L'audit de la protection des données personnelles à l'aune du Règlement Général sur la Protection des Données[1]

Sous la direction de Monsieur Jacques Vera
Directeur du master Audit et gouvernance des organisations à l'IAE Aix-Marseille

Mémoire de Msc 2 en Audit et gouvernance des organisations
Dirigé par Monsieur Jacques Vera

Nadège Rispoli

Année universitaire 2016-2017

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. Aussi appelé GDPR (General Data protection Regulation)

SOMMAIRE

REMERCIEMENTS

Avant de débuter la lecture de ce mémoire, je souhaite remercier les personnes qui ont contribué, chacune à leur manière, à la réalisation et à l'aboutissement de ce travail.

Je remercie Jacques Vera, directeur du master Audit et gouvernance des organisations, de m'avoir donné l'opportunité d'intégrer cette formation.

Je remercie Danièle Audap, directrice adjointe de l'audit interne d'Engie, pour son suivi et son implication dans la réalisation de ce mémoire.

Je remercie Jacques Perret, Correspondant Informatique et Libertés d'Engie, pour son aide précieuse. Je remercie également Leonie Marion, apprentie juriste données personnelles et Adelaide Paternoga, juriste données personnelles, de m'avoir accompagnée tout au long de la rédaction et de m'avoir permis d'enrichir mon travail.

Je remercie Philippe D'arco, manager audit interne au sein du groupe Engie, pour ses conseils et son regard expérimenté.

Je remercie, par ailleurs, toutes les personnes que j'ai pu rencontrer et avec lesquelles j'ai eu l'occasion d'échanger sur les enjeux de la protection des données personnelles et qui m'ont permis d'avoir une vision plus claire du sujet.
Ainsi je souhaite remercier Jean-David Benassouli, associé PwC Risk Assurance & Advisory Services et Alix Guiges, directrice des Opérations chez Actecil, pour leurs connaissances techniques en matière de protection des données personnelles.
Je remercie Mick Levy, directeur de l'Innovation Business chez Business&Decision et Jérôme Laval, responsable commercial chez Business&Decision, pour les réponses qu'ils ont accepté de m'apporter.

Bonne lecture !

INTRODUCTION

« La donnée est au cœur de ce monde sans couture », c'est ce qu'a soutenu Isabelle Falque-Pierrotin, présidence de la Commission Nationale de l'Informatique et des Libertés (CNIL). Cette citation illustre parfaitement la place centrale des données. Elles sont aujourd'hui à l'épicentre des enjeux de conformité rencontrés à travers le monde, un monde profondément marqué par des cyberattaques de plus en plus fréquentes, nous rappelant à quel point les données personnelles sont une denrée convoitée.

En 2013, Target, entreprise de grande distribution américaine, a été la cible d'un groupe de hackers qui lui ont dérobé les données personnelles de millions de clients. Les conséquences ont principalement été financières, de l'ordre de 250 millions de dollars. Mais plus grave encore ont été les conséquences suite au vol de données en 2015 du site Ashley Madison spécialisé dans les rencontres extraconjugales. Les hackers menaçaient de dévoiler l'identité et les données de l'ensemble des clients du site… Et l'attaque a entrainé une série d'évènements dramatiques dont 4 suicides (celui d'un pasteur ayant été confirmé) ou la démission de cadres dirigeants.
Ces intrusions démontrent bien que les données sont aujourd'hui utilisées comme moyen de pression, leur valeur résident dans leur source : l'intimité de la personne désormais monétisée. A titre d'illustration, Facebook ne peut rester un service gratuit que parce que ses revenus proviennent des données personnelles monnayées des utilisateurs.

Le Ponemon Institute, dans le cadre de ses études indépendantes, a évalué la valorisation du coût par donnée et par type d'incident. Ainsi, en 2017, le coût d'un dysfonctionnement informatique ou d'une erreur humaine représente 126 dollars par donnée compromise, celui d'une attaque malveillante, 156 dollars[2]. Et selon une étude du Boston Consulting Group datée de 2012, « The value of our digital identity », les données personnelles des européens représenteraient 330 milliards d'euros par an pour les organisations publiques ou privées.

Ainsi si les données sont aujourd'hui valorisées, elles n'en doivent pas moins être protégées puisque le principe de libre circulation des données, reconnu par la directive européenne de 1995[3], les rend vulnérables. Et leur traitement, devenant un enjeu crucial, doit être encadré. Et pourtant les entreprises ne sont pas toujours conscientes des risques que peuvent aujourd'hui encourir les données et en particulier les données personnelles. Seules 7 % des organisations considèrent que la cybersécurité est un enjeu prioritaire. Et 17% des entreprises aujourd'hui ont mis en œuvre les facteurs clés de succès d'une approche de cybersécurité[4].

[2] Ponemon Institue, 2017 Cost of Data Breach Study: Global Overview, juin 2017
[3] Directive 95/46/CE 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
[4] Deloitte, Enjeux Cyber, La face cachée de la cybersécurité, 2016

La protection des données personnelles représente pourtant un défi majeur auquel les entreprises doivent faire face et qui gagne du terrain depuis que la publication du Règlement Européen sur la Protection des Données[5] a mis en évidence de nouvelles exigences. "La protection des personnes physiques à l'égard du traitement des données à caractère personnel est un droit fondamental". C'est ce que rappelle dans son premier paragraphe le GDPR[6] publié le 4 mai 2016 et applicable à compter du 25 mai 2018.

C'est dire à quel point aujourd'hui les données personnelles intrinsèquement attachées à l'Homme doivent, du fait de cette nature particulière, faire l'objet d'une protection particulière. Ainsi il s'agira de s'interroger sur les enjeux de conformité actuels, et l'étendue de la réglementation et particulièrement sur les nouvelles obligations que le droit européen impose aux entreprises. Quels comportements, quels outils les entreprises doivent-elles mettre en place pour pouvoir répondre aux obligations nouvelles et surtout faire face aux risques attachés à la protection des données à l'aune de la nouvelle réglementation européenne ? Au-delà, comment permettre une prise de conscience plus étendue en matière de protection des données personnelles ?

Ces questions guideront la réflexion dans la rédaction de ce travail tant au travers de l'étude de la protection des données personnelles (I), que des risques attachés à celle-ci (II) et dans l'élaboration de notre guide d'audit (III). **Ce mémoire a pour but d'aider à la construction d'une démarche d'audit qui s'intéresse au diagnostic de l'existant et à la préparation de l'adaptation à une l'évolution règlementaire à venir.** Cette démarche intégrera la nouvelle règlementation, qui s'ajoute au cadre réglementaire actuellement en vigueur jusqu'en mai 2018.

Le sujet que j'ai choisi de traiter est un sujet vaste et complexe car il est en pleine évolution. Je me suis attachée à y répondre de la manière la plus complète possible tout en m'attachant à rester intelligible.

Les informations de benchmarking proviennent notamment des entreprises suivantes : Engie, Schneider Electric, Orange, La poste, Sanofi, Legrand, BNP Paribas, Société Générale, Colbert, EDF, Areva, SCOR, VINCI, SFR… Pour des raisons de confidentialité, nous ne les citerons pas directement.

[5] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, ou GDPR (General Data Protection Regulation)

[6] GDPR : General Data Protection Regulation

I. La protection des données personnelles

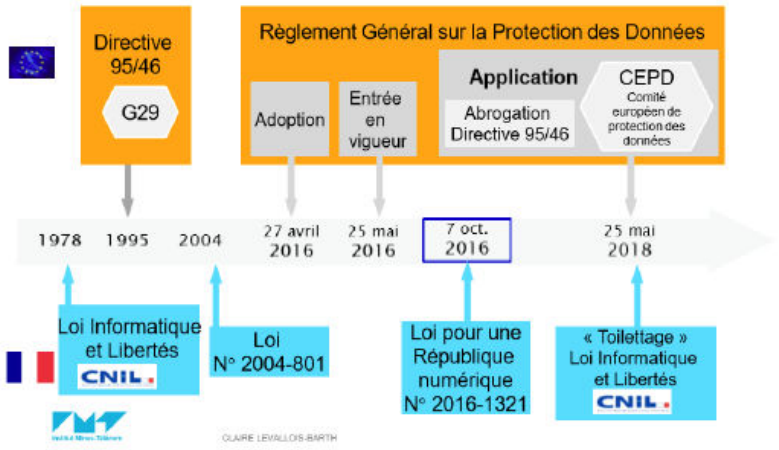
Comme évoqué dans l'introduction, le droit qui régit la protection des données personnelles est en passe de franchir une nouvelle étape avec l'application de la nouvelle réglementation européenne à partir du 25 mai 2018 (B). Mais avant de s'attarder sur celle-ci et sur les transformations qu'elle impliquera dans l'organisation des entreprises, il convient d'abord de revenir aux prémices de la protection des données afin d'en comprendre les contours (A).

A. Le développement de la protection des données personnelles

Pour comprendre le développement de la protection des données personnelles, nous nous intéresserons à l'instauration du cadre légal (1) avant de nous attacher à l'étude des enjeux sociétaux des données personnelles (2).

1. Le cadre légal de la protection des données personnelles

Pour débuter l'étude de l'environnement légal, la frise suivante permet de resituer les temps forts qui ont marqué la protection des données à caractère personnel.



Tout démarre, en France, en 1978 avec la naissance de la loi Informatique et Libertés[7].

a) La loi Informatique et Libertés ou le socle de la protection des données personnelles

La loi Informatique et Libertés est issue du projet SAFARI initié en 1973, projet d'interconnexion d'un grand nombre de fichiers administratifs, sur la base du numéro de sécurité sociale aussi appelé NIR au sein d'un « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus » ou SAFARI pour les intimes !

[7] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

C'est alors que Le Monde titra « SAFARI ou la chasse aux français »[8]. A ce moment-là, la population française est en émoi. Elle découvre rapidement les dangers de la collecte et du transfert de ses données sans encadrement. Les Français craignent, en effet, l'utilisation par les administrations de leurs données si elles les avaient entre leurs mains. En parallèle, l'informatique se développait. C'est pourquoi le législateur a souhaité poser des garde-fous puisque si le traitement des données était rendu plus facile, il convenait de s'interroger sur leur protection.

C'est ainsi que le projet contribuera à la naissance de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui dans son article 1er dispose que « l'informatique doit être au service de chaque citoyen […] » et que « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant »[9]. Au-delà, la loi garantit la maitrise du patrimoine informationnel, la sécurité des informations et elle est gage de qualité.

Pour comprendre la crainte des Français à l'époque quant au NIR ou numéro d'inscription au répertoire attribué à chaque personne physique, un rapide retour en arrière s'impose. Historiquement, le NIR date de 1941. A cette époque, pour l'application du statut des juifs en Algérie, il avait été proposé de modifier le premier chiffre d'une manière telle qu'il permettrait d'identifier les personnes au regard de leurs caractéristiques raciales : ceux relatifs au sexe seraient réservés aux européen (le 1 pour les hommes et le 2 pour les femmes), le 3 et le 4 aux indigènes musulmans, le 5 et le 6 aux juifs indigènes, le 7 et le 8 aux étrangers, le 9 et le 0 pour les statuts mal définis…

Avec la loi Informatique et Libertés de 1978, la France est ainsi apparue, après l'Allemagne en 1970, comme un précurseur puisque le droit européen viendra aussi règlementer par la suite la protection des données à caractère personnel.

(1) Champ d'application de la loi Informatique et Libertés

C'est l'article 2 de la loi qui définit son champ d'application matériel. Elle s'applique « aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers […] ».

Ainsi, pour répondre aux conditions posées par l'article, il faut être en présence :

- D'une donnée personnelle définie par l'article 2 comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres », contenue ou appelée à figurer dans un fichier ;

[8] Le monde, 21/03/1974
[9] Art 1, loi n°78-1

- D'un traitement nominatif, automatisé ou non ;
- Etre hors traitement mis en œuvre dans le cadre d'activités strictement personnelles ou à des fins de copies temporaires ;
- D'un responsable de traitement[10] situé sur le sol français ou dont les moyens de traitements sont situés sur le sol français.

S'agissant maintenant de son champ territorial, l'article 5 de la loi n°78-17 pose deux critères d'application :

- Le critère de l'établissement sur le territoire français du responsable de traitement ;
- Le critère du recours aux moyens de traitement situés sur le territoire français.

Ainsi, trois hypothèses sont à distinguer :

- Lorsque le responsable de traitement est établi sur le territoire français, la loi n°78-17 s'applique, que des moyens soient utilisés ou non sur le territoire ;
- Lorsque le responsable de traitement n'est pas établi sur le territoire français, mais sur celui d'un Etat membre de l'UE, la loi ne s'applique pas, que le moyen de traitement soit situé sur le territoire français ou pas ;
- Enfin, lorsque le responsable de traitement n'est pas établi en France, ni dans un Etat-membre de l'UE, si les moyens de traitement sont situés sur le territoire français, la loi s'applique. En revanche, si les moyens de traitement ne sont pas situés sur le territoire français, elle ne s'applique pas.

	Moyens de traitement situés sur le territoire français	Aucun moyen de traitement situé sur le territoire français
Responsable de traitement établi en France	oui	oui
Responsable de traitement non établi sur le territoire d'un pays de l'UE, hors France	non	non
Responsable de traitement non établi sur le territoire français mais sur celui d'un pays de l'UE	oui	non

Ne sont donc pas concernés, les traitements dont le responsable de traitement est établi dans l'un des pays de l'UE, même si des moyens de traitements sont utilisés en France. Le champs territorial de la loi de 1978 apparait donc limité dès lors que le responsable de traitement se trouve sur un état de l'UE…

[10] Loi n°78-17, Art. 3 « Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens »

(2) Les droits et obligations

La loi Informatique et Libertés reconnait un certain nombre de droits aux personnes concernées par le traitement des données.

Le droit d'accès aux données : Le droit d'accès se définit comme la possibilité pour toute personne concernée[11] qui justifie de son identité d'avoir accès aux informations qui la concernent et d'interroger l'entreprise au sujet du traitement réalisé sur ses données personnelles.

En 2011, Max Schrems, étudiant autrichien, s'est adressé à Facebook afin d'obtenir communication de l'ensemble de ses données détenus par ce dernier. Il a ainsi reçu, quelques semaines plus tard, communication de 1 222 pages en format PDF. Choqué par le volume d'informations conservées (qui comprenaient également des données qu'il avait pu effacer dans le passé), il a décidé de porter plainte et il a créé une association nommée *europe-v-Facebook* qui rassemble aujourd'hui plus de 25 000 plaignants.

Le droit de rectification : Il s'agit de la possibilité pour toute personne concernée d'obtenir une rectification de ses données personnelles quand elles sont erronées ou obsolètes.
Ainsi, toute personne physique justifiant de son identité peut exiger du responsable de traitement que soient :

- Mises à jour les données à caractère personnel la concernant, qui sont « inexactes, incomplètes, équivoques, périmées » ;
- Verrouillées ou effacées les données dont « la collecte, l'utilisation, la communication ou la conservation est illégale », au sens de l'article 40 de la loi de 1978.

L'entreprise est même tenue de procéder d'office à la rectification d'informations dont elle connaitrait l'inexactitude. Il pourrait s'agir par exemple d'un changement d'adresse de livraison sur un site marchand, ou d'un changement de nom demandé au service des Ressources Humaines.

Le droit d'opposition : Toute personne physique a le droit de s'opposer, en amont de la collecte et par la suite au traitement, pour des motifs légitimes, à ce qu'elle figure dans un fichier, sauf si le traitement répond à une obligation légale (ex : déclaration d'accident des salariés) ou si la disposition expresse d'une autorité autorise le traitement (ex : services fiscaux, traitement autorisé par la CNIL, etc.). Le droit d'opposition n'est pas absolu sauf pour l'opposition à la prospection. Le motif de la demande d'opposition doit être indiqué par tout demandeur. Son caractère légitime est apprécié librement par le responsable de traitements, et ce en tenant compte de la situation particulière de chaque personne.

[11] Loi n°78-17, Art. 3 « La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement »

Mais la loi reconnait également un certain nombre de principes et impose des obligations au responsable de traitement.

Le respect du principe de licéité en matière de collecte des données : Au titre de l'article 6 de la loi, les données sont collectées de manière loyale c'est-à-dire que la personne concernée doit être consciente que ses données font l'objet d'une collecte et doit pouvoir s'y opposer. Elles sont collectées de manière licite, les moyens mis en œuvre pour collecter les informations devant être légaux.
Par ailleurs, tout traitement doit avoir un objectif précis prédéterminé : la finalité est le but à atteindre justifiant la collecte des données. Les données collectées et manipulées doivent être justifiées au regard de cet objectif et ne pas être réutilisées ensuite d'une manière qui serait contraire à celui-ci.

Ces principes se traduisent par l'obligation :

- De recueillir le consentement de la personne concernée avant tout traitement de ses données personnelles sauf exceptions[12]. Et sauf exception également, notamment si la personne a donné son consentement exprès, le traitement des données sensibles[13] est interdit ;
- D'informer la personne de l'objectif de la collecte, de l'identité du responsable de traitement, du caractère obligatoire ou non des réponses, des droits qui lui sont reconnus[14] ;
- De conserver les données pendant une durée limitée fixée par le responsable de traitement à défaut d'obligation légale.

Une obligation de sécurité : Le responsable de traitement doit garantir la disponibilité, l'authenticité, l'intégrité et la confidentialité des données contre toute atteinte accidentelle (désastres naturels, incidents techniques, etc.) ou volontaire. Il doit ainsi prendre « toutes précautions utiles afin de préserver la sécurité des informations »[15].

Après le législateur français, l'Union Européenne a elle aussi élaboré des textes relatifs à la protection des données personnelles.

[12] Le consentement est défini comme « toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement » (Article 2, Directive européenne n° 95/46/CE du 24 octobre 1995). Pour les exceptions, voir l'annexe n°1.
[13] Art 8.1 de la loi 78-17 I. « Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. ». On les retrouve en particulier dans le domaine RH. Pour les exceptions, voir annexe n°1
[14] Loi 78-17, Art 32
[15] Loi 78-17, Art 34

b) Le développement du droit européen

Le 24 octobre 1995, le Parlement européen et le Conseil adoptent la directive 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[16].

