juge ?

<p align="center">Objet de l'action de groupe</p>	<p>Cessation du manquement ou engagement de la responsabilité de la personne ayant causé le dommage afin d'obtenir la réparation des préjudices matériels et moraux subis ou ces deux fins. Cependant, la responsabilité de la personne ayant causé le dommage ne peut être engagée que si le fait générateur du dommage est postérieur au 24 mai 2018.</p>	
<p align="center">Mise en demeure – condition préalable à l'introduction de l'instance</p>	<p>Préalablement à l'introduction de l'action de groupe mise en demeure à la personne de cesser ou de faire cesser le manquement ou de réparer les préjudice subis : l'action de groupe ne peut être introduite qu'à l'expiration d'un délai de 4 mois à compter de la réception de la mise en demeure.</p> <p>Le demandeur doit informer la Commission nationale de l'informatique et des libertés.</p>	
<p align="center">L'assignation – Introduction à l'instance</p>	<p>Juge judiciaire</p> <p>L'assignation doit comporter, sous peine de nullité :</p> <ul style="list-style-type: none"> * L'indication de la juridiction devant laquelle la demande est portée ; * La demande de cassation du manquement avec un exposé des faits ; * L'indication des modalités de comparution devant la juridiction et la précision que, faute pour le défendeur de comparaître, il s'expose à ce qu'un jugement soit rendu contre lui sur les seuls éléments fournis par son adversaire ; * Les cas individuels présentés par le demandeur au soutien de son action. 	<p>Juge administratif</p> <p>L'assignation doit comporter, sous peine de nullité :</p> <ul style="list-style-type: none"> * La personne morale de droit public ou l'organisme de droit privé chargé de la gestion d'un service public visé par l'action ; * La nature du manquement et des dommages invoqués ; * Les éléments permettant d'apprécier la similarité des situations des personnes en faveur desquelles l'action est présentée ; * Les cas individuels au vu desquels l'action est engagée.

Abonnez-vous à notre Newsletter :

www.avocats-mathias.com



Mathias Avocats

Nous sommes un cabinet spécialisé dans le droit du digital et accompagnons nos clients au gré des changements que le monde numérique implique.

Nos clients font partie des plus grands groupes bancaires ou sont des entreprises leaders dans l'innovation digitale. Nous représentons également des startups, au développement desquelles nous avons participé au fil des ans.



Avez-vous une question ?

Une équipe dédiée pour vous accompagner dans la réalisation de vos ambitions.

01 43 80 02 01

contact@avocats-mathias.com

19, rue Vernier – 75017 – Paris

Retrouvez les conseils pratiques de nos avocats
sur Twitter :
[@GaranceMathias](https://twitter.com/GaranceMathias)

