Mathias Avocats

LIVRE BLANC

Anticiper le Règlement européen sur les données personnelles

14 fiches pratiques

www.avocats-mathias.com

LABEL CNIL FORMATION

SOMMAIRE

Fiche n°1 : Historique

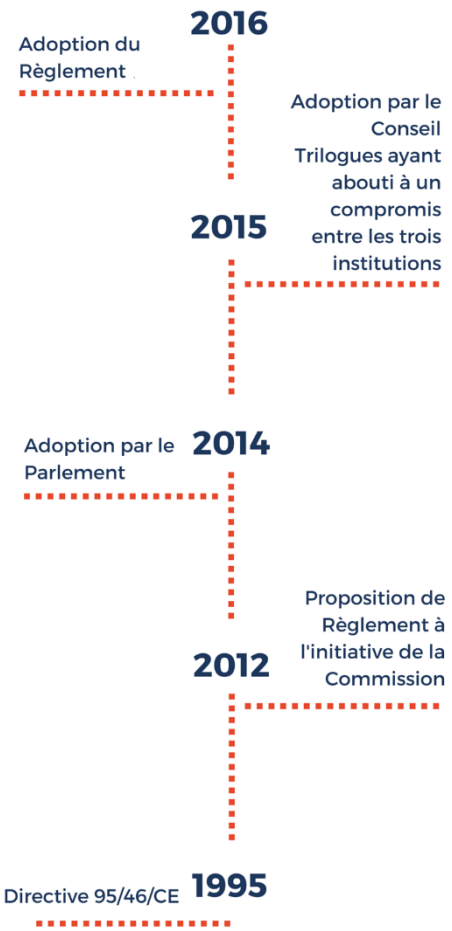
2016 est l'année de la protection des données personnelles. Après quatre années de débats, la Commission européenne, le Parlement européen et le Conseil de l'Union ont abouti à un texte de compromis le 15 décembre 2015.

Le Règlement a été formellement approuvé par les institutions et publié au Journal Officiel de l'Union européenne **le 4 mai 2016**.

Rappelons que l'ancienne réglementation résulte de la directive 95/46/CE du 24 octobre 1995[1], chaque Etat membre de l'Union européenne ayant ensuite transposé cette directive dans son droit national.

Le processus de négociation du nouveau cadre avait été lancé en 2012 par la Commission européenne, institution à l'origine de la proposition de Règlement. Le Parlement européen avait ensuite adopté sa version du texte en mars 2014. Le Conseil de l'Union européenne avait rendu sa copie en juin 2015. Les réunions du trilogue réunissant les représentants des trois institutions européennes ont débuté le 24 juin 2015 pour se poursuivre jusqu'au 15 décembre 2015.

Le Règlement poursuit notamment un objectif d'harmonisation des législations européennes puisqu'il sera directement applicable dans chaque Etat membre sans qu'aucune transposition ne soit nécessaire. La singularité réside dans le fait que le Règlement ne sera applicable que deux ans à compter de la date de son entrée en vigueur, soit le **25 mai 2018**. Pendant les deux années de transition, période qui permettra à toutes les parties concernées de se mettre en conformité, la Commission européenne envisage d'organiser des opérations de sensibilisation à destination des citoyens et des entreprises[2].



Cette nouvelle réglementation devrait permettre également de favoriser l'innovation au sein du marché unique du numérique tout en garantissant un **niveau élevé de protection** des citoyens.

En effet, le contexte dans lequel s'inscrit ce Règlement n'est pas neutre.

Les citoyens sont aujourd'hui sensibilisés à l'utilisation de leurs données personnelles. De nombreuses entreprises innovantes fondent leur business plan sur l'exploitation de la donnée personnelle, ce qui fait dire à certains que la donnée est l'or noir du XXI^{ème} siècle. De nouveaux outils toujours plus consommateurs et producteurs de données personnelles (objets connectés notamment) voient le jour. L'ère est aux données ouvertes (***Open data***) ainsi qu'au traitement massif des données (***Big data***) grâce à des algorithmes

[1] 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

[2] Agreement on Commission's EU data protection reform will boost Digital Single Market, European Commission, Brussels, 15 December 2015

toujours plus sophistiqués et aux capacités de stockage qui augmentent de manière exponentielle.

Dans le même temps, le scandale des écoutes des citoyens européens par les autorités américaines (« Affaire Snowden ») a démontré toute la complexité de parvenir à une protection efficace. La disparité en Europe du pouvoir de sanction pécuniaire des autorités nationales de contrôle et le faible impact de ces sanctions sur les « GAFA » (Google Amazon Facebook Apple) ont illustré les limites du cadre de protection des données personnelles actuel.

La jurisprudence de la Cour de Justice de l'Union européenne a également nourri les débats sur le renforcement de la protection des données personnelles.

En avril 2014, elle a déclaré l'invalidité de la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public[3]. En mai 2014, elle a reconnu le droit pour toute personne d'obtenir d'un moteur de recherche le déréférencement d'informations[4].

La Cour de Luxembourg a également élargi la notion d'établissement au sens de l'article 4 de la directive 95/46/CE qui permet d'appliquer la loi nationale de protection des données personnelles d'un Etat membre autre que celle du pays dans lequel le responsable de traitement est immatriculé[5]. La Cour de justice a également rappelé qu'une administration devait informer les personnes dont elle traite les données personnelles de leur transmission à une autre administration ainsi que l'obligation pour l'administration destinataire d'informer les personnes sur le traitement qu'elle met en œuvre[6].

La Cour a en outre invalidé la décision d'adéquation de la Commission européenne permettant le transfert de données personnelles aux Etats-Unis dans le cadre de la sphère de sécurité « *Safe harbor* »[7].

La Commission européenne annonçait, sur ce dernier point, le 2 février 2016 s'être entendue avec les autorités américaines sur les bases d'un nouvel accord baptisé le *Privacy Shield*. Selon la Commission européenne, cet accord devrait permettre d'encadrer les transferts de données personnelles outre-Atlantique dans le respect des droits fondamentaux des citoyens européens[8]. Le 12 juillet, les fonctionnaires européens et l'administration américaine ont validé ces nouvelles règles.

Ce Livre Blanc est donc l'occasion d'aborder de manière pratique les principaux points consacrés par le Règlement européen. Des articles seront consacrés plus spécifiquement au **profilage** et au **data mining**, ou encore à l'**anonymisation** des données sur le site Internet de Mathias Avocats.

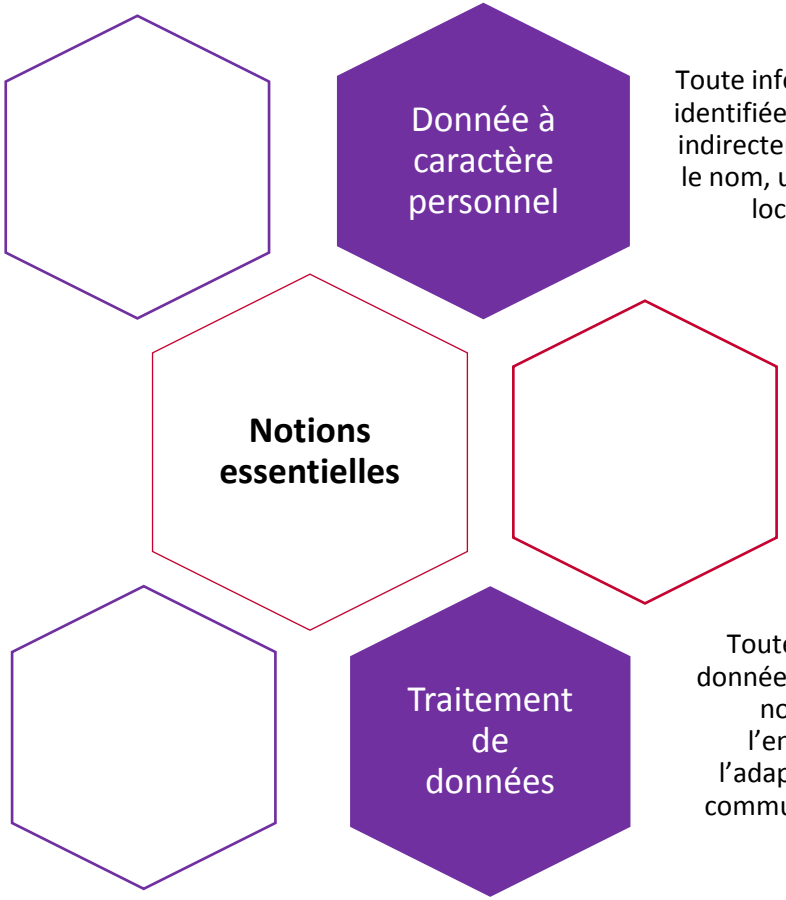
Nous vous souhaitons une bonne lecture, en espérant sincèrement que ces fiches pourront vous être utiles dans vos projets, pour lesquels nous restons à votre disposition.