Et c'est avec quelques années de retard, que la France, en 2004, transposa la directive européenne modifiant ainsi la loi de 1978 par la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel du 6 août 2004[17].

La loi française inspira fortement le législateur européen qui a repris de nombreux principes déjà inscrits dans la loi Informatique et Libertés. En effet, mis à part quelques éléments de précision s'agissant notamment des définitions de donnée à caractère personnel et de traitement, la directive n'entrainera pas d'importantes modifications.

Elle apporte davantage un cadre aux entreprises en vue d'harmoniser les législations en posant les grands principes de la protection des données, à charge pour les états de les introduire dans leur droit. Le champ d'application reste le même, et la directive s'applique dès lors que le responsable de traitement se trouve dans l'UE ou en dehors si des moyens de traitements y sont situés.

Puis, le législateur européen a souhaité renforcer la protection des données. Et c'est ainsi que l'on aboutit à la règlementation européenne, le GDPR, adopté le 27 avril 2016, qui deviendra applicable le 25 mai 2018. A cette date, toutes les entreprises qui collectent, traitent, stockent des données personnelles devront se conformer à cette nouvelle réglementation. C'est ce que nous développerons un peu plus loin.

En pratique, la nouvelle réglementation n'entrainera pas la disparition de la loi Informatique et Libertés, seule la directive sera abrogée. Si le GDPR, d'application immédiate, entraine sa nécessaire mise à jour, la législation nationale ne sera pas supprimée ni effacée. En effet, le règlement encadre le traitement et la manipulation des données mais laisse cependant beaucoup de champ d'action et de liberté de manœuvre aux états membres.

Et avec le développement des enjeux liés aux données personnelles, des acteurs en charge de leur protection ont vu le jour.

---

[16] Directive 95/46/CE 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

[17] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

c) Les acteurs majeurs de la protection des données personnelles à la maille France

Les acteurs ayant un rôle à jouer en matière de protection des données personnelles sont nombreux dans l'entreprise. Mais deux acteurs se détachent puisque leur fonction même est d'être garant de cette protection. Il s'agit de la CNIL (1) et du Correspondant Informatique et Libertés (2).

(1) La CNIL, un acteur incontournable

Pour avoir une vision compète de la place de la CNIL au sein de la protection des données personnelles, nous nous attacherons dans un premier temps à étudier sa composition, et son organisation (a), avant de nous intéresser à ses missions et à son rôle qui ne cesse de se renforcer (b), pour terminer par un aperçu de ses moyens de contrôle (c).

(a) Sa composition, son organisation

La création de la Commission Nationale de l'Informatique et des Libertés ou CNIL est issue de la loi de 1978. C'est alors la mise en place d'une Autorité Administrative Indépendante française.

La CNIL doit sa légitimité à son indépendance puisque ses membres, au nombre 18, ne reçoivent aucune instruction. Ils sont appelés « commissaires » et sont tous issus de fonctions très différentes : ils sont hauts magistrats, parlementaires, conseillers économiques sociaux et environnement ou « simplement » qualifiés. Les commissaires sont élus pour 5 ans ou s'agissant des parlementaires pour une durée égale à leur mandat électif.

La CNIL est ainsi composée de 5 personnalités qualifiées pour leur connaissance du numérique ou des questions touchant aux libertés individuelles, 3 étant nommés par décret et les 2 autres par le président de l'Assemblée Nationale et par le président du Sénat. L'idée est ainsi d'avoir une représentation en termes technologiques.

(b) Son rôle, ses missions

Les missions principales attribuées à la CNIL peuvent se regrouper en 4 catégories :

- Elle a une obligation d'information et de protection. Elle est chargée de garantir le droit d'accès des personnes, le droit d'accès indirect aux traitements intéressant la

sureté de l'état, d'instruire les plaintes, de recenser les traitements déclarés, le registre ou fichier des traitements ;
- La CNIL accompagne, et conseille les autorités, les professionnels et le grand public,
- Elle contrôle les fichiers et la mise en œuvre des traitements, elle règlemente et dispose d'un pouvoir de sanction ;
- Enfin, elle doit anticiper la protection des données en se tenant informée sur l'évolution des technologies.

Et depuis 2016, la loi dite pour une République Numérique[18], mettant à jour la loi Informatique et Libertés en modifiant les sanctions et en créant de nouveaux droits, a confié de nouvelles missions à la CNIL :

- La CNIL est désormais en mesure de délivrer des certifications et des labels pour des procédures relatives à la protection des données personnelles et de publier des référentiels ou des méthodologies générales ;
- De s'interroger sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques ;
- De promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données ;
- De saisir pour avis l'Autorité de Régulation des Communications Electroniques et des Postes ou ARCEP[19] de toute question relevant de la compétence de celle-ci.

Elle est par ailleurs investie d'une mission d'information et de sensibilisation du grand public sur les droits qui leurs sont reconnus. Ainsi la CNIL au travers de différents canaux comme les réseaux sociaux, la presse ou son site web, mène des actions de communication et propose des outils pédagogiques.

(c) Ses contrôles

La CNIL a vu son pouvoir de contrôle étendu depuis l'entrée en vigueur de la loi du 6 Août 2004. En effet, la loi lui a accordé un rôle a posteriori bien plus important.
Son pouvoir en matière de contrôle sur place est renforcé et elle est désormais dotée d'un pouvoir de sanction. Et selon son appréciation, les sanctions financières, qu'elle sera en mesure de prononcer pourront s'élever jusqu'à 3 millions d'euros.
Depuis la loi du 17 mars 2014, elle est également autorisée à mener des contrôles en ligne en plus des contrôles sur pièces ou sur convocation dont elle pouvait déjà user.

Et la nouvelle réglementation européenne va encore renforcer ce pouvoir de sanction…

[18] LOI n°2016-1321 du 7 octobre 2016 dite Loi pour une République Numérique
[19] ARCEP : Autorité administrative indépendante en charge de la régulation des communications électroniques et des activités postales en France

(2) Le Correspondant Informatique et Libertés

Le correspondant Informatique et Libertés ou CIL est l'une des innovations majeures de la loi du 6 aout 2004 qui a refondu la loi informatique et Libertés[20].
Son rôle est de proposer aux responsables de traitements un moyen efficace pour assurer le respect de la règlementation.
Le CIL est chargé d'assurer d'une manière indépendante le respect des obligations prévues dans la loi et de tenir un registre des traitements. Il mène une mission de conseil quant à la mise en œuvre des traitements ainsi qu'une mission de médiation puisqu'il est tenu de recueillir les réclamations des personnes concernées. Il informe, par ailleurs, le responsable de traitement lorsqu'il constate un manquement et ce dernier doit l'aider à y remédier.

La conduite des missions en toute indépendance conditionne l'efficacité du dispositif. Le CIL bénéficie d'un régime protecteur.

- Il exerce sa mission directement auprès du responsable de traitement ;
- Il ne reçoit aucune instruction pour l'exercice de sa mission ;
- Les fonctions ou activités qu'il exerce concurremment ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission ;
- Il n'y a pas de transfert de responsabilité sur le CIL qui ne peut être sanctionné du fait de l'accomplissement de ses missions : il n'engage que sa responsabilité de droit commun pour manquements graves constatés et qui lui sont directement imputables.

Outre un allègement des formalités préalables de déclaration, sa désignation présente des avantages certains pour l'entreprise. L'existence d'un CIL permet de :

- Faciliter les démarches avec la CNIL ;
- Le développement de l'informatique en limitant le danger pour les droits des usagers, des clients et des salariés ;
- D'accompagner et de garantir le responsable de traitement de nombreux risques vis-à-vis de l'application du droit en vigueur.

Ainsi, le CIL apparait comme un personnage-clé dans le paysage de la protection des données personnelles. Il est « un outil » de preuve de respect et d'engagement en matière de protection des données qui contribue à la diffusion d'une culture « protection des données » au sein de l'entreprise.

[20] Art. 22 III de la loi n°78-17

2. Les données personnelles : or noir du XXIème siècle ?

Les données personnelles sont aujourd'hui valorisées mais pour pouvoir approfondir la portée de cette valeur (b), il convient d'étudier les contours de la notion de donnée à caractère personnel (a).

a) L'étendue de la notion de donnée à caractère personnel

Pour pouvoir parler de donnée à caractère personnel, la donnée en question doit se rapporter à une personne identifiée ou identifiable. En effet, l'article 2 de la loi Informatique et Libertés modifiée en 2004 prévoit que « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne».

Une donnée est personnelle quand elle concerne :

- **Une personne physique**. Les données relatives à une société ne sont pas personnelles ;
- **Une personne identifiée ou identifiable**. Une information peut être suffisante à identifier une personne. A l'inverse, le caractère identifiable est caractérisé lorsque « même sans avoir encore été identifiée, il est possible de le faire » au sens de la directive[21]. Dans ce cas, c'est un faisceau d'indices qui permettra de la distinguer ;
- **Directement ou indirectement**. L'information peut identifier clairement la personne ou ses goûts ou habitudes ;
- **Par un numéro ou un élément qui lui est propre**. Est un numéro d'identification le NIR, le numéro de CB, etc. Il est à noter que les éléments permettant l'identification sont évolutifs, le développement des nouvelles technologies rendant les individus toujours plus « transparents ».

Mais la difficulté réside dans l'appréciation de cette possibilité d'identification. Dans les faits, cette possibilité dépendra des moyens à la disposition du responsable de traitement. La détermination relève donc de la casuistique étant donné que ce seront les circonstances d'espèce qui permettront de déterminer si une personne est identifiable ou si elle ne l'est pas. La Commission européenne[22] a permis de préciser le niveau d'identification attendu. Selon cette dernière, un individu peut être identifié directement ou indirectement « par un numéro

[21] Directive 95/46/CE, Art 13

[22] Institution de l'Union européenne qui représente et défend les intérêts de l'Union

de téléphone, de voiture, de sécurité sociale, de passeport ou par un croisement de critères significatifs permettant de le reconnaître à l'intérieur d'un petit groupe par exemple »[23].

> Ainsi, selon la Commission, le nom permet de rendre une personne directement identifiée ou identifiable. Mais parfois l'identification requiert la combinaison de plusieurs éléments, c'est le cas lorsque le nom n'apparait pas suffisant[24]. C'est alors son association à des données comme l'âge ou la profession qui permet cette identification. Les données deviennent ainsi personnelles si les informations permettent d'identifier la personne et de connaitre ses goûts, ses habitudes. Ainsi dans le cadre d'une enquête anonyme, c'est finalement l'ampleur de l'enquête (géographique, nombre de personnes interrogée…) qui permettra d'identifier ou de rendre identifiable une personne.

Finalement, la définition de la loi n'impose pas « un haut degré d'identification »[25], ce qui par conséquent oblige les juristes et les CIL à étudier chaque donnée avant de pouvoir déterminer si elle permet d'identifier la personne concernée.

Nous verrons que le règlement viendra encore préciser la notion de personne identifiable.

La définition de la catégorie des données personnelles permet d'y faire rentrer un nombre important d'informations, c'est pourquoi il apparait plus judicieux de faire l'étude des informations exclues de cette catégorie ce qui permettrait de la rendre plus homogène[26]. Or, dès lors qu'une information peut être classée dans cette catégorie, elle fait l'objet d'une protection particulière et cette question soulève de nombreuses interrogations face aux enjeux du big data particulièrement.

Ainsi, une fois la donnée personnelle caractérisée, qu'en est-il de la protection des droits de la personne concernée ?

b) Données personnelles et protection des droits des personnes

L'exploitation des données est indispensable mais surtout c'est la connaissance du client qui devient essentielle au modèle économique (1). Or, une limitation de l'exploitation des données risquerait d'entrer en conflit avec la créativité et le développement empêchant la valorisation des données. Il s'agira ici de voir comment associer cette utilisation des données avec le respect de la vie privée (2).

---

[23] COM(92) 422 final SYN 287, 15.10.1992, p.10, cité par l'avis 4/2007 du Groupe de travail « article 29 » à la Commission sur le concept de donnée à caractère personnel

[24] Cas d'exploitation d'un fichier afin de déterminer le nombre de personnes ayant le même patronyme et leur répartition sur le territoire. Le juge décida le nom n'est pas une donnée personnelle.

[25] EYNARD J., *Les données personnelles, quelle définition pour un régime de protection efficace ?*, Michalon, 2013, p. 45

[26] EYNARD J., ouvr. cité., p. 46

(1) Connaissance client et big data

Les dernières dizaines d'années ont été marquées par des **enjeux nouveaux face à l'explosion du volume de données issues de nos actions informatiques quotidiennes**.

Alors que la réglementation européenne est en passe d'évoluer, un sujet intéresse particulièrement les entreprises et les autorités : le Big Data, aussi appelé données massives. Il se définit comme un ensemble de « données structurées ou non dont le très grand volume requiert des outils d'analyse adaptés ». Le Big data représente une nouvelle terre de conquête et de développement pour les entreprises de sorte que certains parlent aujoud'hui d' « or noir du 21ème siècle » pour qualifier les données personnelles.

Dès lors que le big data vise généralement à collecter des données en vue de les traiter pour des finalités ultérieures, il nécessite une protection renforcée. Et, à ce titre, la loi Informatique et Libertés ainsi que la directive de 1995 imposent que les données « ne soient pas traitées ultérieurement de manière incompatible » avec les finalités pour lesquelles elles ont été collectées.

Avec le développement du numérique, le consommateur se sent libéré puisqu'il peut agir sur différents canaux pour se renseigner, comparer ou affiner son choix avant de consommer. Il a désormais un parcours aux multiples facettes : comparateurs en ligne, e-boutique, forums d'avis… et laisse de nombreuses traces... C'est ce qui permet à l'entreprise de développer le *data-driven marketing, ou* « marketing éclairé par les données »[27]. Dans le cadre d'une mission d'audit, cette fonction sera particulièrement intéressante à auditer.

[27] FAILLET C., « Le data-driven marketing, qu'est-ce que c'est ? », l'Observatoire Influencia, novembre 2015

Ce concept donne les moyens au travers des données de bien connaitre sa cible et de la tracer pour mieux la servir[28].

> En juin 2015, la Harvard Business Revue citait « oubliez tout ce que vous avez appris sur le marketing ! ». Car le *data-driven*, qui permet de structurer les données pour mieux comprendre les comportements des clients, représente un intérêt stratégique pour l'entreprise sur le plan concurrentiel.

Et pour connaitre son client, la constitution et la maitrise de fichiers clients, aujourd'hui assimilés aux bases de données, sont un avantage certain dans le développement de l'entreprise. Construire une base de données clients s'avère indispensable avant toute activité de prospection afin de s'assurer des ventes croissantes et d'asseoir la fidélisation client. Mais pour ne pas que « trop d'informations tue l'information », il convient de structurer les informations en fonction de l'utilisation que l'entreprise souhaite en faire.

A partir de ces bases de données, les entreprises développent des outils de marketing direct qui soulèvent des interrogations quant à la protection des données. Le développement du e-commerce a été suivi par des actes de prospection[29] toujours plus nombreux. L'idée derrière cet usage est d'abord de mieux connaitre le client et également de transformer ce premier contact en acte d'achat. Ainsi, si les entreprises ont compris l'intérêt de tels fichiers, la loi Informatique et Libertés encadre cette collecte d'informations.

La loi de 1978 prévoit qu'en cas de prospection, notamment commerciale, le motif est présumé légitime et ne nécessite alors aucune justification c'est-à-dire que si le responsable de traitement estime pouvoir invoquer des raisons légitimes, il était alors tenu d'en apporter la preuve. Par ailleurs, et avec le nouveau règlement, lorsqu'un traitement est utilisé à des fins de prospection, la personne pourra exercer son droit d'opposition à l'encontre du profilage[30] lié à cette prospection. Ainsi les activités de profilage seront désormais traitées et définies par le GDPR, ce qui apparait essentiel dans la mesure ou la majorité des informations disponibles sur internet est issue d'une traçabilité de la navigation.

Aujourd'hui, le volume de donnée permet aux entreprises de repousser leurs limites en matière de ciblage…[31]. L'entreprise dispose de moyens de plus en plus étendus lui permettant de connaitre ses clients, dans un contexte économique tendu. Les outils et moyens technologiques se multipliant, ils doivent être sélectionnés et utilisés avec prudence pour

---

[28] Ibid.

[29] Prospection = Action de recherche de la clientèle par différents moyens

[30] GDPR, Art 4 « Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »

[31] VALLEE M., « Une éthique des données personnelles doit être le fondement du marketing « data driven », Les Echos, avril 2016

miser sur des informations de qualité. Dans le cadre d'une mission d'audit, ces méthodes seront particulièrement intéressantes à auditer.

La prospection peut ainsi revêtir des formes très variées : papier, fax, appels téléphoniques ou courriers électroniques (mails, SMS, MMS…).

> L'e-mailing qui consiste à envoyer des mails en masse à un nombre important de destinataires est une pratique couramment employée. Ce procédé est souvent décrié lorsqu'il est utilisé à outrance. Pour être utilisé comme un canal privilégié, il doit être employé avec prudence. Selon Directinet, spécialiste de l'emailing, 80 à 90 % des ouvertures suite à un mail est réalisé par 5 à 10% des destinataires. Il convient donc pour l'utilisation de cet outil de la rigueur en privilégiant dans un premier temps la qualité du message pour avoir plus de visibilité sur les destinataires réceptifs. Ce qui donnera à l'entreprise le « feu vert » pour davantage solliciter ce « futur » client.
>
> En réalité, si l'attachement des consommateurs français aux e-mails est réel, leurs habitudes vis-à-vis du digital évoluent. Ils s'ouvrent davantage aux autres canaux de communication et intègrent les réseaux sociaux dans leur réflexion obligeant les entreprises à se tenir informées des usages en matière de marketing digital. Et aujourd'hui les méthodes de marketing direct[32] ne cessent de se diversifier.

Ainsi, si on peut parfois croire à une coïncidence et penser que notre ordinateur nous comprend mieux que quiconque, ce n'est, en réalité, pas vraiment le fruit du hasard. Car ce que recherchent aujourd'hui les entreprises c'est faire de la publicité un outil efficace et par conséquent personnalisé.