Garance Mathias
Avocat à la Cour

[3] CJUE, gde ch., 8 avril 2014, aff. C-293/12, Digital Rights Ireland
[4] CJUE, gde ch., 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc.
[5] CJUE, 3e ch., 1er oct. 2015, aff. C-230/14, Weltimmo
[6] CJUE, 3e ch., 1er oct. 2015, aff. C-201/14, Bara
[7] CJUE, gde ch., 6 oct. 2015, aff. C- 362/14, Schrems
[8] Le « Privacy Shield » : un bouclier pas si protecteur ?, Mathias avocats, http://www.avocats-mathias.com/donnees-personnelles/privacy-shield-donnees-personnelles

Fiche n°2 : Les notions essentielles de la protection des données à caractère personnel

Avant de procéder à l'analyse proprement dite du Règlement européen, nous vous proposons un rappel terminologique des notions clefs de la protection des données enrichi des apports du Règlement[9].

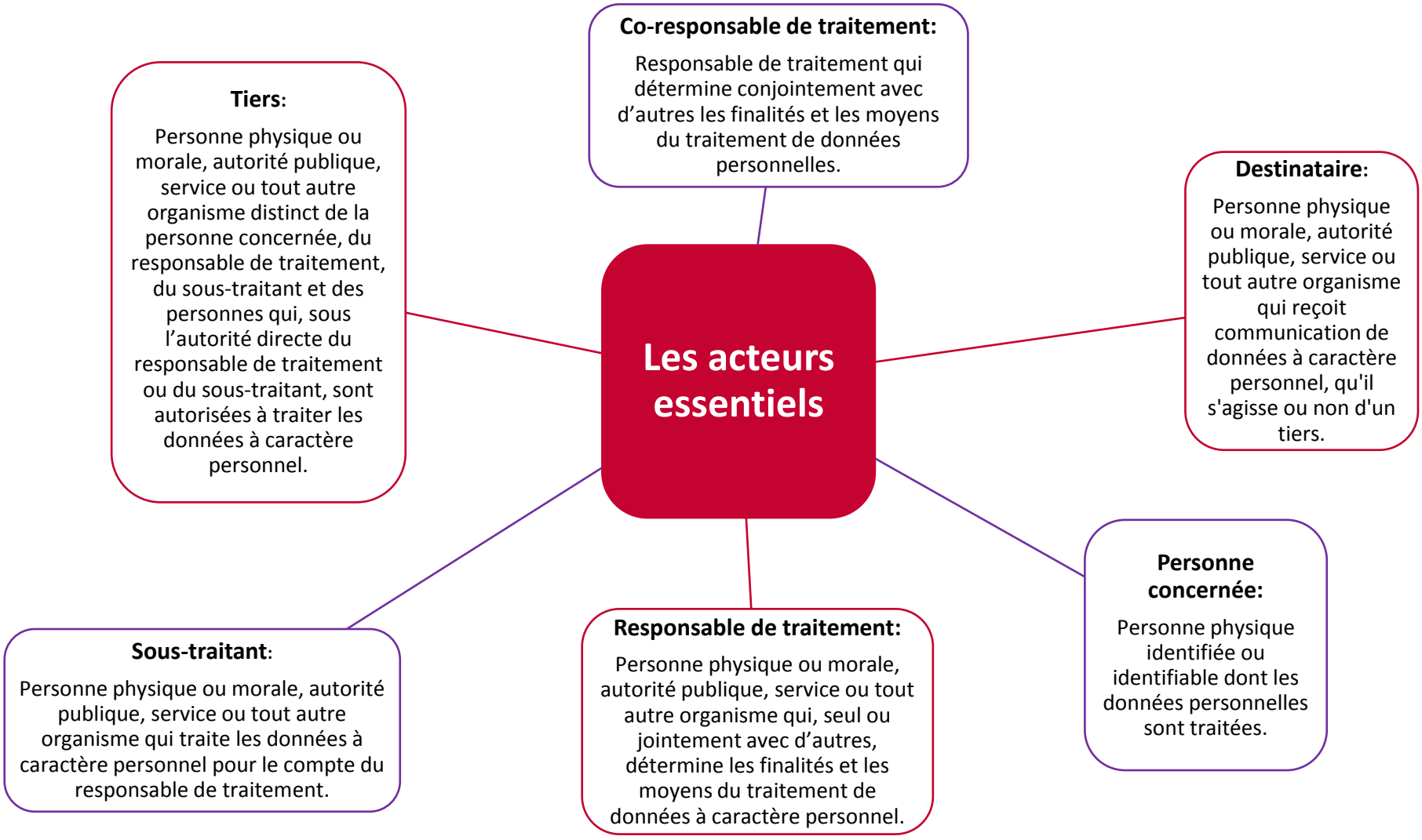


Toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement par référence à un identifiant tel que le nom, un numéro d'identification, une donnée de localisation, un identifiant en ligne, etc.

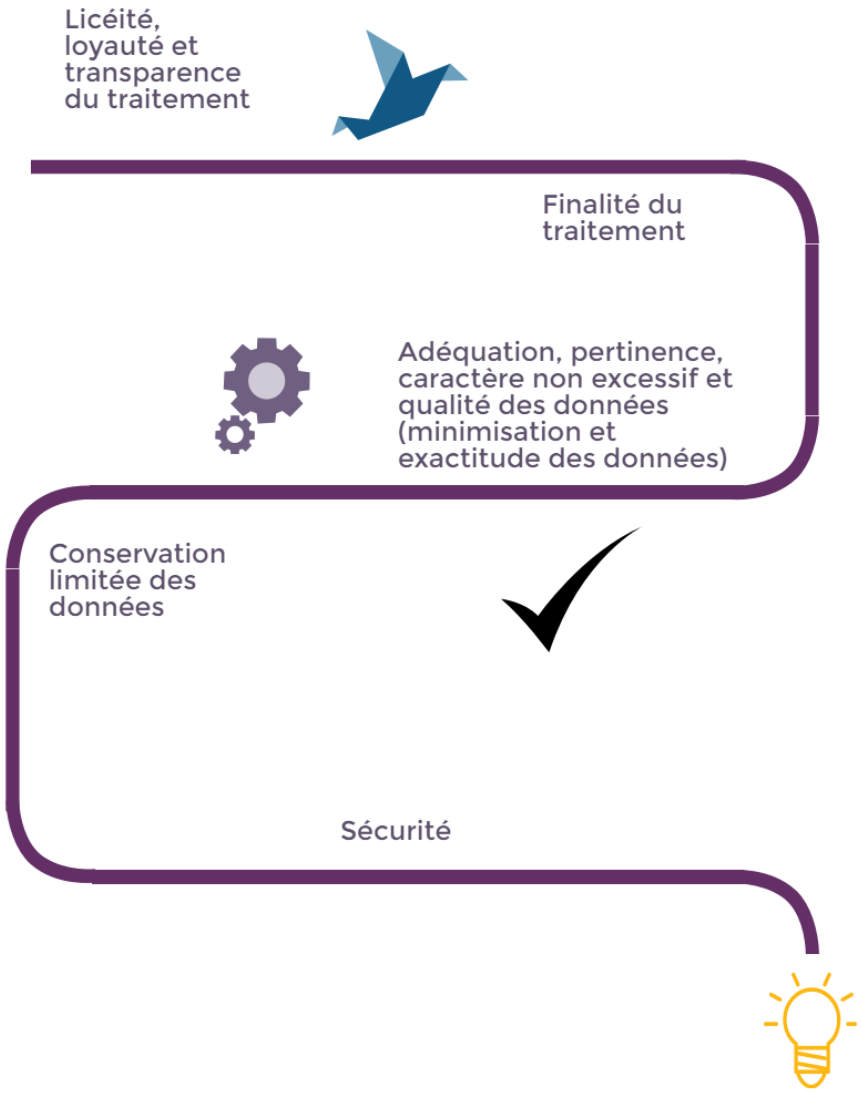
Toute opération ou ensemble d'opérations effectués sur des données à caractère personnel que le procédé soit automatisé ou non. Constituent notamment un traitement la collecte, l'enregistrement, l'organisation, le stockage, l'extraction, l'adaptation ou la modification, la consultation, l'utilisation,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

[9] Article 4 « *Définitions* » du Règlement européen

Fiche n°3 : Les acteurs de la protection des données à caractère personnel



Fiche n°4 : Les principes de la protection des données personnelles réaffirmés



Les principes, clé 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 Règlement.

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 actuelle, les responsables de traitement continueront de devoir justifier, après l'entrée en vigueur du Règlement, d'une finalité déterminée, explicite et légitime pour tout traitement de données à caractère personnel mis en œuvre.

Ils devront 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 personnelles.

Qu'est-ce que la minimisation des données ? Ce principe désigne la proportionnalité entre les données personnelles traitées et la finalité du traitement (caractère adéquat, pertinent et non excessif des données traitées).

La qualité des données personnelles compte également parmi les principes de la protection des données. Celles-ci devront 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 sera un enjeu important pour le responsable de traitement car elle devra 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

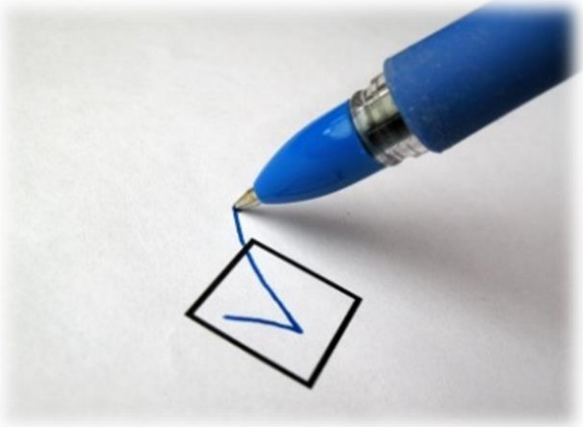
Les conditions de la licéité d'un traitement sont définies par l'article 6 du Règlement. En tant que responsable de traitement, un organisme pourra fonder la légitimité du traitement sur l'un des critères suivants :

- 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 Règlement 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 Règlement). 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 Règlement européen prévoit un régime spécifique aux traitements de données personnelles 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 effet, le consentement des personnes dépositaires de l'autorité parentale devra être recueilli. 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 n°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 Règlement européen 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, sera soumise aux exigences du Règlement.

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 État 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 traitement 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 devra 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.

Fiche n°6 : Le principe d'accountability

Au système déclaratif actuel, le Règlement 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 personnelles.

Article 24 du Règlement

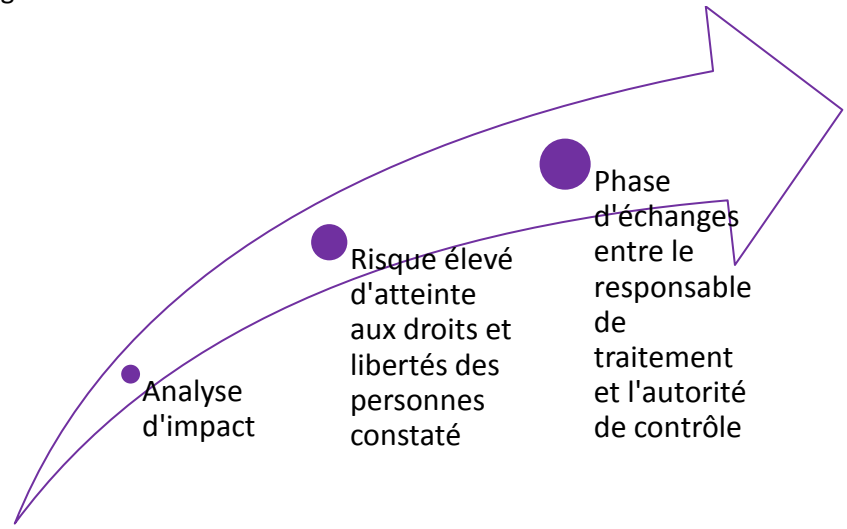
« 1. Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre des mesures techniques et organisationnelles 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.

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

Toutefois, l'article 36 du Règlement européen prévoit un régime de consultations préalables de l'autorité de contrôle comme illustré par la figure ci-dessous.



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. 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.

En pratique, le principe de responsabilité impliquera que le responsable d'un traitement de données personnelles 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 devront également être identifiés ainsi que leur probabilité de survenance et gravité évaluées. Les mesures ne seront donc pas les mêmes pour tous les organismes. **Les études d'impact et analyses de risques devront être privilégiées.**

La politique de protection des données personnelles adoptée au sein d'un organisme sera ainsi rédigée sur-mesure.

Des mesures diversifiées

Les mesures techniques et organisationnelles mises en place par le responsable de traitement seront de nature diverse. De manière générale, elles seront matérialisées par toutes les dispositions prises par l'entreprise pour respecter les obligations qui lui incomberont en application du Règlement européen (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 personnelles par défaut et dès la conception feront 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* »[10]).

La protection des données personnelles devra être intégrée dès la conception des systèmes et des technologies mis en place. Le Règlement précise que ce principe devra 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** personnelles, principe en vertu duquel les données personnelles doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* »[11].

Ce principe connu des responsables de traitement, puisqu'il figure 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 Règlement prévoit expressément que les données personnelles ne devront pas être rendues accessibles à « *un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée* ». Une marge de manœuvre devra donc être laissée aux personnes dont les données sont traitées. De ce point de vue, la personne retrouve la **maîtrise** de ses données personnelles puisqu'il lui appartiendra de modifier les paramètres.

[10] Article 25 du Règlement européen

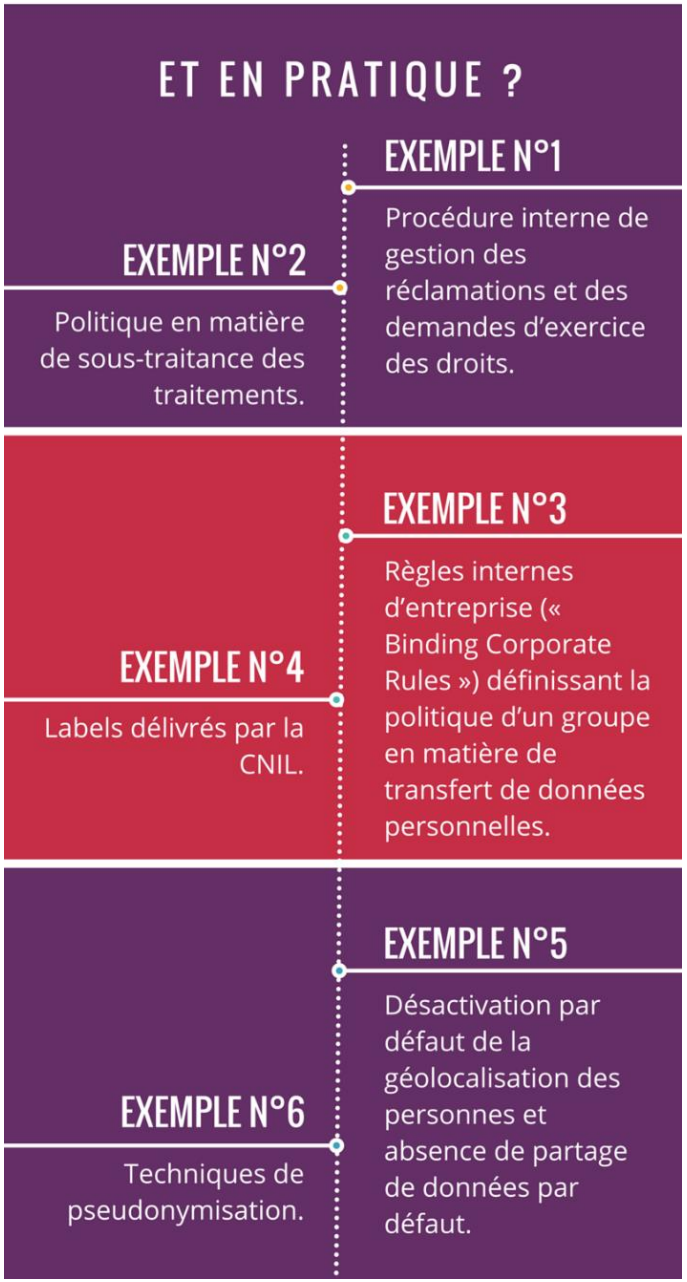
[11] Article 5,1, c) du Règlement européen