> La publicité ciblée consiste pour une entreprise à utiliser notre profil obtenu par des activités de profilage afin de pouvoir nous proposer des offres conformes à nos envies, nos goûts. Les profils sont constitués à partir de nos requêtes dans les moteurs de recherche, de notre navigation, de nos clics sur bannières… toutes ces informations sont analysées. Le data Mining permet notamment par une exploration automatique de rendre une donnée personnelle utile une fois croisée avec d'autres, ce qui permet de découvrir des corrélations ou des typologies complexes. Cette solution permet de pouvoir anticiper sur les besoins du consommateur en lui proposant, au moment le plus opportun, des produits ou services correspondant à des nécessités futures.
>
> C'est cette publicité ciblée qui permet aux moteurs de recherche ou aux réseaux sociaux de nous offrir des services gratuits. C'est ainsi que nos informations personnelles peuvent être revendues à d'autres sociétés à prix d'or. Le Boston Consulting Group a estimé que ces données collectées via le marketing ciblé ou les programmes fidélité

[32] Marketing direct = Démarche commerciale d'approche du client ou prospect sans intermédiaire et à distance

valaient, en 2011, 315 milliards d'euros[33]. C'est pourquoi les réseaux sociaux, forums de discussions… deviennent des canaux intéressants et souvent riches d'expériences.

L'article 32 de la loi de 1978 modifiée par l'ordonnance du 24 aout 2011[34] transposant la directive 2009/136/CE dite « Paquet Telecom » pose le principe selon lequel pour pouvoir tracer une personne, cette dernière doit avoir donné son consentement.
Par l'option « opt-in », le prospecteur doit, en amont de tout envoi interroger le particulier sur sa volonté de recevoir de la publicité.
Selon l'option « opt-out », l'autorisation de la personne est considérée comme accordée de manière implicite. Cette option permet à cette personne *a posteriori* de s'opposer à recevoir des publicités futures par un moyen que le prospecteur aura choisi. Il peut s'agir d'un lien sur lequel cliquer ou encore d'une messagerie électronique. Cependant, si le consentement préalable est obligatoire en B to C, il ne l'est pas en B to B[35].

Au-delà, de nouvelles activités captant et partageant de l'information se développent, et se retrouvent au centre des préoccupations attachées au big data.

Ils régulent la température, deviennent des coachs sportifs, derrière les objets connectés qui nous facilitent la vie, se cache des technologies permettant de grandes exploitations de données personnelles. Des capteurs placés sur des objets du quotidien permettent au concepteur de l'application de récolter de nombreuses données relatives aux habitudes d'un consommateur pour se démarquer de la concurrence. Ces technologies poussent à l'extrême cette connaissance du client en le suivant dans ses faits et gestes. Et le risque en termes de protection des données personnelles est élevé puisque les informations collectées deviennent personnelles à partir du moment où l'objet peut explicitement être associé à son utilisateur. N'atteint-on pas ici les limites de la protection des données ? A quand les lentilles de contact qui permettront de surveiller voire d'enregistrer notre vie quotidienne ?

La loi de 1978 apporte des garanties en prévoyant la loyauté de la collecte des données, notamment via des objets connectés, collecte qui doit être proportionné à l'objectif poursuivi. Et si des règlementations en vigueur existent déjà pour ce sujet, le GDPR constitue un tournant puisque la notion de confidentialité des données, dans le cadre du règlement, est très large et implique la mise en place de nouvelles obligations que nous étudierons.

[33] Fiche d'information de la Commission d'Accès à l'Information du Québec, « Le profilage et la publicité ciblée », octobre 2013
[34] Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques
[35] B to C = vente aux particuliers ; B to B = ventes à des professionnels

(2) Connaissance client, éthique et protection de la vie privée

Le big data permet aujourd'hui de caractériser les données par les « 3V »[36] : Volume qui correspond à la masse de données, Variété car les données collectées sont très diverses et Vélocité qui fait référence au traitement en temps réel. Mais selon certains, comme Mouloud Dey, directeur des solutions émergentes chez SAS France, un 4ème V manque à cette suite aujourd'hui ; celui correspondant au terme Valeur. En effet, si les données ont longtemps été à l'abandon, elles reviennent aujourd'hui sur le devant de la scène et représentent un levier de croissance. Mais encore faut-il que ce levier soit maitrisé et c'est la toute la difficulté puisque comme le rappelle Mike Gualtieri, expert à l'institut d'étude Forrester, le traitement des données nécessite « d'agir efficacement, de prendre des décisions, de réduire les risques potentiels et, surtout, de toujours servir au mieux les consommateurs ».

Il est vrai que l'enjeu de la collecte et de l'externalisation des données personnelles est associé à deux problématiques : la protection de la vie privée et la sécurisation de la ressource. Et si les entreprises doivent repenser leurs business models, le législateur prend aussi en compte le big data puisque que cette collecte massive de données posent des questions relatives aux droits et libertés des personnes concernées notamment en ce qui concerne la surveillance électronique utilisé par l'employeur et le profilage.

Issu de la loi du 17 juillet 1970, le droit au respect de la vie privée est intégré dans le code civil à l'article 9 qui dispose que « chacun a droit au respect de sa vie privée ». Déjà en 1948, l'article 12 de la déclaration des droits de l'homme puis la Convention Européenne des Droits de l'Homme en 1950, consacraient le droit au respect de la vie privée.
Mais les contours de la notion ont bien évolué depuis. Aujourd'hui la sphère de l'espace privée se réduit drastiquement avec le développement des technologies de l'information permettant aux entreprises de « suivre » les individus. De sorte que le respect de la vie privée inquiète les internautes qui estiment dans 70% des cas n'avoir qu'un contrôle partiel sur leurs données. L'agence Publicis ETO a mené le baromètre annuel de l'intrusion qui lui a permis de constater qu'une majorité de français (78%) ne croient pas à la confidentialité de leurs données.

Ainsi, la transparence et la loyauté dans la collecte des données sont le gage d'une confiance du consommateur qui sera plus apte à donner son consentement. C'est pourquoi la relation client implique la mise en place d'une «éthique des données personnelles »[37], dans le cadre d'une collaboration entre les acteurs de la protection des données, afin d'anticiper le développement de nouveaux produits et de permettre le développement d'une approche globale qui dépasse les réglementations en vigueur. L'idée derrière cette notion est de faire prendre conscience aux acteurs que les enjeux actuels de la protection des données vont plus

[36] SCHMIDT S., « Les 3 V du big data : volume, vitesse et variété », JDN, mai 2012
[37] VALLEE M., ouvr. cité

loin que la simple application de la loi : la protection des données est aujourd'hui un atout pour le développement de l'entreprise et qui passe par l'adhésion des consommateurs.

Cette problématique fait partie de la catégorie de l' « autodétermination des données » au centre des réflexions de la CNIL notamment. C'est la marque d'une recherche permanente visant à rendre aux individus le pouvoir de disposer de leurs données, de les rendre possesseur de ce que Frederic Kaplan a appelé le « minerai biographique ».

Par ailleurs, des études ont été réalisées par des spécialistes de la protection des données et le Contrôleur Européen de la Protection des Données (CEPD)[38], dans son avis du 19 novembre 2015 sur les défis des données massives, considère que les entreprises doivent agir sur 4 points :

- **Garantir la transparence ;**
- **Donner aux personnes un contrôle accru sur leurs données ;**
- **Intégrer la protection des données dès la conception du système ;**
- **Et rendre des comptes sur leurs traitements de données.**

Ces quatre points sont centraux dans le règlement européen.

Finalement, la question ici n'est pas de savoir si la réglementation est applicable au big data mais plutôt de savoir de quelle manière appliquer cette réglementation face à de nouveaux environnements. Le croisement de ces travaux à la fois législatifs, institutionnels et de recherche agit de façon prescriptive sur ce que doit être l'éthique des données et contribue à la création d'une attente de la part des citoyens vis-à-vis des entreprises manipulant des données personnelles. Des solutions à priori plus respectueuses de la data privacy et de l'autodétermination émergent, on peut par exemple citer le cas du Web éphémérique[39]. Il est probable qu'un règlement propre au développement d'un droit « Ethics by design » des algorithmes[40] voit le jour dans les années à venir.

Ainsi le contexte dans lequel s'inscrit le règlement européen n'est pas neutre, puisque les citoyens sont aujourd'hui davantage sensibilisés quant à l'utilisation faite de leurs données.

B. Protection et gouvernance des données personnelles à l'aune du GDPR

Le GDPR renforce la protection accordée aux personnes. Pour appréhender l'importance de cette nouvelle protection, l'essence du GDPR sera notre premier point d'étude (1) avant de

[38] Actuellement Giovanni Buttarelli, chargé de veiller à ce que les institutions de l'UE respectent le droit des citoyens à la protection de leur vie privée

[39] Web instantané et effaçable (snapchat, blink, wickr…)

[40] Outil utilisé dans le cadre du data mining

nous interroger sur son intérêt économique pour les entreprises qui peinent parfois à le percevoir… (2).

1. L'essence du GDPR

Etudier l'essence du GDPR nécessite de s'interroger sur les origines de la réforme (a) avant de pouvoir comprendre les évolutions qui en sont issues (b).

a) Les origines de la réforme

Il convient dans un premier temps de comprendre les raisons qui ont poussé l'UE à adopter le GDPR. Le règlement européen fait suite à plusieurs années de débats, de négociations, d'une ampleur que jamais l'UE n'avait connue par le passé.
L'idée à la création du règlement était de **prendre en compte les nombreuses évolutions technologiques de ces dernières années**. En effet, 20 ans se sont écoulés depuis l'entrée en vigueur de la directive européenne, et une véritable refonte, visant à prendre en compte les révolutions informatiques comme l'apparition des réseaux sociaux, le développement du commerce en ligne et le recours à des solutions telles que le cloud computing[41], s'imposait.

Mais il vise également à **renforcer la protection des personnes sur leurs propres données personnelles.** Ceci étant un deuxième objectif du règlement. Les sanctions de la CNIL n'étaient pas assez dissuasives ce qui a permis d'expliquer un certain désintérêt des entreprises ou en tout cas de certaines d'entre elles à l'égard de la protection des données personnelles. La nouvelle règlementation créée un nouvel environnement juridique de nature à inciter les entreprises à respecter et protéger les données à caractère personnel[42]. L'objectif de la réforme est ainsi de rendre les consommateurs confiants. Et la confiance constitue un élément essentiel à l'innovation et au développement économique. En consolidant ainsi le marché unique du numérique le règlement favorise la libre circulation des données personnelles.

Par ailleurs, le règlement permettra **d'introduire une harmonisation entre les différentes législations au sein des états membres**. En effet, la gestion des données différait notamment en matière commerciale notamment. La logique anglo-saxonne s'articulant autour du concept de défaut d'opposition est très différente de la logique française qui est, elle, davantage tournée vers le consentement préalable. Et le GDPR renforce le consentement et la notion de transparence.

---

[41] Cloud computing ou « internet en nuage » : système permettant de mettre sur des serveurs localisés à distance des données de stockage ou des logiciels qui se trouvent habituellement sur l'ordinateur d'un utilisateur
[42] BARRAU L. et TESSONNEAU A., « Protection des données personnelles et risques juridiques », *Les enjeux des données numériques*, n°147, avril 2013, p. 25

D'application directe, ses effets juridiques s'imposent de manière simultanée, automatique et uniforme.

b) Les évolutions introduites par le GDPR

Le règlement s'inscrit indéniablement dans la continuité de la directive de 1995 (1). Il présente cependant quelques évolutions (2).

(1) La continuité de la directive européenne

La définition de la donnée à caractère personnel reste globalement la même. Le règlement la définit en effet comme « toute information se rapportant à une personne physique identifiée ou identifiable, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, ou un identifiant en ligne, ou un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».
Il vient néanmoins préciser dans son considérant 26 ce qu'il entend par « identifiable ». Pour déterminer si une personne est identifiable, il convient de prendre en compte « l'ensemble des moyens raisonnablement susceptibles d'être utilisés soit par le responsable de traitement, soit par une toute autre personne… tels que le ciblage » et considérer « l'ensemble des facteurs objectifs tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci ».

La notion de traitement des données à caractère personnel conserve globalement son champ actuel. Il existe à partir du moment où l'on collecte, traite, conserve, modifie, transfère des données, que celui soit automatisé ou non. De manière simplifiée, le traitement existe dès lors que la donnée a été organisée pour être rendu exploitable.

En ce qui concerne le consentement, la définition évolue légèrement et permet de compléter celle de la directive 95/46/CE puisqu'il repose désormais sur un acte positif clair. Mais à l'instar de la directive, il devra être indubitable.

Par ailleurs, les principes clés de la loi de 1978 restent : il s'agit des principes de licéité des données qui comprend la finalité et la qualité des données, la donnée devant être non excessive, pertinente et collectée pour une finalité, le principe de conservation des données, de flux des données, de protection des données sensibles, et de confidentialité et de sécurité.

Le GDPR introduit cependant de nouvelles définitions et de nouveaux principes (2).

(2) Les changements

Les changements concernent tant le champ d'application du règlement (a) que les nouvelles obligations et garanties qu'il reconnait (b).

(a) Le champ d'application

Un changement majeur concerne le champ d'application du GDPR. La directive s'applique à un responsable de traitement non établi sur le territoire de l'UE lorsque de moyens, automatisés ou non, y sont situées. Mais cette notion déjà large méritait toutefois d'être précisée.
Le règlement trouve application si le responsable de traitement ou le sous-traitant est établi dans l'UE, sans considération du lieu du traitement lui-même. A défaut d'établissement dans un pays de l'UE, le règlement s'applique si les personnes concernées par le traitement se trouvent dans l'UE et si les activités de traitement sont liées soit :

- « à l'offre de biens ou de services à ces personnes dans l'UE [même gratuitement et y compris des services cloud] ;
- ou au suivi du comportement dans l'UE de ces mêmes personnes »[43], par exemple si l'entreprise est un réseau social. C'est ici le critère du ciblage qui est retenu.

Le champ territorial est ainsi considérablement étendu : l'approche pour le règlement doit se faire au-delà d'une approche européenne. Il y a ainsi une exportation du système de protection de l'UE à l'extérieur de celle-ci contrairement à la loi Informatique et Libertés qui prévoyait le critère de la localisation de l'entreprise sur le territoire de l'UE.

Désormais, dès lors qu'un citoyen européen sera visé par un traitement de données, y compris par internet, le règlement s'appliquera. Les géants de l'information comme Google ou Facebook seront donc concernés. Il suffit donc en tant que commerçant, de vendre ou de proposer des services en ligne à des personnes situées dans l'UE, pour se voir soumis au règlement.

Le responsable de traitement en question devra désigner un représentant au sein de l'UE, physique ou morale qui aura vocation à le représenter.

Par conséquent, le GDPR permet de créer des conditions de concurrences équivalentes entre les entreprises de l'UE et celle hors de l'UE proposant des biens et services dans l'UE qu'il pourra désormais s'appliquer à des entreprises dont le responsable de traitement se situerait en dehors de l'UE.

[43] GDPR, art 3

Par ailleurs, si le règlement s'applique aussi bien au secteur privé que public, c'est désormais **le lieu d'établissement du responsable de traitement qui détermine la manière dont sera mis en œuvre le traitement, ou de son sous-traitant qu'il convient de prendre en compte.**
Ainsi, si un responsable de traitement ou un sous-traitant est établi dans plusieurs pays de l'UE, c'est là que le règlement prend tout son sens puisqu'il met en place un « guichet unique » permettant de solutionner l'absence de coordination entre les autorités nationales compétentes au regard de la directive. L'autorité de contrôle compétente sera celle dont relève l'établissement principal ou l'établissement unique du responsable de traitement. Elle devient l' « autorité chef de file ». Et une seule législation sera applicable.

L'entreprise devra être en mesure de démontrer que son établissement principal se situe sur l'un des états membres, c'est généralement le lieu de son administration centrale, ou à défaut l'établissement où sont prises les décisions relatives aux finalités/modalités du traitement.

Détermination du « guichet unique »

Responsable de traitement établi dans plusieurs états membres	Sous-traitant établi dans plusieurs états membres
L'administration centrale dans l'UE	L'administration centrale dans l'UE
Sauf si : les décisions sont prises dans un autre établissement de l'UE et que l'établissement dispose du pouvoir de faire appliquer ces décisions	A défaut de siège central dans l'UE : le lieu dans l'UE ou se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant

Avec l'instauration du guichet unique, les entreprises disposeront d'un interlocuteur unique au sein de l'UE en cas de traitements transnationaux. Les particuliers pourront s'adresser à cet interlocuteur unique dans leur propre langue.

Par ailleurs, à partir de mai 2018, le règlement impose aux entreprises de mettre en place une gouvernance qui devra s'inscrire dans un contexte de conformité mais également de positionnement concurrentiel.

(b) De nouvelles obligations et une gouvernance renforcée

Outre les droits d'accès, d'opposition et de rectification, le GDPR consacre de nouveaux droits aux individus :

Alors que la directive ne faisait du droit à l'effacement qu'un corolaire du droit d'accès, le GDPR consacre à l'article 17 **un droit à « l'oubli » ou droit à l'effacement** : la personne concernée peut désormais obtenir l'effacement de ses données dans six cas énumérés par le

GDPR[44]. Ce droit est consacré pour la personne mineure. Pour certains, cette énumération apparait comme une régression par rapport à la directive qui prévoyait seulement la possibilité de demander l'effacement en cas de non-conformité à la directive. Cependant, les cas sont plutôt exhaustifs et le règlement prévoit que ce droit à l'oubli peut être invoqué suite au droit d'opposition lui-même élargi.

> Ainsi, ce droit à l'oubli s'article avec l'article 21 du règlement qui donne à la personne concernée un droit d'opposition élargi en inversant la charge de la preuve. Désormais si une personne exerce son droit d'opposition, le responsable de traitement devra faire droit à sa demande sauf s'il parvient à démontrer des motifs « légitime et impérieux ». Ce droit à l'oubli ou droit à l'effacement des données est indispensable pour le respect de la vie privée. Le règlement fait également référence au droit au déréférencement par les termes « effacement des liens » de l'article 17, qui permettent de ne pas limiter cet effacement à une source primaire d'informations[45].