ACCOUNTABILITY

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, voici quelques exemples.



Mathias Avocats

Le registre de traitement pour tous, une mesure pertinente

La **généralisation** de la tenue d'un registre des traitements mis en œuvre[12] participera également de la démarche de responsabilité des organismes. Jusqu'à présent, le registre des traitements de données personnelles était celui établi par le Correspondant Informatique et Libertés (CIL) de l'organisme responsable de traitement qui l'avait désigné.

Le Règlement 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.* ». Le Règlement ne prévoit pas qu'il appartienne au délégué à la protection des données personnelles (DPO) de tenir ce registre. Toutefois, en pratique, il est possible de s'interroger sur la marge de manœuvre laissée à un CIL devenu DPO pour ne plus tenir ce registre. Dans ce type de situation, la continuité de la mise à jour du registre n'imposerait-elle pas que le DPO assure ce suivi ?

Indépendamment de cette question, notons que les entreprises de moins de 250 salariés ne seront 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 personnelles sensibles ou relatives à des condamnations et infractions pénales.

Certains des éléments du registre énumérés par le Règlement sont déjà mentionnés dans le registre du CIL, d'autres sont nouveaux. Ainsi, 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 personnelles) ;
- les finalités du traitement ;
- la description des catégories de personnes concernées, des catégories de données et des catégories de destinataires des données personnelles ;
- les transferts de données personnelles 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 donnée.

Comment faire face à ces exigences ?

Afin de vous préparer au Règlement européen, il est d'ores et déjà possible d'identifier et de passer en revue les différentes politiques internes en lien avec la protection des données personnelles. Un audit des traitements mis en œuvre peut également être réalisé avec l'assistance d'experts techniques et juridiques. Une comparaison de l'existant avec les exigences du Règlement vous permettra ensuite de déterminer un plan d'action sur deux ans.

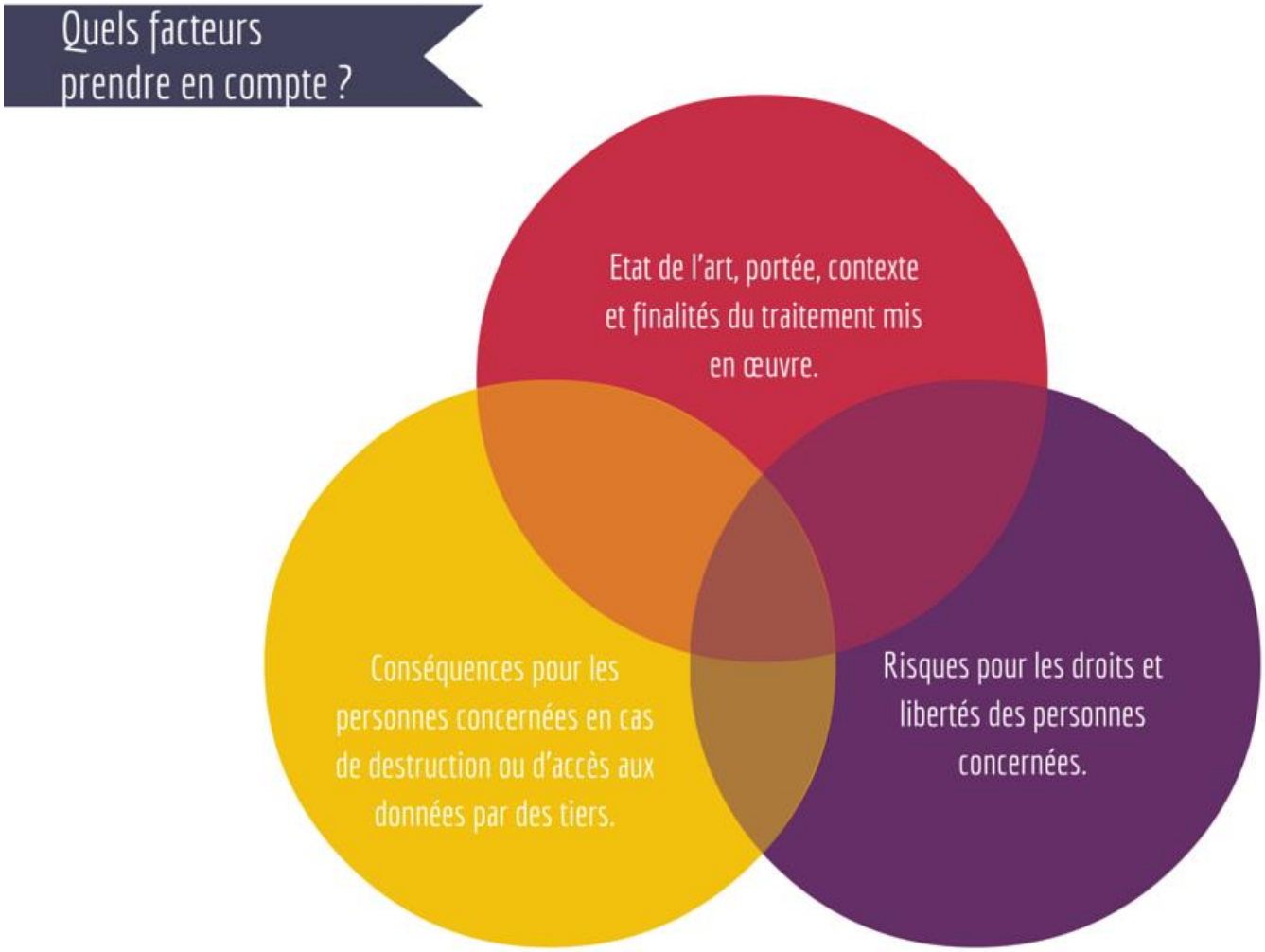
[12] Article 30 du Règlement européen

Fiche n°7 : La gestion de crise renforcée

La **sécurité des données** personnelles est depuis toujours un enjeu technique et juridique de la protection des données personnelles. **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 personnelles devra être assurée, en application du Règlement, tant par le responsable de traitement que par le sous-traitant. En effet, l'article 32 du Règlement 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 devront 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 pourront être déterminées qu'après identification des risques. Dès lors, les analyses de risques classiquement utilisées aujourd'hui demeureront un précieux outil.

Par ailleurs, le Règlement 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 devront donc être renforcés.

L'ensemble de ces mesures devra 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 personnelles, conformément au principe de responsabilité. En outre, l'exigence d'adaptation des mesures de sécurité imposera d'évaluer l'efficacité des mesures prises pour les réajuster le cas échéant.

La notification des violations de sécurité généralisée – en aval

Les responsables de traitement devront impérativement être proactifs lorsqu'il s'agira de notifier à la CNIL les violations de données à caractère personnel.

Le Règlement généralise l'obligation de notifier ces violations aujourd'hui à la charge des seuls fournisseurs de services de communication électroniques (fournisseurs d'accès à l'Internet, opérateurs de téléphonie fixe ou mobile par exemple)[13]. La violation de données à caractère personnel se définit comme la violation de sécurité entrainant la destruction, la perte, l'altération, la divulgation des données à caractère personnel traitées[14].

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 - pourra - être effectuée à partir du site de la CNIL au moyen d'un formulaire en ligne[15].

En cas de sous-traitance du traitement des données, une **collaboration avec les prestataires** est organisée par le Règlement. En effet, l'article 33 du texte[16] prévoit que le sous-traitant devra notifier au responsable de traitement toute violation dont il a connaissance dans les meilleurs délais. Dans ce contexte, le responsable de traitement devra s'enquérir auprès de ses prestataires des délais dans lesquels ils sont en capacité de lui notifier toute violation de sécurité.

Cette collaboration sera d'autant plus indispensable que la violation devra, dans certains cas, être portée à la connaissance des personnes dont les données personnelles sont traitées (pour autant que la violation génère un risque élevé pour les droits et libertés de ces personnes). Cela étant, le texte ne précise pas si cette information sera laissée à la discrétion du responsable de traitement. Néanmoins, une fois avertie, on peut penser que la CNIL, appréciant les mesures prises pour atténuer la violation de données, indiquera au responsable de traitement s'il doit ou non informer les personnes. Une procédure de notification devra être établie par le responsable de traitement afin d'être en mesure de réagir rapidement.

[13] Sources : Ordonnance du 24 août 2011 transposant l'article 2 de la directive 2009/136/CE du 25 novembre 2009, article 34bis de la loi Informatique et Libertés

[14] Article 4 du Règlement

[15] https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

[16] Article 33§2 du règlement européen

Fiche n°8 : Le DPO au cœur de la démarche de conformité

Les institutions européennes ont placé le DPO au centre de la démarche de conformité des organismes.

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

Par ailleurs, les institutions européennes ont, de par les compétences exigées du DPO et les missions qui lui seront confiées, institué un nouveau métier de la protection des données personnelles.

Une désignation quasi-systématique du DPO

Au cours des discussions sur le Règlement, 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 Règlement 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.

Notons par ailleurs que la **procédure de désignation est moins encadrée que celle qui existe aujourd'hui**. Cette souplesse se caractérise notamment par l'absence d'information des institutions représentatives du personnel.

L'engagement écrit de la personne désignée n'est par ailleurs plus exigé et les types de désignation (étendue, générale, partielle) ont été supprimés. La prise d'effet de la désignation à l'issue d'un délai d'un mois à compter de la notification à la CNIL disparait également.

Un positionnement fort du DPO

Le DPO devra directement faire rapport «*au niveau le plus élevé du responsable du traitement ou du sous-traitant*». Il devra donc pouvoir accéder aux instances décisionnaires de son organisme (comité exécutif, secrétariat général, direction générale, etc.). Preuve du positionnement fort du DPO, ce dernier **pourra avoir accès aux données à caractère personnel et aux traitements de données à caractère personnel**. Il pourra donc apprécier concrètement les conditions dans lesquelles les traitements sont mis en œuvre.

Cependant, tous les organismes ne pourront pas consacrer un poste à plein temps de DPO. Le Règlement prévoit qu'il puisse exercer d'autres missions dans l'entreprise dès lors qu'il n'est pas en situation de conflits d'intérêts.

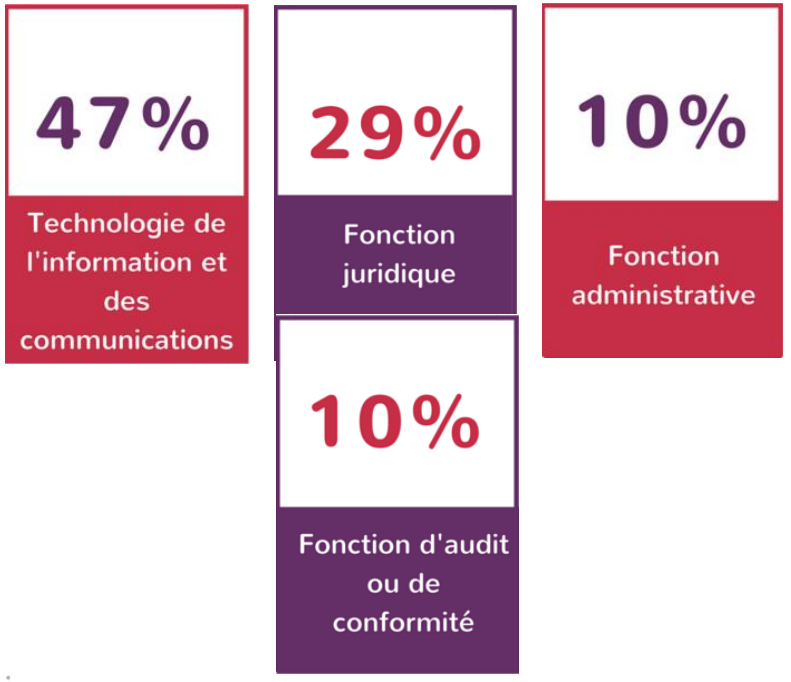
Le DPO ne bénéficiera pas du statut de salarié protégé. En revanche, le texte prévoit expressément que le DPO ne puisse pas être sanctionné en raison de l'exercice de ses missions. Cela étant, la fin de mission du DPO n'est pas encadrée par le Règlement. Faudra-t-il s'en remettre aux règles internes ? La politique de protection des données personnelles interne à chaque entreprise pourrait-elle en effet prévoir une durée pour la mission du DPO, renouvelable ou non ?

Des compétences reconnues et des missions diversifiées

Règlement européen (article 37§5)

« *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.* ».

Quel est le parcours des CIL au sein de leurs structures ? En 2015, la CNIL a réalisé une enquête pour le savoir dont voici les chiffres[17].



[17] https://www.cnil.fr/fr/cil-un-metier-davenir

Le Règlement définit le **profil du DPO** plus précisément que ne le faisait la réglementation jusque-là. Les futurs DPO devront avoir des connaissances juridiques ou se faire accompagner par son service juridique et/ou un avocat.

En interne, le DPO aura 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 devra être associé à toutes questions en matière de protection des données personnelles.

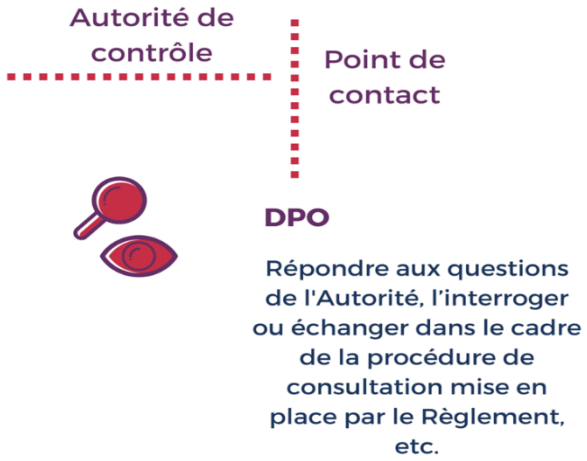
Le DPO devra également informer et conseiller les salariés dont la mission sera de traiter les données personnelles. A ce titre, le **DPO a un rôle de sensibilisation et de communication renforcé** par rapport au CIL actuel.

A cet égard, une maitrise du Règlement européen mais également des textes sectoriels impactant la protection des données personnelles est requise. Le Règlement prévoit en effet que certains domaines soient laissés à l'appréciation du droit national de chaque État membre.

Des compétences juridiques seront également mobilisées lorsqu'il s'agira de contrôler la conformité de l'organisme au regard du Règlement européen, 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 devra porter, à savoir la répartition des responsabilités (cas de la coresponsabilité de traitement ou de recours à un sous-traitant par exemple). La sensibilisation et la formation du personnel devrait également inclure les règles spécifiques applicables en matière de protection des données personnelles.