Il leur reconnait, par ailleurs, un **droit à la portabilité des données**[46] qui correspond au droit de transmettre les données à un autre responsable de traitement ou de les récupérer dans un format standard et lisible par tout type de matériel de manière complète, par exemple dans le cadre ou la personne souhaite que ses informations soient transmises à un fournisseur d'accès.

Enfin, le règlement reconnait un **droit à la limitation du traitement**[47] qui permet la personne à demander non pas une suppression des données mais une limitation de leur utilisation. Elles seront alors seulement stockées. C'est par exemple le cas dans le cadre d'un abonnement arrivé à terme.

Par ailleurs, **le droit d'information est renforcé**. L'information est dorénavant plus claire et plus accessible. Elle doit contenir de nouvelles mentions telles que les coordonnées du DPO ou la durée de conservation.

Désormais avec le GDPR et pour l'ensemble des droits des personnes concernées, le responsable du traitement est tenu de répondre à la demande présentée par l'intéressé dans le délai d'un mois renouvelable une fois pour deux mois.

L'obligation de notification en cas de violation de la sécurité[48] n'est désormais plus réservée aux fournisseurs de service de communication électroniques. Ce devoir est

[44] Voir annexe n°1

[45] Le droit au déréférencement vise la suppression de certains résultats de recherche associés au nom et prénom d'un moteur de recherche sans effacer l'information sur le site source.

[46] GDPR, Art 20

[47] GDPR, Art 18

[48] GDPR, Art 4 Violation qui entraîne, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données

généralisé à l'autorité de contrôle et le responsable de traitement devra effectuer cette notification à la CNIL dans un délai maximum de 72h. La notification doit avoir lieu dans ce délai qu'on ait ou pas l'ensemble des informations et même si le responsable de traitement n'est pas sûr que la violation a véritablement un impact sur les individus.
Elle concerne désormais l'ensemble des acteurs concernés par le traitement. Cette communication implique les métiers qui vont être porteurs de l'action et c'est eux qui vont devoir communiquer et participer à la prise de décision. Ainsi, le respect de cette obligation passe par la sensibilisation car tout le monde est en mesure d'informer. Et le règlement prévoit également une collaboration avec les sous-traitants qui devront également notifier au responsable de traitement toute faille dont ils auraient connaissance dans les meilleurs délais selon l'article 33 du règlement. Ce sera donc un point à prendre en compte dans la rédaction du contrat…

Au-delà, le GDPR incite les entreprises à repenser la gouvernance de la protection des données.

La gouvernance, c'est le fait d'identifier, classer, piloter et contrôler les données à travers des processus, acteurs et instances de décision clairement définis et partagés au sein de l'organisation[49]. Ainsi développer une gouvernance, c'est développer un environnement qui permettra d'exploiter les données tout en leur important un niveau suffisant de protection[50].
Avec le nouveau règlement, l'entreprise devient acteur et régulateur dans la collecte des données. L'approche est différente. Désormais l'entreprise et le responsable de traitement sont face à une double responsabilité : juridique d'abord puisque l'entreprise se doit de respecter des obligations pour ne pas se voir sanctionner mais l'entreprise apparait également comme un régulateur qui, par la collaboration qu'elle développe avec l'autorité de contrôle, permet à la personne d'exercer ses droits.
La personne concernée est placée au centre de la nouvelle règlementation, elle a des droits et l'entreprise doit en faciliter l'exercice.

D'un point de vue juridique, avec le règlement européen, le régime des formalités préalables[51] prévu par la directive de 1995 disparait. Le règlement introduit un changement majeur à travers le principe de responsabilité ou « accountability ».

D'abord, dans les entreprises de plus de 250 salariés, le responsable de traitement devra tenir un registre de l'ensemble de ses traitements de données personnelles. De plus, toutes les entreprises manipulant des données personnelles auront l'obligation de mettre en place une documentation sur tout ce qui relève de la protection des données qu'elles traitent et qui lui

[49] FERRANDON P., « Pourquoi une gouvernance de la donnée ? », JDN, septembre 2016
[50] PwC, « Gouvernance des données, mieux maitriser vos données », brochure
[51] La loi de 1978 impose que tout traitement de données personnelles fasse l'objet de formalités préalables (déclaration, demande d'autorisation)

permettent de prouver à tout moment à leur autorité de contrôle qu'elles se conforment au règlement. L'idée est d'assurer une pérennité dans la protection des données.

L'entreprise est ainsi responsabilisée. Et chaque action ou réalisation depuis le diagnostic est concernée. Cette documentation devra par conséquent être précise. En pratique l'entreprise devra être capable de présenter à son autorité de contrôle l'ensemble des informations dont elle a besoin pour savoir où l'entreprise en est en matière de protection des données. Ainsi, cette nouvelle obligation entrainera des conséquences majeures sur les process de l'entreprise. Et si des procédures ne sont pas formalisées, non communiquées, pas respectées ou pas mises à jour, la CNIL sera en droit de sanctionner l'organisme. C'est pourquoi elle exige un réexamen régulier de ces procédures. Ce qui risque de compliquer la tâche des entreprises…

L'entreprise doit construire, étapes par étapes, des raisonnements permettant d'apporter la preuve que tous les traitements ont été conçus de manière à respecter la réglementation puisque, rappelons-le, l'entreprise aide la personne à voir ses données respectées. C'est l'esprit du principe de « privacy by design »[52]. Partie intégrante du principe d' « accountability », c'est l'une des conséquences les plus importantes du règlement. C'est la protection des données au moment de la conception de l'outil technologique, du logiciel par exemple. Ce concept implique de ne pas attendre que le produit soit en production ou que les données soient traitées pour s'interroger sur les mesures de sécurité qui permettent de respecter la protection des données.

Les avantages sont multiples : réduction des risques, services conformes à la législation, réduction des coûts de développement, et des dépenses a posteriori. Il est, en effet, moins coûteux de prévoir et mettre en œuvre que de rectifier.

L'article 25 du règlement met par ailleurs en avant que la protection compte deux étapes : une première avant la conception et une seconde pendant le traitement. Les entreprises se doivent de penser privacy et pour ce faire, il leur appartient de combiner ce premier principe à celui de « privacy by default », puisque c'est la meilleure façon de protéger les droits des personnes. Cet esprit doit, pour être bénéfique, faire partie intégrante de l'organisation. Si de la protection est faite au moment de la conception, elle ne peut être assurée que si elle est déclinée au moment du traitement de la donnée. L'entreprise doit donc mettre en place des garanties, des garde-fous pour s'assurer de ne pas collecter des informations qui dépasseraient la finalité du traitement considéré. En pratique, l'entreprise, dans le cadre d'une collecte, peut insérer des champs qui se limitent à la finalité prévue.

L'entreprise doit donc être capable de démontrer qu'elle respecte ses obligations tant juridiques, techniques qu'organisationnelles.

[52] GDPR, Art 25

Et pour pouvoir démontrer à tout moment sa conformité, le responsable de traitement peut avoir recours aux analyses d'impact, également intégrées au concept d' « accountability », pour certains traitements particuliers susceptibles d'engendrer des risques pour les droits des personnes. C'est une autre nouveauté du règlement que nous développerons dans une seconde partie relative aux risques.

Par ailleurs, **le GDPR impose désormais que de nouveaux outils de conformité soient mis en place. Le responsable de traitement devra nommer un Délégué à la Protection des Données ou DPO (Data Protection Officer)**. Il est, selon le considérant 97 du règlement, « une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données [qui] devrait aider le responsable de traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement ». Ainsi, le DPO devient un « véritable pilote de la conformité interne au cœur du GDPR »[53]. Son existence sera obligatoire, dans toutes les entreprises du secteur public ainsi que dans les entreprises dont le traitement des données personnelles revêt un caractère sensible, ce qui représente la majorité des cas[54]. Il peut y avoir un DPO groupe à condition qu'un DPO unique soit facilement joignable à partir de chaque entité.

Le DPO se devra d'exercer des missions nouvelles :

- Il sera chargé de « monitorer » le respect du GDPR, d'autres dispositions légales et des règles internes y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel ;
- Il aura un rôle d'information et de conseil envers le responsable de traitement et le sous-traitant ;
- Sur demande, il sera tenu de dispenser des conseils relatifs à l'analyse d'impact que nous développerons dans une seconde partie. Et la CNIL recommande que le responsable de traitement s'adresse au DPO sur la méthodologie à suivre lors d'une analyse d'impact ;
- De manière plus générale, il tiendra compte des risques associés aux traitements ;
- Il sera également un point de contact pour les salariés et l'autorité de contrôle sur les questions relatives au traitement, avec laquelle il coopérera par ailleurs.

Dans la pratique, par ailleurs, si le responsable de traitement tient le registre des activités de traitement, il revient au DPO de réaliser l'inventaire des traitements.

Finalement, le DPO est un interlocuteur privilégiée pour l'autorité de contrôle et les personnes concernées. Certains parlent de « chef d'orchestre »[55]. Ainsi, le poste qu'il occupe est stratégique et dépasse largement celui du CIL[56].

---

[53] CNIL, Règlement européen sur la protection des données : ce qui change, 28 février 2017

[54] Cas de désignation du DPO : voir annexe n°1

[55] Livre Blanc, Business&Decision, « GDPR, En route vers la conformité », avril 2017

[56] Ibid.

Certaines entreprises comme le groupe SMA spécialisé dans l'assurance n'ont jamais désigné de CIL. C'est le RSSI qui est chargé du suivi et de la sensibilisation des acteurs du groupe. Le groupe s'est d'abord fait accompagner par Deloitte qui a mené une mission de diagnostic. Puis SMA a choisi d'ouvrir un poste de stagiaire en données personnelles avec l'idée de transformer ces compétences acquises en DPO pour 2018.
Il convient donc que ces entreprises remédient à une telle situation car le CIL est actuellement la pierre angulaire du GDPR, il informe et relaye les messages de la CNIL auprès de l'organisation. Et si le DPO ne sera pas nécessairement le CIL, il apparait évident que le CIL aura vocation à devenir DPO à compter du 25 mai 2018.

Ainsi pour répondre aux nouvelles exigences européennes, les entreprises se doivent d'effectuer une revue de leurs processus et de l'architecture de leurs systèmes d'information. Et si aujourd'hui la règlementation est synonyme de contraintes, les entreprises pourraient à l'avenir en faire un atout si elles intègrent cette question à leur offre.

Une sorte de « révolution » est en cours et elle vise à instaurer un véritable changement des pratiques. La gouvernance en matière de données personnelles représente un bénéfice pour les entreprises qui auront davantage de visibilité sur leur patrimoine informationnel.

Au sein d'un groupe des télécommunications également, la protection des données personnelles représente un engagement fort. En 2012, la protection est intégrée dans la charte du groupe. Elle est ainsi placée au rang de ses préoccupations majeures. En 2013, alors que le PDG fera une intervention publique sur les « engagements d'orange pour la protection des données personnelles et le respect de la vie privée », la politique de protection des données personnelles sera publiée. Puis en 2014, suivra un manuel de compliance. Enfin en 2016, le Comex décide de la création du data strategy and governance Board qui remplace le data governance board ainsi que la désignation d'un DPO groupe.

Ainsi, si la question de la protection des données personnelles apparait aujourd'hui plutôt contraignante, le règlement contribue à permettre aux citoyens d'avoir le contrôle de leurs données. Elle pourrait devenir un véritable avantage concurrentiel pour les entreprises qui en feront un atout de leurs propositions commerciales.

2. Le GDPR, contraintes ou opportunités ?

Les entreprises font face à de nombreuses difficultés dans leur mise en conformité puisque le chantier imposé par le GDPR est important et nécessite une refonte du système d'information, et parce que l'échéance arrive à grand pas. Une étude de KPMG portant sur les 4 enjeux majeurs de la mise en conformité a permis d'obtenir les résultats suivants[57].

[57] Enquête General Data Protection Regulation, KPMG, 2017

- ➔ L'intégration des nouveaux droits reconnus aux personnes est considérée comme difficile dans 72% des cas ;
- ➔ Pour 68%, c'est la gouvernance qui s'avère complexe, notamment au travers de la mise en place des bons interlocuteurs ;
- ➔ C'est même dans 62% l'identification des données personnelles qui pose question ;
- ➔ Et 52% considère que les risques en matières de sécurité des systèmes d'information sont des préoccupations majeures au sein de l'entreprise.

Mais le règlement, s'il apparaît comme contraignant, présente de belles perspectives pour les entreprises. Au-delà de la pure conformité, le GDPR présente l'opportunité pour les entreprises de se démarquer de leurs concurrents. En repensant la façon de gérer les données et en permettant aux clients d'en conserver le contrôle, ces derniers accepteront plus facilement de les transmettre et surtout de transmettre des données à forte valeur ajoutée. Ainsi, l'entreprise retirera un avantage certain à revoir son approche de la protection des données s'agissant de la collecte et de leur utilisation en vue de créer un climat de confiance voire même un nouveau « contrat de confiance »[58] et ainsi d'améliorer sa connaissance du client. C'est pourquoi l'anticipation est primordial pour pourvoir dès l'application du règlement obtenir rapidement un retour sur investissement[59].

Les sous-traitants également pourraient tirer profit de la nouvelle réglementation. Au même titre que la protection de l'environnement, ces derniers peuvent faire de la protection des données un véritable argument commercial pour se distinguer de la concurrence en attendant d'obtenir le label de la CNIL, argument qui permettra selon Thomas Beaugrand, avocat au barreau de Paris, « un écrémage des acteurs qui ne seront pas conformes »[60]. On peut d'ailleurs déjà voir quelques sites de fournisseurs mettant en avant leur prochaine conformité à la réglementation européenne.

Désormais, les responsables de traitement ou les directeurs de systèmes d'information se doivent d'adopter de nouvelles pratiques ce qui implique de connaitre et de comprendre les nouveaux principes de protection, à les appliquer bien sûr mais surtout à le faire savoir ![61]

Par ailleurs, la CNIL a créé, fin 2014, un label de gouvernance Informatique et Libertés destiné à améliorer la confiance des utilisateurs en termes de protection de la vie privée envers des produits et des procédures. Il contient 25 exigences répartis en 3 catégories : l'organisation interne liée à la protection des données, la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés et enfin la gestion des réclamations et incidents. Ce projet est animé par la volonté de transformer les contraintes du règlement en avantage concurrentiel en renforçant la confiance des clients, des partenaires, des collaborateurs et de

[58] Livre blanc Deloitte, « Par où commencer ? », janvier 2017, p. 14
[59] MOURIER E., « Le GDPR comme tremplin vers une gouvernance des données gagnant-gagnant », Les Echos, décembre 2016
[60] BISEUL X., « La conformité, un avantage compétitif », Zdnet, juin 2017
[61] MATTATIA F., *Le droit des données personnelles*, Editions Eyrolles, 2013, p. 3

permettre l'anticipation du règlement et des normes ISO[62]. Facteur de transparence et de sensibilisation, le label constitue ainsi un indicateur de confiance par la mise en avant d'un comportement responsable.

Mais pour pleinement percevoir en l'application du règlement une véritable opportunité, il revient au Conseil d'Administration et au management de pouvoir démontrer aux parties prenantes de l'entreprise leur engagement vis avis des exigences du règlement.

[62] Exemple norme ISO/IEC 29134 qui fournit un cadre pour mener des analyses d'impact sur la vie privée

CONCLUSION

Le GDPR poursuit trois objectifs : celui de renforcer les droits des personnes, celui de responsabiliser les acteurs et celui d'inciter une coopération renforcée entre les acteurs de protection des données ce qui permettra l'adoption de décisions communes notamment dans le cadre de traitements transnationaux.

Mais le GDPR est un texte complexe et comprend encore quelques fois des zones d'ombres.

Pour faciliter sa mise en œuvre, le G29[63] travaille à la publication de lignes directrices en recourant à une méthode inédite. Trois à quatre thèmes de travail sont sélectionnés. Une consultation publique est organisée sur le site de la CNIL. Le contenu du texte est ensuite discuté lors d'un atelier de travail nommé Fablab à Bruxelles qui rassemble des personnalités académiques et des représentants de secteurs professionnels. Deux versions seront nécessaires pour aboutir à une publication après une deuxième consultation par les parties prenantes.

Actuellement, 4 lignes directrices ont été publiées : celles concernant le droit à la portabilité, le délégué à la protection des données, l'autorité « chef de file » s'agissant de l'établissement principal et l'analyse d'impact vie privée. Et on attend encore celles sur la certification, le consentement, le profilage et la notification des violations de données.

En permettant de clarifier le nouveau cadre juridique posé par le règlement, la CNIL aide les entreprises dans la gestion de leurs risques.

[63] Groupe de travail « article 29 » sur la protection des données. Il est un organe consultatif indépendant sur la protection des données. Il conseille la Commission européenne.

II. Les risques attachés à la protection des données à caractère personnel à l'aune du GDPR

La place du risque prend une importance capitale dans la mise en œuvre du règlement. A titre d'illustration, Daniel Le Metayer, Directeur de recherche INRIA, a relevé que les termes de risques et d'analyse d'impact apparaissent plus de 100 fois dans le GDPR alors que la directive ne les citait que 8 fois. C'est dire à quel point la gestion des risques en interne et donc la responsabilisation deviennent des enjeux majeurs **dans le renforcement de la protection des données personnelles.**

Avant de s'attacher à l'évaluation des risques (B), il convient de déterminer les risques attachés à la protection des données et particulièrement aux enjeux du GDPR (A).

A. Les risques attachés à la protection des données personnelles, à l'aune du RGPD

Les risques ont évolué en matière de protection des données ; les vulnérabilités ne sont plus seulement attachées aux applications c'est-à-dire aux serveurs et aux réseaux mais elles atteignent les données essentielles à l'activité et les process. Si la sécurisation des systèmes d'information consistait en l'installation de pare-feu ou de programmes de mise à jour de nouvelles versions de systèmes d'exploitation, elle nécessite aujourd'hui d'intégrer le facteur humain. C'est pourquoi il est nécessaire que les processus soient renforcés grâce à la technique mais aussi et surtout par la sensibilisation.