Enfin, le DPO devra vérifier que les analyses d'impact sont réalisées. Ses conseils pourront également être sollicités dans ce cadre.
Pour ce qui est des tiers à l'organisme, la **visibilité du DPO** va être renforcée par la publication de ses coordonnées à destination du public (site Internet institutionnel, site Internet marchand, documents émis par l'organisme, etc.). A ce titre, le DPO sera 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.

En dernier lieu, le DPO sera le point de contact avec l'autorité de contrôle avec laquelle il devra collaborer.



Comment préparer la désignation d'un DPO ?

Afin de préparer au mieux la désignation d'un DPO, il pourrait 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 Règlement à leur égard (fourniture de moyens, entretien des connaissances, etc.).

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

Fiche n°9 : Le renforcement des obligations des sous-traitants

L'application du Règlement européen aura 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 personnelles des manquements à la réglementation. Le sous-traitant était, de ce point de vue, à l'abri des sanctions infligées par la CNIL.

Le Règlement 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. Le Règlement 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 devra désigner un représentant au sein de l'Union par mandat écrit. Tel sera le cas si ce sous-traitant procède au traitement des données personnelles 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[18].

Le sous-traitant devra également **désigner un délégué à la protection des données personnelles**[19].

Sans qu'il s'agisse d'une nouveauté, le sous-traitant devra également **présenter des garanties 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 Règlement. Ces garanties constitueront d'ailleurs un critère de choix que les responsables de traitement devront prendre en compte[20]. Cette exigence pourra par exemple être satisfaite lorsque le sous-traitant appliquera un **code de conduite** approuvé par une autorité de contrôle. Si ce n'est le cas aujourd'hui, le responsable de traitement devra procéder à des vérifications, ne serait-ce que demander au prestataire pressenti sa **politique** en matière de protection des données personnelles.

En outre, la généralisation du registre des activités de traitement s'étend au sous-traitant. En effet, il devra **tenir un registre des traitements mis en œuvre pour le compte de responsables de traitement**[21].

[18] Considérant 80 et article 27 du Règlement européen
[19] Fiche n°8 : Le DPO au cœur de la démarche de conformité
[20] Considérant 81 et article 28§1 du Règlement européen
[21] Article 30§2b du Règlement européen

Le sous-traitant est directement **soumis à l'obligation de sécurité** prévue à l'article 32 du Règlement ainsi qu'à une obligation de collaboration tant avec l'autorité de contrôle de protection des données personnelles qu'avec le responsable de traitement[22].

Compte tenu des obligations que le sous-traitant aura à respecter, le Règlement prévoit expressément qu'il puisse être sanctionné en cas de manquement. Le montant maximal des sanctions encourues sera identique à celui encouru par le responsable de traitement[23].

Le renforcement des obligations contractuelles du sous-traitant

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

❖ *Des stipulations sur le traitement de données personnelles 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 personnelles traitées ainsi que les catégories de personnes concernées devront également figurer dans le contrat.

❖ *Des stipulations sur les missions du sous-traitant*

Le responsable de traitement devra 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 devront 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 devra également prévoir que le sous-traitant veille à ce que les personnes traitant les données (salariés, consultants

[22] Articles 28 et 31 du Règlement européen

[23] Fiche n°14 : Le caractère dissuasif des sanctions

notamment) s'engagent à respecter la confidentialité des données ou soient soumises à une telle obligation.

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

En outre, la clause relative à la protection des données personnelles devra préciser qu'une autorisation écrite préalable du responsable de traitement est nécessaire pour tout recours à un prestataire de second rang. Cette autorisation pourra être spécifique ou générale. Dans ce dernier cas, une obligation d'information pèsera sur le sous-traitant.

En sus, les obligations contractuelles que le responsable de traitement aura imposées au sous-traitant de premier rang devront être répercutées aux prestataires de second rang. Par ailleurs, le Règlement prévoit que, vis-à-vis du responsable de traitement, le sous-traitant de premier rang sera responsable de la mauvaise exécution de ses obligations par le prestataire de second rang.

Le sous-traitant sera également tenu d'une obligation contractuelle de collaboration puisqu'il devra 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 pourront être réalisés. Le sous-traitant devra par ailleurs démontrer par tout moyen qu'il respecte ses obligations (cf. Fiche n°6 : Le principe d'*accountability*).

La fin du contrat est également encadrée par le Règlement en ce qu'il prévoit que le contrat impose au sous-traitant la suppression des données personnelles ainsi que celle des copies ou la restitution intégrale des données traitées.

L'utilisation par le sous-traitant des données personnelles confiées

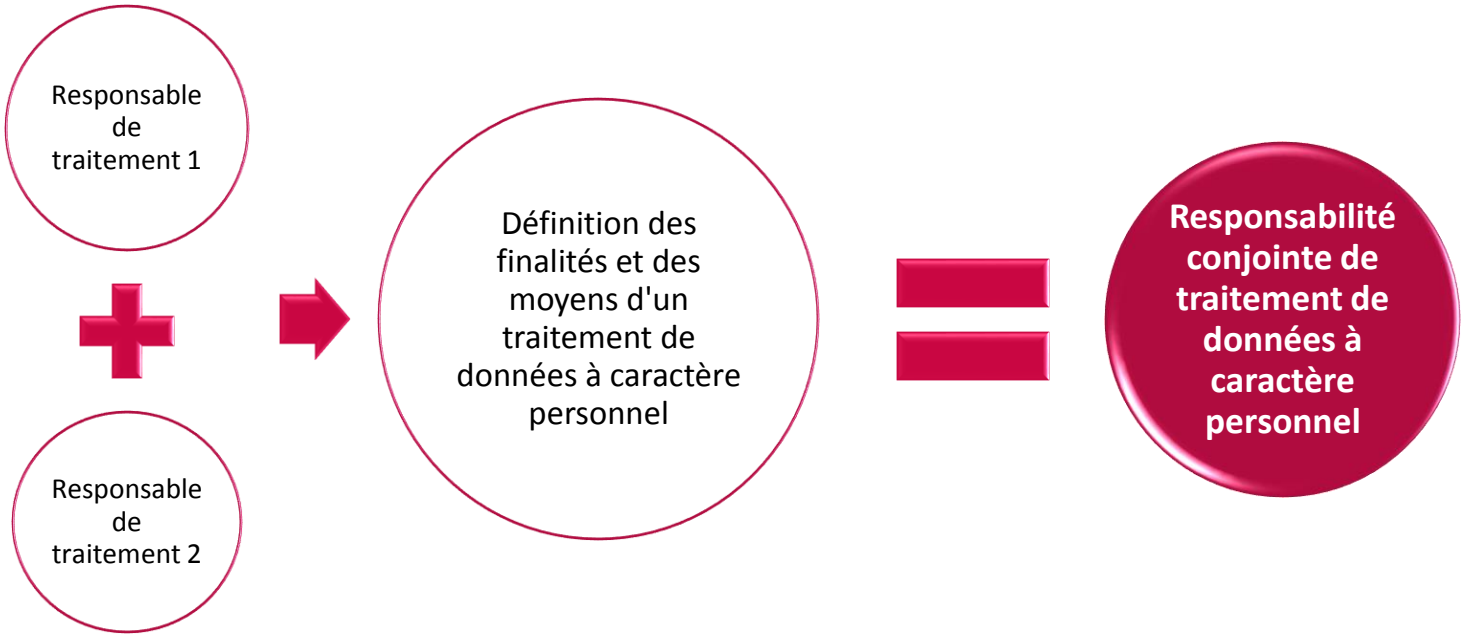
Le futur Règlement européen prévoit expressément que « *si, en violation [du Règlement] un sous-traitant détermine les finalités et les moyens du traitement de données, il est considéré comme un responsable de traitement pour ce traitement* »[24]. Cette hypothèse trouverait à s'appliquer lorsque le sous-traitant, en violation du contrat conclu avec le responsable de traitement, réutilisait les données personnelles 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 engagerait sa responsabilité vis-à-vis du responsable de traitement mais il encourrait également des sanctions pénales et administratives.

[24] Article 28§10 du Règlement européen

Fiche n°10 : La responsabilité conjointe de traitement organisée[25]

La directive 95/46/CE[26] avait pris en compte la responsabilité conjointe de traitement de données à caractère personnel. 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 personnelles 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[27]. Il convient de préciser que si le sous-traitait 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 de *cloud computing*, ni celle qui détermine la nature des données personnelles traitées ou encore la durée de conservation des données.

Le Règlement européen n'est donc pas novateur quant à la définition de la responsabilité conjointe de traitement. En revanche, il détermine le régime qui lui est applicable. Notons que le risque d'application de plusieurs lois nationales disparait, le Règlement étant applicable sur tout le territoire de l'Union européenne.

[25] Article 26 du Règlement européen
[26] Article 2, d) de la directive 95/46/CE
[27] CNIL, Cloud computing : les 7 étapes clés pour garantir la confidentialité des données, 1er juillet 2013

Un accord entre les responsables conjoints de traitement

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

La situation de responsabilité conjointe impliquera toutefois qu'ils définissent leurs **obligations respectives**. Cette répartition devra faire l'objet d'un accord entre les deux organismes, accord qui devra organiser le respect des droits des personnes et l'obligation d'information.

Une mise à disposition de l'accord

Le Règlement européen prévoit que « *les grandes lignes* » de l'accord devront 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 n°11 : 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 personnelles 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 Règlement européen (article 12). Ce principe postule que le responsable d'un traitement de données personnelles délivre aux personnes une **information concise, transparente, intelligible et dans une forme aisément accessible en utilisant un langage clair**.

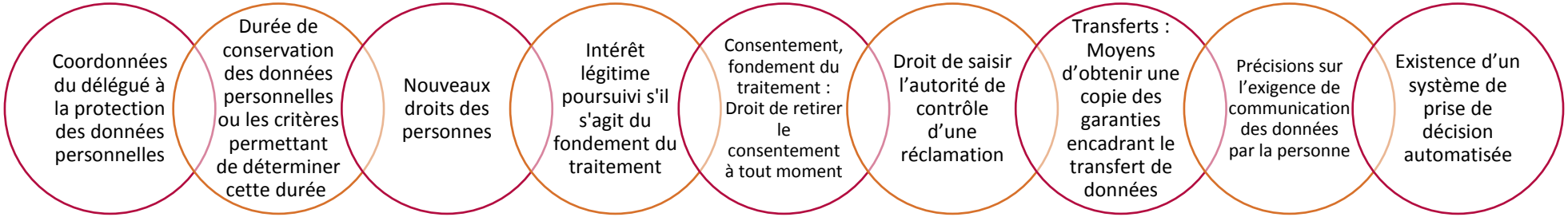
Ce principe de transparence n'est pas limité à l'information des personnes puisque qu'il impose au responsable de traitement de **faciliter l'exercice par les personnes des droits qui leur sont reconnus**. Les actions menées en vue du traitement de la demande formulée par la personne ainsi que, le cas 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 est aujourd'hui 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, devra 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 pourra 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 Règlement européen 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 directe, le responsable de traitement devra compléter son information.



Des droits nouveaux

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

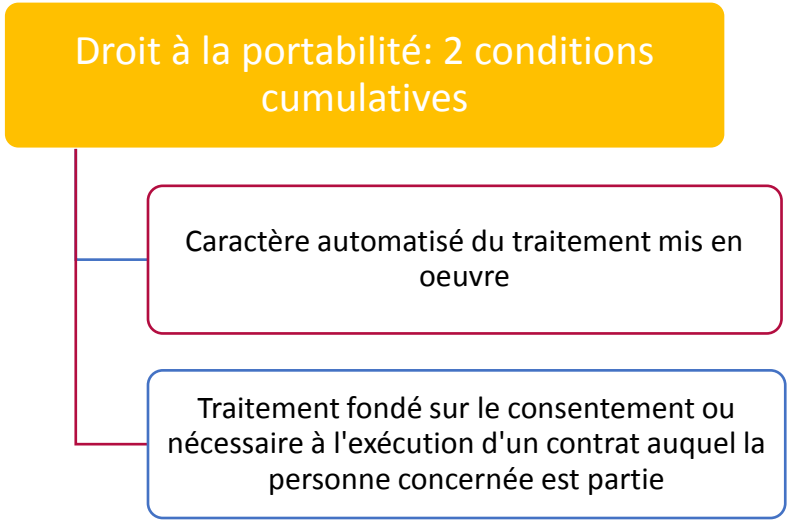
Le **droit à la portabilité des données**[28] représente sans doute l'archétype du pouvoir que les institutions ont souhaité redonner aux personnes sur leurs données personnelles.

L'exercice de ce droit permettra aux personnes de récupérer les données personnelles qu'elles ont communiquées afin de pouvoir les transférer vers un autre prestataire de services. La transmission de ces données personnelles entre deux responsables de traitement pourra également être demandée par la personne concernée.

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

Notons d'ores et déjà que le droit à la portabilité des données n'est pas sans borne comme le montre le schéma ci-après.

[28] Article 20 du Règlement européen

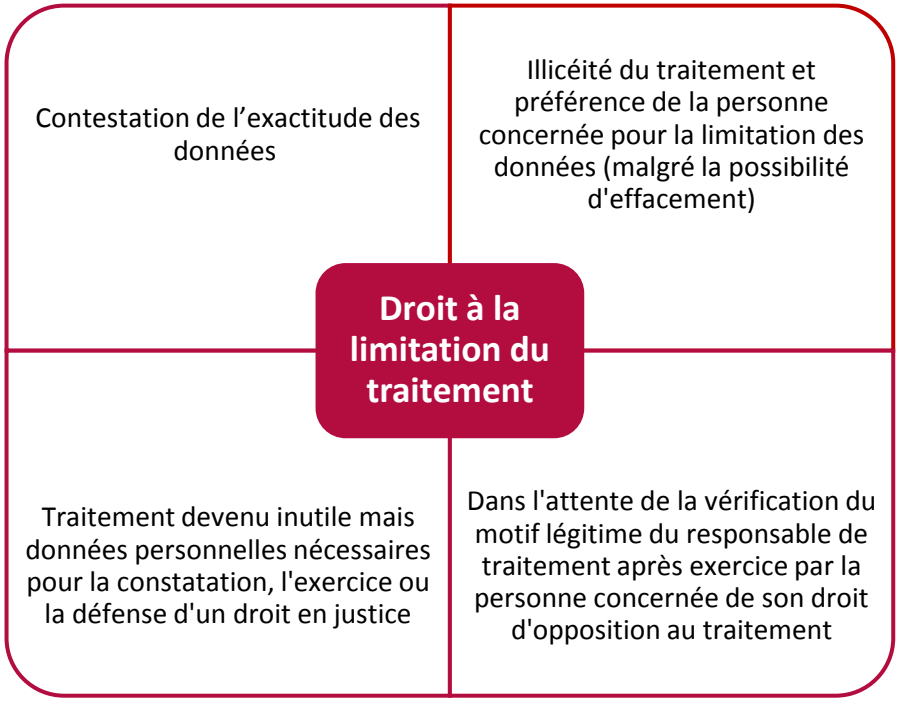


La consécration de ce droit devrait *a priori* conduire à une mise en concurrence des prestataires de services, les institutions européennes partant du postulat que les personnes se dirigeront vers les prestataires les plus engagés en matière de protection des données personnelles.

Le droit à la portabilité des données aura également **des implications d'un point de vue technique**. Le considérant 68 du Règlement 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 devront 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.

On peut également se demander si les données enrichies grâce à l'investissement et au savoir-faire de l'entreprise responsable de traitement ne devraient pas être exclues de l'assiette du droit à la portabilité des données.