Pour pouvoir traiter ces risques, nous les identifierons dans un premier temps (1) avant de les prioriser (2).

1. Identification des risques

Si le règlement européen permettra de les limiter, une mauvaise mise en œuvre ne sera pas sans présenter des risques pour l'entreprise et ses acteurs. Ainsi, sans toutefois avoir la prétention d'être exhaustifs, nous présenterons les risques principaux à savoir le risque d'image rattaché au risque business (a), le risque juridique (b), le risque opérationnel (c), le risque financier (d), le risque extraterritorial (e) et le risque d'efficacité (f).

a) Risque d'image et risque business

Une étude IBM/Ponemon Institute a permis de démontrer que sur 350 entreprises réparties sur 11 pays différents, une violation de données représente un cout total consolidé de 3,62 millions de dollars qui le rend supérieur de 20% par rapport à 2013[64].
Or, la divulgation ou le vol de données qui ne sont pas assez sécurisées peut avoir un impact sur la confiance des clients et entamer profondément l'image de l'entreprise.

Plus grave encore, le risque d'image étant lié au risque commercial, lui-même lié au risque sécurité, l'absence ou l'inefficacité de mesures de sécurité à la fois logiques et physiques peuvent entrainer la perte d'importants volumes de données. L'entreprise s'expose à la perte de son portefeuille clients et à une baisse de son chiffre d'affaire. Ce sont donc des conséquences considérables sur l'image de cette dernière qui peuvent potentiellement

[64] Ponemon Institue, 2017 Cost of Data Breach Study : Global Overview, juin 2017

engendrer une dégradation des relations d'affaire. La presse représente ainsi un vecteur de l'atteinte à la réputation de l'entreprise.

Ainsi pour se prémunir de ces risques, l'entreprise doit mettre en place une gouvernance de ses données conformément au GDPR.

Nous l'avons vu, la non-conformité au règlement européen peut représenter un désavantage certain vis-à-vis de la concurrence. L'entreprise qui n'est pas « privacy-compliant » prend le risque de voir son image de marque être dévalorisée sur le marché.

Par ailleurs, en cas de non-conformité au règlement européen, la CNIL est en mesure, au titre de son pouvoir de sanction, de prononcer un avertissement pouvant être public. L'avertissement ne nécessite de mise en demeure préalable et il se justifie par un manquement grave mais non constitutif d'une situation d'urgence.
En 2012, La Fnac direct[65] à l'issue de la formation restreinte de la CNIL du 19 juillet a reçu un avertissement public du fait d'une conservation des données bancaires de ses clients non sécurisée. Ces données étaient conservées dans un même fichier sans cryptage ni durée limitée. Il est indéniable que l'avertissement public porte atteinte à l'image de l'entreprise.

b) Risque juridique

Si le risque juridique pèse essentiellement sur l'entreprise et sur son responsable de traitement (a), le règlement vient étendre aux sous-traitants une large partie des obligations imposées aux responsables de traitement (b).

(1) Risque juridique pour le responsable de traitement

En cas d'atteinte particulièrement grave, la CNIL peut dénoncer au Procureur de la République les infractions à la loi informatique et Libertés. Notre cadre législatif français prévoit ainsi des sanctions pénales qui peuvent s'élever aujourd'hui à 5 ans d'emprisonnement et 1 500 000 euros d'amende.

Tableau des sanctions pénales :

Thème	Infraction	Texte	Peine	Amende
Délit d'entrave	Délit d'entrave lors du contrôle	Art 51 de la loi I&L	1 an	15 000 euros
Condition de collecte	Collecter des données personnelles par un moyen frauduleux, déloyal ou illicite	Art 226-18 CP	5 ans	300 000 euros

[65] Fnac Direct édite le site Fnac.com

	Détourner des données personnelles de leur finalité	Art 226-21 CP	5 ans	300 000 euros
Encadrement des données à risque	Procéder à un traitement de données personnelles personnel incluant le numéro de sécurité sociale	Art 226-16	5 ans	300 000 euros
	Conserver des données sensibles sans le consentement exprès de la personne concernée	Art 226-19	5 ans	300 000 euros
Durée de vie des informations	Ne pas respecter le délai de conservation imposé par la loi ou le règlement	Art 226-20	5 ans	300 000 euros
Sécurité et confidentialité	Ne pas respecter la confidentialité et sécurité des données	Art 226-17	5 ans	300 000 euros
	Divulguer à des tiers non autorisés	Art 226-22	5 ans	300 000 euros
	Défaut de notification des failles de sécurité	Art 226-17-1	5 ans	300 000 euros
Droits des personnes	Ne pas respecter le droit d'opposition	Art 226-18-1	5 ans	300 000 euros
	Ne pas respecter l'obligation d'information (contravention)	R 625-10	-	1 500 euros
	Ne pas respecter le droit d'accès (contravention)	R 625-11	-	1 500 euros
	Ne pas respecter le droit de rectification (contravention)	R 625-12	-	1 500 euros

S'agissant de la personne morale, les peines d'amendes sont multipliées par cinq.

L'approche pénale présente cependant des limites. Les peines sont extrêmement élevées. A titre de comparaison, un homicide involontaire est par exemple puni de 3 ans d'emprisonnement et de 45 000 euros d'amende (art 221-6 Code Pénal). D'autre part, les sanctions financières n'atteignent jamais ce montant, se limitant à quelques milliers d'euros, et les condamnations sont rares[66]. On peut éventuellement trouver un pouvoir dissuasif à ces sanctions puisque les entreprises ne peuvent se permettre d'entacher leur image de marque. Mais ce pouvoir dissuasif reste à nuancer car les sanctions véritablement mises en œuvre se sont, jusqu'à présent, généralement limitées à des sanctions administratives de la CNIL relativement faibles ce qui explique un certain désintérêt des entreprises au chiffre d'affaire conséquent. En 2014, la CNIL a notamment condamné Google à 150 000 euros (maximum autorisé par la directive de 1995) ce qui représente 0,0003 % de son chiffre d'affaires mondial en 2012. Mais cette condamnation est apparue symbolique de la nécessité de repenser les sanctions souvent inefficaces.

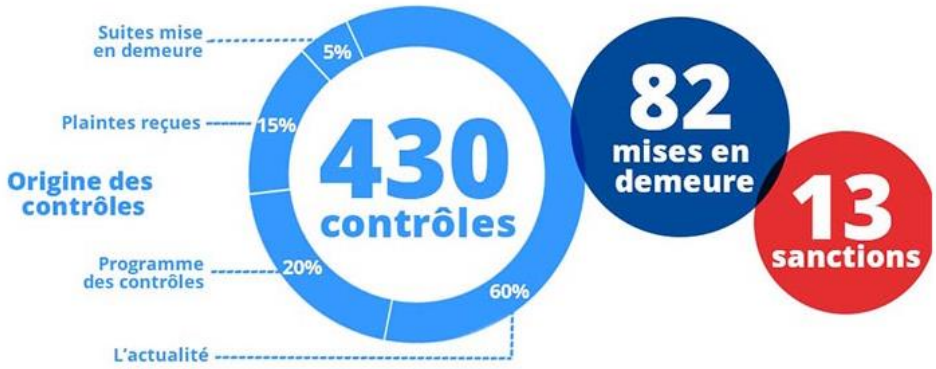
[66] MATTATIA, F., ouvr.

Les choses sont désormais en passe d'évoluer. Depuis l'entrée en vigueur de la loi pour une République Numérique, le plafond maximal des sanctions pécuniaires que la CNIL peut prononcer est passé de 150 000 euros à 3 millions d'euros. De plus, avec l'application du règlement européen, les amendes administratives pourront s'élever à 20 millions ou pour une entreprise jusqu'à 4% du chiffre d'affaire annuel mondial. Le législateur français a ainsi souhaité anticiper le GDPR. Ainsi une entreprise aujourd'hui peu respectueuse de la protection des données personnelles a grandement intérêt à se mettre en conformité. C'est l'article 83 du règlement qui prévoit ces amendes administratives.

Tableaux des nouvelles amendes administratives :

✓ 10 000 000 € jusqu'à 2 % du CA annuel mondial (entreprise), le montant le plus élevé étant retenu.	- Privacy by Design/by Default - Analyses d'impact - Tenue du registre - Désignation d'un DPO - Sécurité des traitements et violations des données (notification)
✓ 20 000 000 € jusqu'à 4 % du CA annuel mondial (entreprise), le montant le plus élevé étant retenu.	- Droits des personnes concernées - Traitement des données sensibles - Licéité du traitement et consentement - Non-respect des injonctions des autorités de contrôle

Si la CNIL dispose effectivement d'un véritable pouvoir répressif qu'elle a pu démontrer détenir, il convient de nuancer cette pratique puisqu'au regard des statistiques réalisées en 2016, les mises en demeure, donnant un nouveau délai à la personne pour s'exécuter, sont en hausse. Ainsi avant toute sanction pécuniaire, la CNIL préfère agir par la mise en demeure. Elle apparait ainsi être dans une volonté pédagogique.



CNIL, Rapport d'activité de la CNIL 2016

Avec l'application du GDPR, il est probable que les dispositions pénales soient modifiées pour être alignés à la nouvelle réglementation.

(2) Risque juridique pour les sous-traitants

Le sous-traitant est au sens de la loi Informatique et Libertés[67], « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement ». Il est le prestataire de service qui s'engage contractuellement à exécuter un travail que le responsable de traitement n'a pas le temps ou les moyens de faire lui-même.

Le règlement vient renforcer les obligations mises à la charge du sous-traitant, rééquilibrant ainsi les relations entre le responsable de traitement et son sous-traitant qui répondra aussi des manquements à la règlementation. Le sous-traitant sera soumis à certaines des obligations du sous-traitant comme la tenue d'un registre et la désignation d'un DPO. Il est, par ailleurs, également soumis à l'obligation de sécurité[68].
Le règlement renforce par ailleurs les obligations contractuelles du sous-traitant, même si certaines de ces exigences étaient en pratique déjà utilisées. Le contrat liant le responsable de traitement et le sous-traitant se trouve enrichi en matière de protection des données avec la future application du règlement. Certaines informations devront apparaitre dans le contrat comme l'objet, la durée, la finalité du traitement et les catégories de données traitées. S'il ne peut agir que sur instruction du sous-traitant, le contrat doit désormais contenir cette exigence.
Le sous-traitant doit également présenter des garanties suffisantes (connaissances du domaine d'intervention, ressources notamment) pour assurer la mise en œuvre des principes de sécurité et de confidentialité mentionnées à l'article 34 du règlement. Ainsi, des mesures techniques et organisationnelles devront être mises en œuvre pour assurer cette protection des données pour le compte du responsable de traitement (chiffrement, pseudonymisation[69]…). Si elle s'impose de fait, il conviendra néanmoins de contractualiser cette obligation. Et dans le cadre du principe d' « accountability », les sous-traitants sont ainsi responsables de la mise en place d'une documentation des traitements.

Le sous-traitant ne peut agir que sur instruction du responsable de traitement mais cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Mais si le sous-traitant ne respecte pas ses obligations ou s'il agit en dehors des instructions du responsable de traitement, le règlement prévoit que le sous-traitant sera considéré comme responsable de « son » propre traitement et par conséquent du dommage

[67] L78-17, Art 35
[68] GDPR, Art 28 et 30
[69] Pseudonymisation = Procédé permettant de manière réversible de supprimer tout caractère identifiant à un ensemble de données, à l'inverse de l'anonymisation

causé. Plus précisément, si le sous-traitant réutilise les données confiées par le responsable de traitement pour un traitement dont lui seul déterminerait la finalité et les moyens, sera considéré « […] comme un responsable de traitement pour ce traitement »[70]. Dans ces hypothèses, outre la responsabilité vis-à-vis du responsable de traitement, le sous-traitant encourra les mêmes sanctions pénales et administratives que le responsable de traitement.

Par ailleurs, si la directive prenait déjà en compte le principe de responsable conjoint de traitement, le règlement vient en organiser le régime. Le responsable de traitement et le sous-traitant deviennent des responsables conjoints de traitement lorsqu'ils déterminent conjointement les finalités et les moyens du traitement[71]. Ils ont ainsi des activités de traitement en commun.
Dans cette hypothèse, les co-responsables de traitements définissent de manière transparente leurs obligations respectives et la répartition des tâches par « voie d'accord » entre eux :

- Quant à l'exercice des droits de la personne concernée ;
- Quant à la communication des informations ;
- Quant au point de contact pour les personnes concernées qui sera désigné dans l'accord.

Et même si le texte ne l'impose pas, en pratique, ces obligations doivent être mentionnées dans le contrat le liant au responsable de traitement pour éviter tout contentieux postérieur.

Chacun des responsables de traitement est alors soumis aux dispositions du règlement (accountability, privacy by design, privacy by default, etc.) et par conséquents exposé aux mêmes sanctions.

<u>Récapitulatif des nouvelles obligations pesant sur le sous-traitant</u>

Nouveaux devoirs pour le responsable de traitement	Nouvelles obligations pour les sous-traitants
Désigner un Délégué à la Protection des Données (DPD)	**D**ésigner un Délégué à la Protection des Données (DPD)
Obligation de documenter (acocuntability)	X
Obligation d'information renforcée	X
Analyse d'impact obligatoire	**A**ssistance au responsable de traitement pour l'analyse d'impact
Notification des failles de sécurité dans les 72h	**N**otification des failles de sécurité au responsable de traitement (meilleurs délais)
Tenue d'un registre des traitements	**T**enue d'un registre des traitements

[70] GDPR, Art 28
[71] GDPR, Art 26

Mesures techniques et organisationnelles appropriées	**M**esures techniques et organisationnelles appropriées
Privacy by design/ Privacy by default dans tout projet	**G**aranties suffisantes
Mise en place des mesures de sécurité	**M**ise en place des mesures de sécurité
Respecter les nouveaux droits des personnes (droit à la portabilité, droit à l'oubli, droit à la limitation d'un traitement)	X
Renforcement du consentement	X
Protection spécifique pour les données des mineurs	X
Autorisation écrite préalable nécessaire pour recruter un autre sous-traitant	**A**utorisation écrite préalable nécessaire pour recruter un autre sous-traitant

c) Risque opérationnel

Depuis le dispositif Bale II[72], le risque opérationnel est défini comme le risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'évènements extérieurs. Le nouveau règlement va nécessiter d'apporter une analyse sur l'organisation des systèmes d'information, et du pilotage. La mise en conformité nécessitera d'entreprendre une approche par les risques opérationnels pour permettre une meilleure gouvernance des données.

L'entreprise devra notamment :

- Mettre en place des technologies automatisées associées à de nouvelles politiques notamment pour le respect des durées de conservation ;
- Déterminer des emplacements de stockage ;
- Agir en matière de sécurité informatique où l'impact du GDPR sera particulièrement important. Les nouvelles exigences règlementaires vont nécessiter une refonte des processus opérationnels informatiques ainsi que de l'architecture des systèmes d'information, et de la gestion des programmes ;
- Permettre la formation des collaborateurs ainsi que le développement des nouveaux outils pour renforcer la collaboration entre le service informatique et les acteurs principaux de la protection des données à savoir le DPO, et le CIL en vue de permettre un échange global d'informations.

Ainsi, le projet est vaste et appelle à davantage de vigilance de la part des entreprises ainsi que des sous-traitants. Il concernera également la révision des contrats notamment en cas

[72] Les normes **Bâle II** (le second accord de Bâle) constituent un dispositif prudentiel permettant de mieux mieux appréhender les risques bancaires et en particulier le risque de crédit ou de contrepartie, dans l'objectif d'assurer la solidité financière en garantissant un niveau minimum de capitaux propres

d'infogérance[73]. Ces travaux seront complexes dans la mesure où ils nécessiteront la mobilisation de nombreux interlocuteurs et de plusieurs services pour permettre une mise en conformité réussie. La mise en place du règlement va donc nécessiter plus de ressources et éventuellement pénaliser certaines activités particulièrement dans des PME, plus limitées en termes de ressources.

d) Risque financier

Au-delà du risque juridique qui dans le cadre du GDPR est attaché à des sanctions financières très lourdes, le risque financier est en réalité commun à tous ces risques et c'est finalement le risque financier qui permet véritablement d'apprécier l'ampleur et la portée des autres risques. Il est un risque indirect mais qui donne finalement « l'état de santé de l'entreprise » auquel les actionnaires s'intéresseront.
Ce sont en effet les conséquences de l'atteinte au risque juridique qui peut être graves pour l'entreprise et pas forcément le risque juridique en lui-même. Le risque d'image par exemple entraine une perte de légitimité et pour que l'entreprise « revienne », elle doit prévoir un budget conséquent pour redorer son image d'où un impact financier.
Son ampleur est difficile à évaluer, elle dépendra principalement du niveau de conformité au GDPR.

e) Risque extraterritorial

Au-delà des frontières de l'UE, le GDPR renforce l'encadrement des transferts. Le transfert en dehors de l'UE est interdit sauf à ce que le pays destinataire assure un niveau de protection suffisant. Cependant, cette interdiction ne concerne pas les pays tiers ayant transposé dans leur droit national les dispositions de la directive 95/46/CE à savoir l'Islande, le Liechtenstein et la Norvège.

Pour transférer des données hors UE, le responsable de traitement doit donc prévoir des outils permettant de les encadrer afin d'offrir ce niveau de protection suffisant aux données transférées. Ainsi, en dehors de toute décision d'adéquation de la Commission Européenne qui peut décider qu'un pays tiers ou une organisation internationale assure une protection adéquate[74], il est conseillé de mettre en place des Binding Corporate rules (BCR)[75] ou règles contraignantes d'entreprises, ou de s'appuyer sur des auto-certifications (ex « Privacy

[73] Externaliser une partie ou l'ensemble de la gestion du système informatique
[74] A ce jour, c'est le cas de d'Andorre, de l'Argentine, du Canada, des Iles Féroé, de l'Ile de Man, de Guernesey, de Jersey, d'Israël, de l'Uruguay, la Nouvelle Zélande, le Royaume-Unis, la Suisse
[75] BCR = Code de conduite qui définit la politique d'une entreprise en matière de transferts de données personnelles et permet d'assurer une protection adéquate aux données transférées à des pays tiers au sein d'une même entreprise ou d'un même groupe

Shield »)[76]. Et à défaut de prévoir des clauses contractuelles types de protection des données adoptées par la Commission…

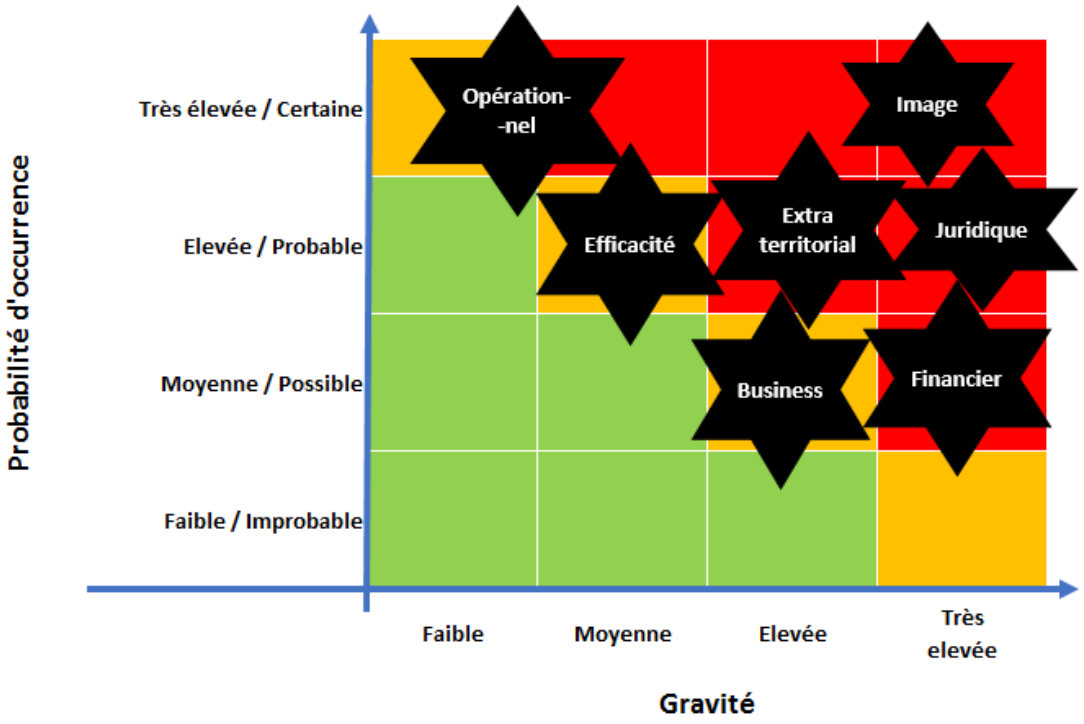
L'effet extraterritorial, dans le cadre du GDPR puisqu'au-delà des données transférées restent soumis également au droit de l'Union les traitements ultérieurs du destinataire vers un autre pays. Ainsi, les fournisseurs ou partenaires devront également présenter des garanties. Une entreprise européenne pourra transmettre des données à l'extérieur seulement si ce fournisseur sera capable d'apporter la preuve au travers d'un audit ou d'une certification par exemple qu'il apporte une sécurité des données conforme au règlement européen.

f) Risque d'efficacité

Le risque d'efficacité ou de performance est le risque lié à l'efficacité de l'exercice des activités, comme la productivité des processus et l'excellence opérationnelle, de manière à maintenir des coûts compétitifs. Ce risque est attaché à l'inefficience ou l'inadaptation des procédures qui peuvent avoir des impacts sur la mobilisation des ressources à la fois financières et temporelles de l'entreprise. Dans le contexte du GDPR, ces procédures ou étapes « inutiles » apportent de la lourdeur au programme de mise en conformité.

[76] Privacy Shield = mécanisme d'auto-certification reconnu par la Commission européenne pour les entreprises établies aux États-Unis, offrant un niveau de protection adéquat aux données à caractère personnel transférées depuis l'UE vers des entreprises établies aux États-Unis

2. Hiérarchisation des risques



B. L'évaluation des risques dans le cadre du GDPR

Une gouvernance efficace nécessite d'identifier les risques de l'organisation, de les prioriser et de les traiter en proposant des contrôles appropriés, puisque qu'une bonne protection des données personnelles permet de faire face à chacun des risques que nous avons étudié.

Si le règlement européen prévoit la suppression des formalités préalables, les responsables de traitement se voient en contrepartie davantage responsabilisés puisqu'ils devront tenir une documentation détaillée à jour pour pouvoir apporter la preuve de la conformité de leurs traitements. La revue de conformité qui est un préalable à la mise en conformité devra ainsi être complétée par des analyses d'impact, qui apportent une approche plus précise d'analyse des risques pour les traitements que la revue aura permis d'identifier.

Ainsi, il convient de distinguer l'analyse d'impact au sens du GDPR (2) et l'analyse de risques en matière de vie privée, qui passe notamment par la réalisation d'une revue de conformité préalable (1).

1. Revue de conformité préalable

La revue de conformité est le préalable à l'analyse d'impact. Elle consiste à s'assurer du respect des principes de la protection des données personnelles.

Cette revue permet d'atteindre un premier pallier en terme de conformité au règlement européen et doit donc porter particulièrement sur les droits et nouveaux principes du règlement qui ont été étudiés.

Elle permettra de manière assez globale d'identifier les données et de les cartographier, les finalités de traitements, les utilisateurs des données ainsi que les destinataires et de recenser les flux. La revue facilitera la compréhension des procédures mises en place pour protéger les droits des personnes, la sécurité des données et permettra de déterminer les mesures éventuelles à apporter. L'auditeur devra consulter les métiers particulièrement la DSI, la direction des Ressources Humaines, la direction commerciale et le DPO.

A ce stade, la revue sert donc au diagnostic et permet de répondre à la question suivante : suis-je conforme ou pas au moment de l'audit ? C'est une porte d'entrée. La revue en question permettra de détecter des traitements à risque qu'elle formalisera aux travers de recommandations qui feront l'objet par la suite d'une analyse d'impact.

2. L'analyse d'impact vie privée

a) Les principes de l'analyse d'impact vie privée

Les enjeux nouveaux, ainsi que l'évolution des process et donc des menaces nécessitent une gestion des risques de plus en plus précise qui permet de définir des mesures nécessaires et suffisantes. Le PIA (Privacy Impact Assessment) ou EIVP (Evaluation d'Impact sur la Vie privée), également appelé analyse d'impact vie privée permet d'analyser les traitements de données à caractère personnel, de prioriser les risques afin de pouvoir les traiter proportionnellement à l'impact ou à l'importance des traitements concernés.

Si aujourd'hui la CNIL encourage fortement la réalisation d'études d'impact avant la mise en œuvre d'un traitement, celle-ci deviendra obligatoire avec l'article 35 du Règlement Européen. Cet article dispose en effet que « lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, le responsable de traitement effectue, avant le traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ».

Ainsi l'analyse d'impact s'impose lorsque le traitement de données implique des données sensibles, du profilage ou de la surveillance à grande échelle d'une zone accessible au public.

La régulation a pour avantage principal d'offrir au travers de cette gestion des risques une plus grande flexibilité. En effet, le responsable de traitement évaluera lui-même les risques d'atteinte à la vie privée au sein de son entreprise.
Mais certains craignent que cette liberté nouvelle accordée au responsable de traitement n'aboutisse en réalité à une réduction des droits des individus. Le G29 est cependant venu préciser que l'analyse de risque ne doit pas affecter les droits des individus… Le règlement impose donc à l'entreprise de tracer ses décisions, d'être capable de rendre des comptes et d'expliquer ses démarches et les décisions qu'elle a pu prendre. C'est le principe de l' « accountability ». La CNIL cherche avant tout à déceler la bonne foi de l'entreprise dans la recherche d'une protection effective des données.

En ce sens, la CNIL conseille de **suivre 4 étapes dans la méthodologie d'une analyse d'impact** qui correspondent en réalité aux étapes classiques d'analyse des risques.

- La définition du contexte : elle intègre les traitements, leur finalité, les données traitées, les supports ;
- La définition des mesures juridiques, organisationnelles, sécuritaires, existantes ou prévues ;
- La définition des risques : il s'agit ici de s'intéresser aux sources de risque, et aux évènements redoutés. Chaque risque identifié devra faire l'objet d'une analyse de sa probabilité et de sa gravité ;
- Le processus de prise de décision qui consistera à expliquer le plan d'action.

b) L'analyse d'impact en pratique : comment s'articule une analyse d'impact ?

L'informatique est un outil fantastique qui ne doit cependant pas se développer au détriment de la personne physique. Les analyses d'impact reposent sur ce principe.

Le « privacy by design » a déjà permis d'identifier des mesures logiques, physiques et organisationnels. Pour que l'analyse soit complète, il convient de se poser la question des risques. Ainsi la démarche de PIA doit être utilisée dès la conception du produit avant que le système ne soit mis en place pour ainsi éviter de remettre en question les décisions prises.

Illustration

Nous allons ici étudier un projet de gestion des accès à un parking.

Finalité : Mise en place d'une gestion automatisée de parking 24/7

Caractéristiques techniques

- Accès par système de badge ;
- Mise à jour et maintenance effectuée par internet ;
- Le système offre une haute tolérance aux conditions météorologiques ;
- Le déploiement est simple et rapide ;

Spécifications techniques

- Système serveur : Windows 2000 ;
- Stockage : interne ou réseau.

Condition d'attribution

Les places sont proposées aux collaborateurs disposants d'un véhicule, à raison d'une par personne. Le demandeur devra fournir copie de sa carte grise qui sera archivée.

Informations stockées dans le système : Nom/prénom ; adresse/CP/ Ville, photo, ~~date et lieu de naissance~~, n° matricule, plaque d'immatriculation, identifiant badge, référence parking, type parking, date début contrat/date fin contrat, ~~nom et prénom des parents~~, année de présence, ~~statut nouveau conducteur si le demandeur a moins de 21 ans~~, assurance du véhicule, assurance du véhicule.

On peut déjà remarquer que des informations n'ont pas à figurer dans le formulaire de collecte au regard de la finalité du traitement.

Vraisemblance des risques

En cas d'accès non autorisé aux données, d'altération des données, de destruction des données.

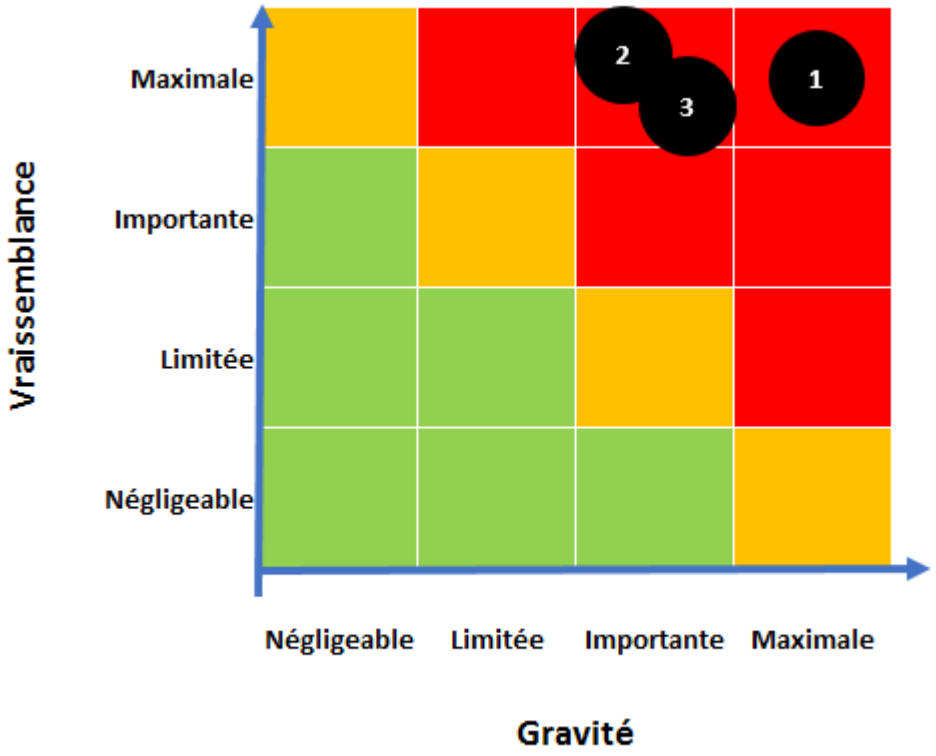
	Menace	Risque de vraisemblance	Mesures exactes	Risque global
Accès aux données (1)	Un salarié est une menace humaine Pas de système de journalisation : on ne sait pas qui entre dans le dispositif	**Menace très vraisemblable** = risque a minima important	Mesures exactes mises en place pour sécuriser l'accès aux données ? c'est assez flou = niveau de protection 0.	Maximal
Modification (2)	Même menace	Idem	Pas de mesures	Maximal
Destruction (3)	Menace supplémentaire	Idem	Pas de mesures	Maximal

Gravité

	Caractère identifiant	Impact	Gravité	Mesures	Risque global
Accès aux données (1)	Difficile de se tromper sur l'identité de la personne	Falsification de documents	Si je n'ai pas veillé à supprimer la carte grise = Gravité maximale	Pas d'adéquation des données avec les mesures juridiques	Maximal
Modification (2)	Idem : Risque maximal	Risque de faire payer le salarié davantage ou de lui faire croire que son contrat est arrêté	Blocage au parking = Gravité limitée	Pas de mesures	Important
Destruction (3)	Idem : Risque maximal	Idem	Blocage = Gravité limitée	Pas de mesures (quid sauvegarde ?)	Important

A partir de ces résultats, une cartographie des risques a pu être établie.

Cartographie des risques



La zone en rouge impose de saisir la CNIL pour avis si les risques sur la vie privée n'ont pu être réduits avec la mise en œuvre de mesures de remédiation. La zone orange signifie qu'un plan d'action est éventuellement à mettre en place. Pour la zone verte, le plan d'action n'est pas nécessaire.

c) Retours d'expérience sur la démarche d'analyse des risques

Il apparait évident, et les retours d'expériences analysés par le projet européen PIAF[77] permettait déjà de le démontrer en 2012, que l'analyse d'impact, pour être avantageuse, doit être initiée le plus tôt possible pour contribuer à la conception de l'outil. Elle doit s'intégrer dans un processus global de gestion des risques sans se limiter à la production d'un rapport. Il a également été démontré que la démarche nécessite une implication de l'ensemble des parties prenantes car, seul, le DPO, n'y parviendra pas.

Illustration de la mise en pratique de PIA :

Un spécialiste des infrastructures électriques axe son innovation sur les objets connectés réunis au sein du « programme Eliot » qui intègre depuis 2015 pleinement la sécurité des données et le respect de la vie privée. Depuis, la direction juridique travaille avec le service marketing et les Business Units pour permettre de prendre en compte le respect de la vie privée dès la conception du produit. Sur les produits Eliot, le groupe mène des PIA. Le groupe s'est doté d'une méthodologie de réalisation du PIA avec notamment un manuel PIA. Le PIA nécessite outre une forte mobilisation en accompagnement des équipes pour leur permettre une bonne appréhension des concepts relatifs à la data privacy, du temps. Ainsi, le groupe consacre des journées d'accompagnement au PIA.

Par ailleurs, une autre société a connu sa première expérience de PIA en 2014 suite à une demande d'autorisation auprès de la CNIL pour pouvoir utiliser la biométrie dans l'accès à certains locaux dangereux. L'analyse, dans ce cas, a permis de s'interroger sur les risques en cas de piratage du système. La question de la proportionnalité dans l'utilisation de cet outil est cruciale pour la CNIL qui l'a admis pour certains usages mais refusé pour d'autres comme pour l'accès à un espace copie.

Une deuxième expérience a suivi en 2016 dans cette entreprise suite à la mise en place d'une nouvelle application RH avec la volonté d'archiver tous les documents du personnel. L'analyse d'impact a permis d'analyser précisément tous les critères de protection des données personnelles afin de définir leur sécurité. Elle a permis de décider le retrait du numéro de sécurité sociale des contrats de travail puisque cela ne répondait à aucune règlementation et surtout cette précision présentait un risque pour les salariés.

Le groupe se prépare désormais à l'application du règlement en s'attachant à familiariser les opérationnels encore souvent perplexes, avec la démarche afin qu'ils puissent développer leurs compétences sur les données sensibles particulièrement.

[77] Recommendations for a privacy impact assessment for the European Union, PIAF (Privacy Impact Assessment Framework), préparé pour la Commission européenne, novembre 2012

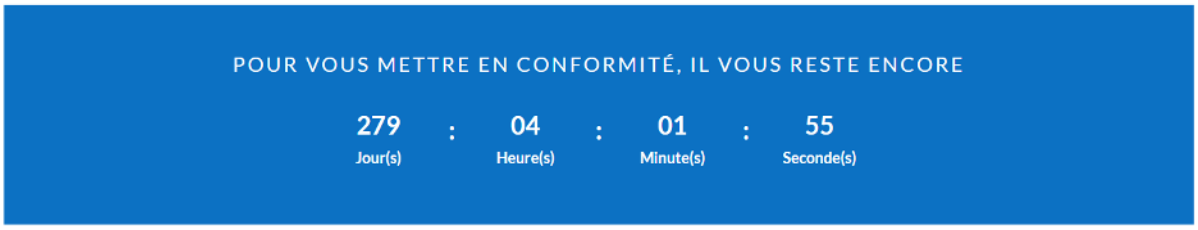
CONCLUSION

Ainsi, la démarche d'analyse des risques dans le cadre du GDPR dépasse la pure mise en conformité. Elle représente en pratique un outil permettant d'accompagner la conformité dès la conception du produit. Si l'analyse de risques n'est pas une « science exacte », le plus important pour une entreprise est d'être en mesure de démontrer son implication dans la mise en conformité par la mise en place d'une traçabilité de ses décisions.