Le **droit à la limitation du traitement de données à caractère personnel**[29] est également une nouveauté. Il est une illustration du pouvoir redonné par le Règlement aux personnes concernées. En pratique, le Règlement limite la portée de ce droit en ce qu'elle énumère des hypothèses dans lesquelles il pourra être exercé.



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 devront obtenir du responsable de traitement qu'il efface les données personnelles les concernant. En pratique, ce droit trouvera à s'appliquer lorsque la personne aura retiré son consentement et que ce dernier était le fondement du traitement ou encore parce que les données personnelles ne s'avèreront 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 Règlement européen. Les responsables de traitement qui auront rendu des

[29] Article 18 du Règlement européen

données à caractère personnel publiques devront 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 pourront 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 devront être modifiées pour tenir compte des nouvelles exigences européennes.

Les modalités de mise à disposition des garanties utilisées pour encadrer les éventuels transferts de données personnelles devront également être définies. En fonction de la politique que les organismes auront choisie de mettre en place, les clauses contractuelles types pourraient 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 seront rendues publiques.

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

Fiche n°12 : Les transferts de données personnelles

Les transferts de données personnelles 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 personnelles sont pour leur grande majorité reprises aux articles 44 et suivants du Règlement.

Clauses contractuelles types et BCR : deux outils confortés

Les outils de transfert existants ne sont pas remis en cause. Ainsi, **les clauses contractuelles types et les BCR pourront être utilisées sous l'empire du Règlement.** A des fins de simplification, le Règlement prévoit la suppression du mécanisme d'autorisation par la CNIL des transferts encadrés par ces outils.

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

Des contrats, *a priori* distincts des clauses contractuelles types, pourront être conclus entre des responsables de traitement ou entre responsable de traitement et sous-traitant pour encadrer les transferts. Cependant, ces contrats seront soumis au contrôle de la CNIL. Ce mécanisme de vérification existe déjà aujourd'hui chaque fois que les clauses contractuelles types de la Commission européenne sont modifiées par un responsable de traitement.

Précisons que l'autorisation de transfert obtenue de la CNIL après soumission de clauses distinctes de celles de la Commission européenne demeurera valable lorsque le Règlement sera applicable. En revanche, les modifications seront soumises aux conditions prévues dans le Règlement alors applicable.

Le responsable de traitement pourra se référer à la liste des pays établie par la CNIL sur laquelle figure le niveau de protection des données personnelles assuré par chacun d'eux[30].

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 Iles Féroé, Guernesey, Israël, l'Ile 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 serait susceptible de faire l'objet de modifications à tout moment. **Les décisions d'adéquation de la Commission européenne prises en application du Règlement européen seront 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 personnelles 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 Règlement européen à moins qu'un accord international le prévoie.

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

[30] CNIL, Transferts hors UE : Liste des pays et niveau de protection des données

Fiche n°13 : 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 personnelles, de sensibilisation du public et d'accompagnement des responsables de traitement et des sous-traitants. Ces compétences s'exerceront par principe sur le territoire de l'Etat membre dont l'autorité relève.

En revanche, la collaboration entre autorités de protection des données personnelles fait l'objet d'une organisation nouvelle, notamment en raison de l'instauration de la règle du guichet unique. Ce système sera l'un des sujets prioritaires examinés par la G29 dans les semaines à venir[31].

Le système du guichet unique

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

Pour le responsable de traitement, l'établissement principal correspondra au *« lieu de son administration centrale dans l'Union »*. Cette définition semble indiquer que l'autorité compétente sera 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 de traitement est exercé dans un autre établissement, compétence sera donnée à l'autorité de contrôle du pays dans lequel cet établissement se trouve.

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 sera celui où « *l'essentiel des activités de traitement* » est effectué. Les termes choisis sont pour le moins imprécis en ce que les activités de traitement peuvent être disséminées dans plusieurs établissements sur le territoire de l'Union. Le volume de traitement prévaudra-t-il sur la nature des traitements mis en œuvre ?

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

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

Toutefois, le Règlement européen maintiendra une compétence résiduelle des autres autorités de contrôle. En effet, chaque autorité de contrôle nationale demeurera 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 Règlement si celle-ci n'affecte que les personnes concernées dans l'Etat membre dont elle dépend.

L'autorité chef de file devra être informée de cette réclamation ou infraction au Règlement et pourra ensuite décider de gérer ou non le cas.

[31] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf

❖ *Comment les autorités de contrôle vont-elles coopérer ?*

Le Règlement organise la coopération des autorités de contrôle en ce qu'elles devront s'échanger des informations, et s'apporter une **assistance mutuelle**, voire mener des opérations conjointement (enquêtes et contrôles notamment)[32].

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 pourront également mener des audits auprès des organismes responsables de traitement et sous-traitants.

Elles pourront **adopter des mesures dites correctrices** qui consisteront par exemple à avertir un responsable de traitement de la non-conformité des traitements mis en œuvre avec le Règlement. Elles pourront en outre ordonner 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 disposeront 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 personnelles. 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 Règlement européen.

Ce Comité veillera surtout à l'application uniforme du Règlement 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 Règlement 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).

[32] Articles 56, 60 et 61 du Règlement européen

Fiche n°14: Le caractère dissuasif des sanctions

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

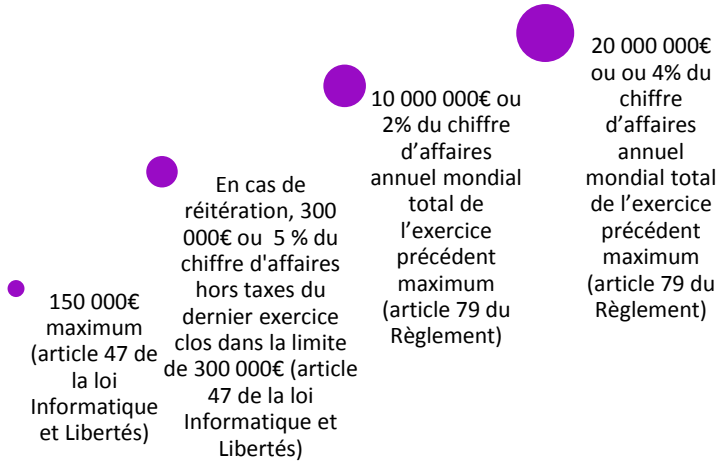
L'amende maximale de 150 000€ prononcée par la CNIL à l'égard de la société Google a été médiatisée sans pour autant contraindre le géant américain à infléchir sa politique en matière de protection des données personnelles ou dissuader les autres GAFA[33]. En témoigne la récente mise en demeure publique de la société Facebook par la CNIL en raison de nombreux manquements à la législation en vigueur[34].

C'est sans doute la raison pour laquelle les institutions européennes ont tenu à faire figurer dans le Règlement que **les amendes prononcées en cas d'infraction aux règles applicables doivent être « *effectives, proportionnées et dissuasives* »**[35].

Quels organismes seront passibles de sanction ?

En application de la réglementation française et européenne actuelles, seul le responsable de traitement encourt des sanctions administratives prononcées par la CNIL. Le sous-traitant n'a en effet pas d'autres obligations que celles fixées en matière de sécurité et de confidentialité des données personnelles dans le contrat conclu avec le responsable de traitement.

Le Règlement introduit du changement en la matière. En effet, tenu à des obligations en application du Règlement européen, le sous-traitant sera susceptible d'être sanctionné par la CNIL en cas d'infraction.



Les critères pris en compte

Le Règlement énumère une série de critères que les autorités de contrôle devront 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 pourront 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 pourront 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 personnelles, infraction aux règles applicables au consentement ou encore infractions aux dispositions relatives aux transferts de données personnelles hors de l'EEE).

[33] « La formation restreinte de la CNIL prononce une sanction pécuniaire de 150 000 € à l'encontre de la société GOOGLE Inc. » (règles de confidentialité) ou encore « Droit au déréférencement : la formation restreinte de la CNIL prononce une sanction de 100.000 € à l'encontre Google » (droit au déréférencement)

[34] https://www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi

[35] Article 83 du Règlement européen

Mathias
Avocats