III. La mise en conformité au GDPR

Les acteurs concernés par le processus de mise en conformité au GDPR sont au cœur de la démarche d'audit (A). Une fois les acteurs identifiés, nous nous intéresserons aux modalités de conduite du projet de mise en conformité dans des délais fortement contraints (B). Et ce chapitre fournira un guide d'audit de la protection des données à l'aune du Règlement Général sur la Protection des Données (C).

Le vendredi 18 août, à 19h58…[78]

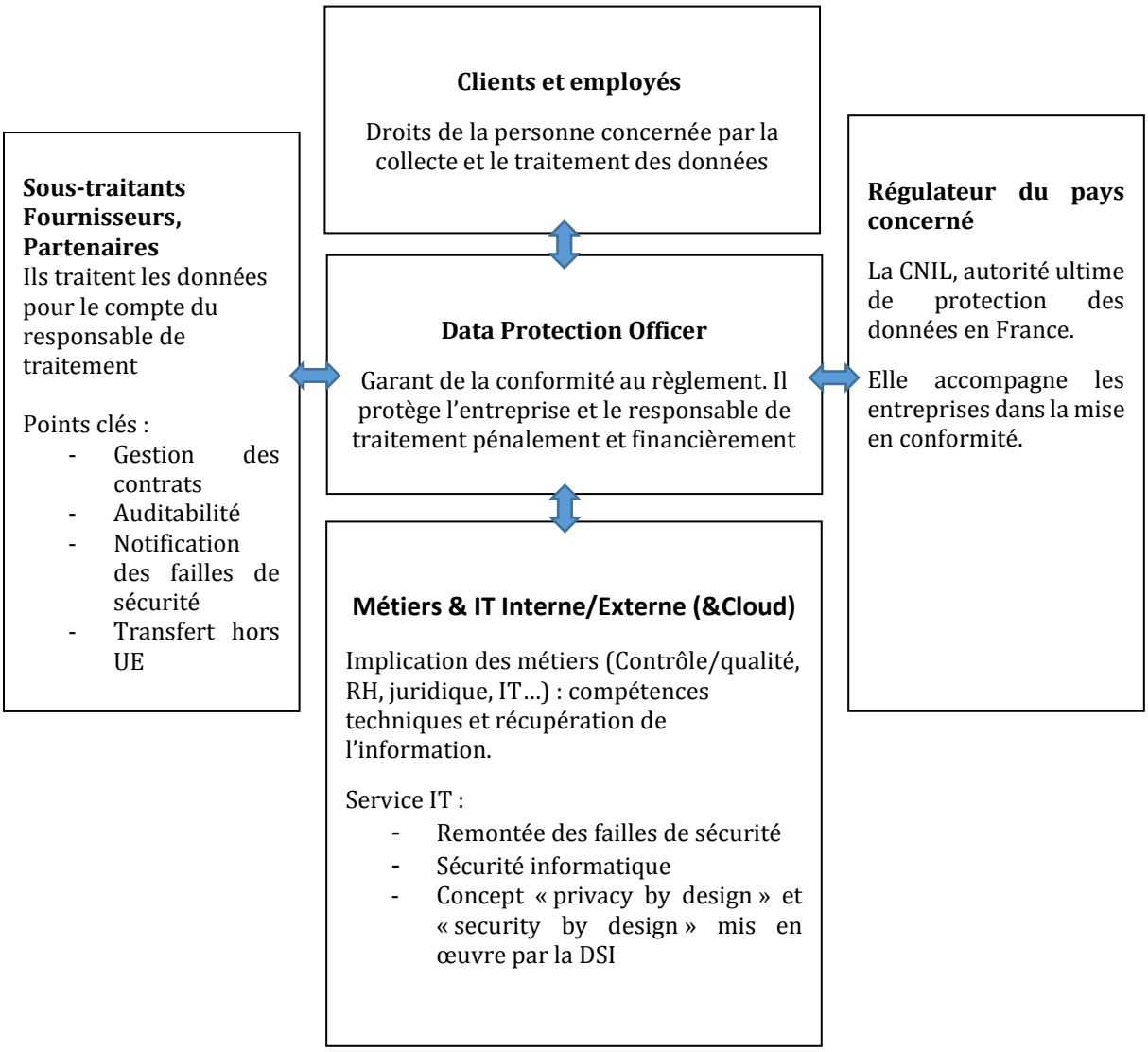


[78] Compte à rebours du site web Brainnwave GRC, leader européen de l'Identity Analytics

A. Les acteurs de la mise en conformité

Une cartographie permettra d'identifier les acteurs dont le rôle est clé pour une mise en conformité réussie (1.). Au-delà, un audit de la protection des données personnelles pourra à ce stade s'avérer nécessaire pour contrôler que ce programme de conformité est « entre de bonnes mains »… (2.)

1. La cartographie des acteurs



2. L'audit des données personnelles

L'audit, nous l'avons vu, permet s'il est réalisé avant toute mesure de mise en conformité, de faire le point sur l'existant. Mais il peut aussi être utilisé comme outil de mise en conformité. Il est alors essentiel pour donner une assurance quant aux différentes étapes de conformité au règlement européen.

L'audit de conformité des données personnelles dépasse les exigences classiques en matière de sécurité des données. Il fournit une assurance qualité sur les données et comprend l'étude :

- Des mécanismes permettant de s'assurer que l'information est obtenue légalement ;
- De la conservation des données ;
- De la documentation applicable ;
- De la conformité aux droits des personnes ;
- De la conformité à la législation.

Si les entreprises disposent de diverses méthodes pour les aider à entreprendre des activités comme l'amélioration continue, le modèle d'excellence ou les tableaux de bords prospectifs, la démarche d'audit permet, en amont et en une seule approche, de mettre en relation dysfonctionnements, causes et impacts, recommandations et plans d'action. L'audit fournit ainsi au management une feuille de route pour le management. Cette ligne de conduite servira de référence pour mesurer les améliorations quant à la conformité de l'entreprise au GDPR.

Lorsque l'auditeur mène un audit de la protection des données personnelles, il répond à trois objectifs[79] :

- Celui de vérifier qu'il y existe un système de protection des données en place dans l'entreprise conforme aux obligations ;
- De s'assurer que l'ensemble des acteurs concernés sont impliqués : c'est-à-dire qu'ils sont conscients de l'existence du système de protection, qu'ils comprennent le système de protection, et qu'ils l'utilisent ;
- Enfin de vérifier que le système en place est effectif et approprié.

Ainsi, l'analyse portera sur l'implication, dans le projet, de l'ensemble des acteurs concernés par la protection des données personnelles, sur l'existence d'une feuille de route pour une mise en conformité qui respecte une planification et d'un budget. L'audit devra également porter son analyse sur les contrôles internes en testant le caractère suffisant de ces contrôles et en recommandant, le cas échéant, de nouveaux contrôles nécessaires à l'horizon de mai 2018[80].

[79] Data protection audit manual, juin 2001

[80] ATAYA G., « L'auditeur face au chantier du GDPR », *Ouverture sur le Monde*, N°008, 4e trimestre 2016

En pratique, à partir de l'analyse de risque, l'auditeur établit son programme d'audit et ses axes d'investigation[81]. Il jouera un rôle indispensable dans le respect du « privacy by design » puisqu'il contribuera de manière à part entière à la protection des données dès le début du processus de mise en place d'un nouveau traitement. Son analyse portera également sur la capacité du DPO à exercer sa nouvelle fonction. Enfin la refonte de l'architecture du système d'information impliquera d'évaluer la sécurité interne.

Les bénéfices qui ressortent de cet audit seront une conformité facilitée, une meilleure compréhension de la protection des données et une prise de conscience en interne, ainsi qu'une amélioration de la satisfaction du consommateur par la réduction du risque d'erreurs susceptibles d'entrainer des plaintes.

Par ailleurs, quand l'entreprise fait appel à des sous-traitants, la vérification sur la protection apportée par ce sous-traitant à la protection des données peut être limitée, c'est pourquoi un plan d'audit doit intégrer la relation contractuelle. L'entreprise restant responsable des actes de ce sous-traitant, des clauses d'auditabilité doivent être intégrées au contrat pour permettre un contrôle de ce sous-traitant dans sa gestion des données personnelles.

[81] L'auditeur s'attachera à préciser les volets exclus de sa démarche de protection des données dans sa lettre de mission et à centrer sa démarche sur l'approche « conformité au GDPR ».

B. La mise en œuvre du projet de mise en conformité au GDPR

Nous l'avons vu, avec le renforcement des sanctions, une protection des données personnelles conforme au GDPR s'impose.

Il convient ici de se demander si :

1/ L'entité a mis un projet de conformité en place ;

2/ Le projet déployé lui permet d'être conforme en mai 2018.

L'éditeur Symantec[82] a publié un dernier rapport démontrant que le GDPR manque encore de clarté pour bon nombre d'entreprises. En effet, 96% des entreprises françaises allemandes et britannique ne comprennent que partiellement le règlement selon cette étude de 2016. Pire encore, selon 22% des personnes qui ont été interrogées, leur entreprise ne sera pas conforme au règlement à la date butoir…

En outre, la difficulté du projet de conformité au GDPR est **le délai particulièrement court.** Gartner a même permis d'estimer que 40% des entreprises ne seront pas totalement conformes en 2020[83]. C'est pourquoi l'idée est ici de s'interroger sur les activités qui doivent être organisées pendant cette période transitoire, et donc de proposer un parcours de mise en conformité.

[82] Livre Blanc Deloitte, ouvr. cité, p. 14
[83] Gartner, EU privacy Will Impact Delivery of Your Data Security Product Marketing Messages, 10 mars 2017

1. Les enjeux de la mise en conformité

La protection des données personnelles est à la frontière de deux enjeux fondamentaux. Un enjeu technique d'abord qui permet de s'interroger sur la démarche opérationnelle et sur la manière dont elle doit s'articuler pour un maximum d'efficacité dans le traitement des données. C'est le potentiel impact pour l'individu qui guide cette démarche. Si le règlement impose « seulement » de protéger les données en laissant l'entreprise libre de choisir les mesures et outils à mettre en place , ces mesures doivent cependant être adaptées aux risques. Il faut dérouler l'approche sur les risques avant d'entreprendre des activités de traitement. Il va falloir, en effet, modifier la méthodologie et les process IT et ce travail sera plus rapide si une analyse de risque a été faite, car dans ce cas, on adapte ce qui est en place en terme de process.

Il y a ensuite l'enjeu juridique. L'entreprise devra à tout moment être en capacité d'apporter la preuve à son autorité de contrôle que l'ensemble des données personnelles qu'elle exploite sont protégées. A défaut, l'entreprise encoure des sanctions administratives. Par ailleurs, du fait de ces nouvelles exigences en matière de sécurité, les différents contrats conclus avec les sous-traitants devront être revus.

Au-delà de ces enjeux, l'approche méthodologique permet d'appréhender de manière pratique et « terrain » la mise en conformité.

2. Approche méthodologique pour la conduite du projet de mise en conformité

Le chantier auquel les entreprises doivent faire face représente un coût important, et surtout beaucoup de temps pour les entreprises qui doivent repenser leur organisation et l'architecture de leurs systèmes d'information. C'est pourquoi l'anticipation est le maitre mot. Plus elles anticipent et plus elles seront en mesure de déployer une stratégie efficace de protection des données[84].
Les entreprises se doivent donc de trouver un équilibre entre les données qu'elles recueillent, les objectifs, la gestion des risques et la conformité[85]. Cet équilibre ne pourra être atteint que par l'adoption d'un programme de conformité qui devra s'adapter à chaque organisation pour être pleinement adopté. Il s'agit, par ailleurs, d'un projet transverse qui recouvre plusieurs métiers et qui par conséquent implique de rassembler une multiple de compétences.

[84] SOENEN P., « Anticiper la conformité au nouveau Règlement Général sur la protection des données », Tribune Libre, n°008, 4e trimestre 2016
[85] Livre Blanc Deloitte, ouvr. cité, p. 20

La première étape est celle de la compréhension, de l'assimilation. Il faut agir par rapport à l'esprit de son entreprise. Il faut que l'entreprise soit prête, donc il ne sert à rien d'appliquer des standards puisque cela ne fonctionnera pas sur le long terme. La culture de l'entreprise est à prendre en compte. En effet, le texte n'est pas seulement de la conformité, l'idée est de dynamiser l'économie numérique, de transformer les exigences en leviers de compétitivité et d'accompagner l'entreprise dans sa transformation digitale. Ainsi le programme devra pleinement intégrer la stratégie de l'entreprise.

La seconde étape est l'organisation. Cette étape passe par le pilotage et l'identification des parties prenantes au projet. Il est donc important d'embarquer très tôt les membres de la direction dans le projet, La sensibilisation de la direction permet de lancer le projet et de déterminer des éléments tels que la mise en en place d'organes de suivi. C'est ce qui donnera au projet son dynamisme en interne. Et le DPO en pratique ne pourra réussir sa mission s'il n'obtient pas l'adhésion du Comex et du comité de direction.

En outre, cette étape nécessitera l'organisation de formations et une sensibilisation des opérationnels.

A ce moment-là il peut être judicieux de désigner un point de contact dans l'attente que les « acteurs principaux » en interne ne soient désignés. Ce point de contact permettra de superviser le programme et de gérer la planification.

L'entreprise peut ensuite passer à l'action. C'est à partir de la connaissance de l'existant qu'on peut mettre en place l'opérationnel et arriver à une conformité telle qu'elle est exigée par le règlement.

L'entreprise commencera par réaliser un état des lieux de ses traitements et des données traitées, des actions déjà mises en place et respectueuses du règlement, des moyens dont dispose l'entreprise. Cette première étape permettra d'évaluer le niveau de maturité ainsi que les zones de risque, et au travers d'analyses d'écart, de soulever d'éventuels failles pour permettre d'identifier les actions prioritaires à mener. Des questionnaires pourront être envoyés aux entités du groupe pour permettre l'identification de ces actions. A ce stade, une revue réalisée en interne ou par l'intermédiaire d'un cabinet pourra s'avérer nécessaire.

La priorisation de ces actions permettra ainsi d'identifier des traitements de données à risque élevé. Un PIA permettra d'analyser les impacts de chacun de ces traitements et ainsi d'identifier des mesures de remédiation.

En même temps que l'entreprise s'interrogera sur ses traitements de données, l'implication des parties prenantes concernées : RH, communication, marketing… est à organiser très rapidement après la nomination du DPO. Les responsabilités pourront alors être attribuées à la fois en interne mais également sur un périmètre plus large en tenant compte des sous-traitants, hébergeurs… Un comité de pilotage pourra être mis en place ce qui permettra de réunir les parties prenantes.

Une fois la cartographie des données réalisée, les risques évalués et les dysfonctionnements détectés, la feuille de route doit être planifiée afin gérer les objectifs définis en amont. Et en plus d'un planning, un budget sera associé au projet.

Après l'action, c'est la phase de réalisation. La phase des travaux de mise en conformité avec la mise en place de mesures organisationnelles et techniques pourra débuter. Chaque étape de réalisation (du diagnostic à la mise en conformité) devra faire l'objet d'une documentation actualisée pour assurer une protection en continue.

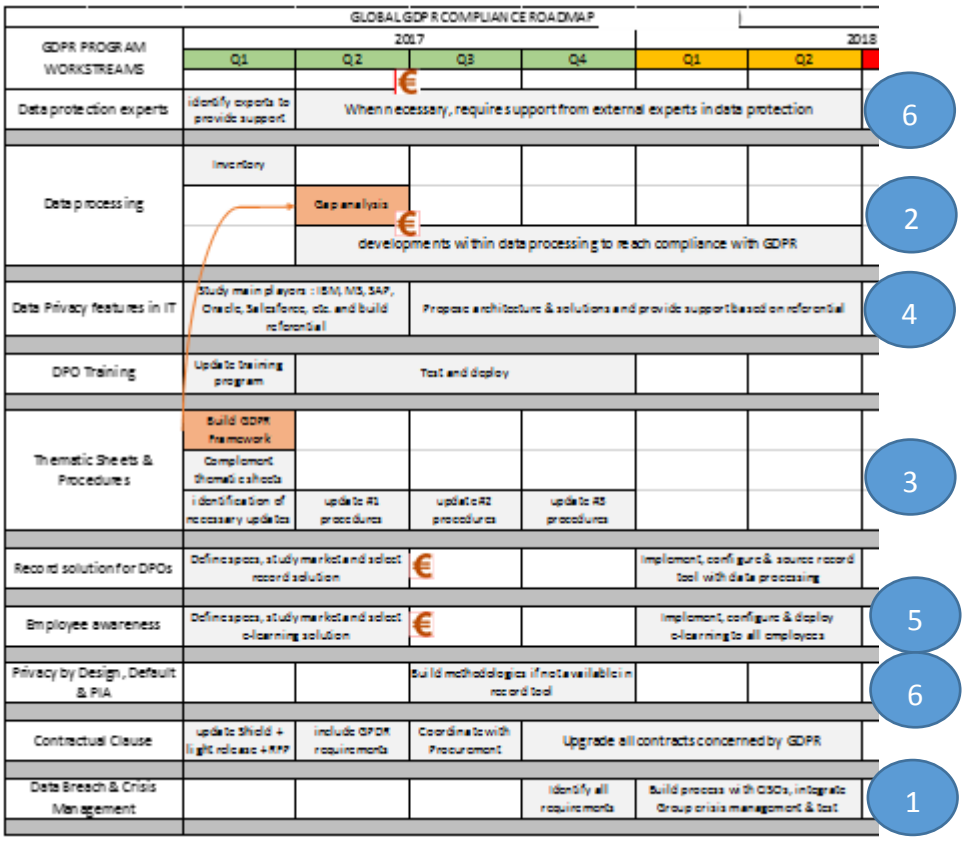
Le système d'information devra évoluer en permanence dans l'entreprise, c'est la conduite du changement. L'idée est de permettre un contrôle continu de la conformité en contribuant à une prise de conscience globale au sein de l'entreprise grâce à une communication étendue[86].

Enfin, l'amélioration continue ne pourra être satisfaite que par la mise en place d'un service de veille juridique, d'un service de contrôle interne et par l'acquisition de certifications.

Ce séquencement sera une aide à l'auditeur pour élaborer son programme de travail et s'assurer de la mise sous contrôle de ce projet de mise en conformité.

[86] Business&Decision, Petit-déjeuner GDPR, 30 mars 2017

Illustration : Les facteurs clés de réussite pour élaborer un programme de compliance dans un délai contraint à partir d'un benchmark réalisé.



1/ L'entreprise s'assure que les clauses réglementaires de protection des données insérées dans les contrats ont été mises à jour.
2/ Elle vérifie que l'inventaire des traitements et les analyses d'écart ont été finalisés.
3/ Elle établit le plan d'action de mise en conformité avec notamment un volet de mise en conformité juridique.
4/ Elle prend en compte des délais de réalisation de la mise en conformité informatique au regard de l'échéance de mai 2018, y compris le rapprochement avec les éditeurs, sous-traitants de la mise en conformité informatique. Il convient de prévoir dans ce dernier cas, une consultation avec la direction des achats pour les challenger.
5/ L'entreprise met, en parallèle, en place des outils de e-learning dédiés à la sensibilisation des collaborateurs et une formation dédiée au DPO.
6/ L'entreprise développe sa matrice du risque data privacy. L'entreprise met en œuvre des méthodologies sur l'analyse d'impact notamment pour faciliter l'application. Et il est ici possible de s'appuyer sur l'exemple donné dans la partie II.
Le benchmark permet de mettre en exergue les éléments clés suivants :

- L'entreprise doit mener une réflexion sur les niveaux de coopération, de coordination à mettre en place et les ressources à mobiliser, éléments qui doivent être particulièrement surveillés.
  Pour cela, l'entreprise détermine le rythme de suivi d'avancement des travaux en intégrant l'après 25 mai 2018, au travers de la mise en place d'un comité de suivi au niveau groupe et de rencontres organisées avec les commanditaires du projet (personne qui porte le projet en interne). L'entreprise met également en place un reporting sur la protection des données, un suivi et échange entre les commanditaires du projet et les acteurs de la mise en conformité.
- Le dispositif de contrôle interne de l'entreprise dès lors qu'il intègre l'analyse de la mise en conformité est un atout pour conduire ce projet.

Par ailleurs, un groupe spécialisé dans le domaine de la réassurance a lancé le projet de mise en conformité il y a plus d'un an. Il a classiquement mis en place une gouvernance qui embarque la totalité des équipes au sein du groupe : IT, compliance, juridique.

Le groupe mène plusieurs actions :

- Il a réalisé un plan d'action avec d'abord l'établissement d'un inventaire des données personnelles et des traitements associés, de la sensibilité des données dans ces traitements pour établir une priorité d'action et un budget afin d'encadrer l'ensemble ;

Le projet est piloté par la gouvernance IT. Et le projet est remonté au comité exécutif et au Conseil d'Administration.

- Le groupe pilote un groupe d'initiative qui réunit le CIGREF, l'AFAI et TECH IN France, et qui vise à élaborer un guide pratique pour se mettre en conformité avec la réglementation. Ce groupe de travail a démarré il y a 11 mois et la production du livrable est prévu en novembre prochain. Le groupe d'initiative réunit les membres de ces 3 associations.
  - Le sous-groupe piloté par l'AFAI[87] réalise la checklist des questions pour se mettre en conformité ;
  - Le CIGREF[88] contribue à identifier les mesures techniques identifiées sur les SI au regard des risques en matière de protection des données ;
  - Et TECH IN[89] France produit les outils juridiques de la conformité GDPR.

Par ailleurs, le groupe s'accompagne également de plusieurs cabinets d'avocats pour avoir une lecture pratique de la réglementation.

[87] AFAI = Association Française de l'Audit et du conseil informatique : association internationale des professionnels des SI qui regroupe plus de 110 000 membres dans 75 pays

[88] CIGREF = Club Informatique des Grandes Entreprises Françaises : association d'entreprises, qui a pour vocation d'aider leurs dirigeants à faire de la culture numérique un outil d'innovation et de performance

[89] TECH IN = A l'origine AFDEL (« Association française des éditeurs de logiciels et solutions internet ») pour représenter les éditeurs de logiciels et contribuer au développement des PME et Starts up du secteur

Il bénéficie, enfin, d'un support de la CNIL qui vient porter un regard croisé par rapport à l'avancement des travaux. Le groupe organise des réunions plénières tous les 3 mois dans le cadre du groupe de travail à l'occasion desquelles la CNIL, invitée, réagit sur l'avancée des travaux. A l'occasion d'une de ces réunions plénières, le projet de ce groupe a été présenté à la CNIL qui s'est montrée intéressée pour l'utiliser comme exemple au sein des entreprises.

Si selon ce groupe, il sera difficile d'être conforme sur la totalité des données et l'ensemble des systèmes d'information, l'important selon lui pour la CNIL est d'avoir engagé un projet avec priorisation des actions en fonction de la criticité des traitements.

C. Guide d'audit, outil transverse pour contrôler le dispositif de contrôle

Ce guide d'audit s'appuie sur le GDPR. Les exigences en vigueur aujourd'hui, telles que les formalités de déclaration préalables auprès de la CNIL, qui auront vocation à disparaitre dès le 25 mai 2018 n'y figureront pas.

Le terme DCP sera parfois utilisé pour désigner les données à caractère personnel. Les termes ST et RT seront également employés pour désigner respectivement le sous-traitant et le responsable de traitement.

GOUVERNANCE

Compos. ante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Politique	- S'assurer que la protection des données personnelles est encadrée et clairement règlementée en interne	- Politique de protection des données claire et diffusée aux acteurs de la protection des données en interne	- Risque de désorganisation - Méconnaissance par les personnes de leurs droits	- Désigner une personne en charge de porter le dossier protection des données et la politique afférente	**-Analyse documentaire** : - Demander une copie de la politique et une trace mail prouvant la diffusion en interne - Vérifier si la politique est passée en Comex : récupérer le compte rendu du Comex qui a validé la politique et sa diffusion
	- S'assurer que la documentation (charte, guide de bonne conduite, procédures, note interne) est mise à jour et diffusée à l'ensemble du personnel de l'entreprise	- Documentation communiquée d'une manière adéquate et facilement accessible (intranet, newsletters, réseau social interne…)	- Le personnel ne détient pas les informations lui permettant d'assurer la protection des données personnelles	- Mettre en place une veille juridique pour maintenir la documentation à jour	- **Analyse documentaire** : - Vérifier que les documents à disposition des salariés sont facilement accessibles : site intranet du groupe, publications de l'entreprise, newsletters, rapports annuels - Demander les dernières procédures pour vérifier la mise à jour effective - **Sondage** : - Sélectionner un échantillon représentatif parmi le personnel à interroger sur leur connaissance de la documentation

Compos. ante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Data Protection Officer	-S'assurer que l'entreprise a nommé en interne une personne chargée de la protection des données ou désigné cette personne en tant que DPO à l'autorité de contrôle	- Vérifier si l'entreprise répond à l'un des cas de désignation obligatoire posés par le GDPR - Moyen de désignation formelle auprès de l'autorité de contrôle - Formalisation des missions du DPO: lettre de mission - Annuaire des DPO	- Risque de non-conformité au règlement - Risque de sanctions financières - Risque d'image et de réputation - Risque d'efficacité et de non atteinte des objectifs	- Mener une réflexion pour identifier une personne en charge de la protection des données personnelles - Etablir une procédure de nomination (interne) et/ou de désignation (externe) - Formaliser les missions confiées au DPO et les ressources dont il dispose - Préparer le plan de communication concernant le DPO - Mettre à jour l'annuaire des DPO en fonction des arrivées/départs - Prévoir une personne remplaçante en cas de période de congés du DPO	- **Analyse documentaire** -Obtenir une preuve formelle de la nomination du DPO (lettre de mission signée) et de la communication de sa nomination en interne ou une trace de sa désignation auprès de l'autorité de contrôle - Interview du DPO pour s'assurer de sa motivation
	-S'assurer que cette personne dispose des ressources adéquates à l'exercice de sa fonction	- Budget nécessaire à ses activités - Formations requises pour son expertise - Disponibilité nécessaire au plein exercice de ses missions	- Risque d'efficacité et non atteinte des objectifs - Risque de non-conformité au règlement - Risque de sanction financières - Risque d'image et de réputation	- Identifier les formations requises lors de l'entretien annuel de performance et planifier son calendrier de formation - Mettre en adéquation le budget avec les enjeux et au vu du rapport annuel d'activité et des priorités de l'année en cours ou à venir - Prévoir d'organiser une réunion avec le RT pour échanger sur l'exercice de sa mission	- **Analyse documentaire:** - Obtenir copie de la feuille de présence aux formations - Demander communication du budget consacré à l'activité - Identification des formations suivies ou à venir - Obtenir trace, le cas échéant, des difficultés liées à l'exercice des fonctions du DPO (manque de disponibilités, manque de ressources) et le plan de remédiation associé

Compos. ante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Relais du DPO	- S'assurer que le DPO a identifié des relais compétents sur son périmètre le cas échéant (interlocuteurs privilégiés du DPO)	- Annuaire de la liste des relais - Lettre de mission des relais - Formations requises pour leur expertise - Disponibilité nécessaire au plein exercice de leurs missions - Intranet protection des données personnelles rendu accessible aux relais - Si nécessaire, justification de l'absence de relais	- Risque de désorganisation/d'efficacité : absence de visibilité sur les traitements en place si absence de relais sur le périmètre du DPO	- Cartographie des traitements et organigramme pour avoir une visibilité sur la répartition centralisée ou décentralisée des traitements (au sein des différentes directions) - Identifier une personne relais au sein de chaque direction - Etablir une procédure de nomination (interne) - Formaliser les missions confiées aux relais et les ressources dont ils disposent (budget consacré au développement des compétences) - Organiser la formation des relais - Préparer le plan de communication concernant les relais - Mettre à jour l'annuaire en fonction des arrivées/départs	-**Analyse documentaire:** Obtenir une preuve formelle de la nomination des relais (sélectionner un échantillon éventuellement) : annuaire, lettre de mission - Accéder à la cartographie des traitements - Identification des formations suivies ou à venir et trace, le cas échéant, des difficultés liés à l'exercice de ses fonctions (manque de disponibilité, manque de ressources) - **Entretien** avec quelques relais pour apprécier leur niveau de compétence et leur implication - Récupérer l'argumentaire le cas échéant (si absence de relais)

Compos. ante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Pilotage de l'activité	- Vérifier que l'entreprise met en place des comités de suivi entre le DPO et les relais au sein des différents services	- Existence et fréquence des comités - Agenda et comptes rendus des comités - Diffusion/publication des comptes rendu par mail ou sur l'intranet de l'entreprise - Tableau de bord de suivi, reporting et préparation du bilan annuel d'activité	- Absence de pilotage et de maitrise de la protection des données : manque d'efficacité et perte de temps dans les décisions - Non pérennité de l'activité	- Identifier les membres du comité : prévoir la présence des acteurs de la protection des données - Mettre en place un planning des réunions de pilotage - Définir les indicateurs des tableaux de bord (par ex lettre de mission signée, nomination et /ou désignation des DPO, identification des relais…) - Mettre en place un calendrier de communication (visibilité sur les thématiques et échéances) - Prévoir au cours de ces comités de faire le point sur les ressources, les problématiques rencontrées…	- **Analyse documentaire :** - Récupérer la note de décision sur le comité (expliquant sa fréquence, ses missions…) - Demander les comptes rendus des 2 ou 3 derniers comités ainsi que les présentations - **Rapprochement**: Accéder au dernier bilan annuel d'activité et le confronter aux comptes rendus des comités de l'année concernée

Compos. ante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Pilotage de la conformité au GDPR	- Vérifier que l'entreprise organise sa mise en conformité, lui permettant de s'assurer que toutes les activités prévues sont en adéquation avec les objectifs et la contrainte "temps" du projet de mise en conformité	- Existence et fréquence des comités de pilotage de la conformité : agendas et comptes rendus des comités - Diffusion/publication des comptes rendus par mail ou sur l'intranet de l'entreprise - Tableau de bord de suivi, et reporting - Budget - Liste des responsabilités dans le projet	- Pas de suivi de la mise en conformité - Risque juridique	- Identifier les membres du comité : Présence acteurs concernés par la conformité au GDPR - Mettre en place un planning des réunions de pilotage - Définir les indicateurs des tableaux de bord (par exemple inventaire des traitement, analyse d'écart, conformité juridique, conformité informatique…) - Faire le point sur les ressources, les problématiques rencontrées… - Mettre en place un calendrier d'exécution des activités et définir des étapes pour s'assurer que les objectifs initiaux sont réalisables - Recenser les ressources dont dispose l'entreprise dans la mise en œuvre du projet	- **Analyse documentaire:** Récupérer la note de décision sur le comité - Demander les comptes rendus des 2 ou 3 derniers comités ainsi que les présentations - Identifier et interroger quelques sponsors du projet (représente le projet) pour s'assurer de leur implication

Compos. ante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Accountability	- S'assurer que l'entreprise documente l'ensemble de ses actions pour démontrer la conformité de ses activités de traitement avec le GDPR	- Registre des traitements (automatisés et non automatisés) - Conformité des traitements, existence de la documentation associée et efficacité des mesures de protection prises - Déploiement des procédures telles que le privacy by design, PIA - Labels, certifications et codes de conduite	- Risque juridique et risque d'image - Impact humain: risque pour les droits et les libertés des personnes - Manque d'efficacité	- Réaliser en amont un audit des traitements et de l'existence des méthodologies (privacy by design, PIA…) - Prévoir des procédures autour de la conformité des traitements, de la mise en œuvre et tenue d'un registre - Revue régulière de la documentation pour assurer une protection des données en continu - Sécuriser le registre des traitements et structurer le registre (traitements lié au fonctionnement de l'organisme et ceux liés à l'activité du service) - Mettre en place un suivi des traitements identifiés par service	- **Rapprochement :** dans le registre, demander l'accès à quelques traitements où la conformité est assurée pour étudier les éléments et d'autres traitements pour lesquels la conformité est en cours , vérifier la documentation associée et les mesures prises - Vérifier le niveau de sécurité du registre : contrôle d'accès, chiffrement...

SENSIBILISATION					
Composante de contrôle interne	**Finalités ou objectifs de contrôle**	**Points de contrôle**	**Impacts**	**Bonnes pratiques de contrôle interne**	**Techniques d'audit**
Sensibilisation/ formation	S'assurer que l'entreprise dispose d'un dispositif de sensibilisation des collaborateurs à tous les niveaux de l'organisation et qu'un suivi y est associé	- Supports de sensibilisation/ formations - Documentation diffusée ou existence d'une plateforme e-learning	- Risque d'erreur et de mauvaise manipulation des données par les collaborateurs	- Sensibilisation par population : identifier les services qui nécessiteront des sensibilisations régulières ou particulières (CA ou Comex et services traitant de données sensibles RH, marketing...) - Prévoir une demi-journée de formation voire une journée en présentiel de ces collaborateurs en interne ou en externe - Insérer dans le dossier du nouvel arrivant, une note d'information sur la protection des données personnelles, ou dans la vidéo de présentation générale de l'entreprise	- **Analyse documentaire**: - Obtenir les supports de sensibilisation et de formation des collaborateurs à la sécurité des données personnelles - Demander les feuilles d'émergement aux informations et accéder au tableau de bord de suivi des formations et sensibilisation, '- '- Analyse du dossier du nouvel arrivant et de la présentation générale de l'entreprise '- **Tester** la plateforme e-learning

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
				- Définir des indicateurs : connaitre le nombre de bénéficiaires des formations, ou personnes participant aux e-learning et des indicateurs de satisfaction des participants - Organiser des ateliers qui pourraient se tenir lors de la journée mondiale de protection des données le 28 janvier - Prendre en compte la culture de l'entreprise dans le choix des outils	

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Communication	- S'assurer de la capacité de l'entreprise à maintenir l'attention sur la protection des données personnelles	- Supports de communication: newsletters, intranet et réseau social interne, forums de discussion… - Existence d'une communication du groupe adaptée à l'intention de l'ensemble des collaborateurs - Identification du DPO par les collaborateurs (référent)	- Risque d'erreur : le personnel ne peut pas se mettre à jour sur la protection des données ni poser de questions	- Informer le personnel sur l'existence de l'interlocuteur clé (DPO) - Mettre en place une veille sur les outils de communication pour les renouveler (application smartphone…) - Adapter l'information en fonction des populations visées et des outils de communication utilisés (en indiquant le destinataire si l'information est ciblée, et passer par la direction de la communication pour des informations plus générales qui touchent l'ensemble des collaborateurs) - Recourir à des outils novateurs : afficher des rappels d'une manière ludique sur les écrans des couloirs ou des ascenseurs, distribution de flyers, faire apparaitre des émoticônes ou personnages sur l'écran aléatoirement	- **Tester:** Vérifier l'efficacité du support de communication en testant des mots clés (pour rechercher des publications) - **Analyse documentaire**: - Récupération des exemples de communication faites par la filière communication pour des informations générales, et sur les supports de communication directement - Analyser la fréquence des newsletters et l'utilisation faite des forums

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Transparence et compétitivité	- S'assurer que l'entreprise rend visible de l'extérieur sa politique en matière de protection des données personnelles pour renforcer le niveau de confiance de ses clients et partenaires externes	- Politique disponible et facilement accessible par la presse ou les individus - Charte protection des données personnelles - Processus de diffusion	- Les tiers et parties prenantes (clients, individus...) ne sont pas informés de l'attention que l'entreprise porte sur les données - Perte de confiance et potentiellement de compétitivité	- Rédiger une note de compétitivité autour des données personnelles en interne (arguments) - Mettre en place un plan de communication autour du marketing de la compétitivité (pour suivre les actions réalisées en matière de compétitivité) - Identifier la personne en charge de ce sujet de compétitivité qui pourra être l'interlocuteur entre l'entreprise et les tiers - Mettre en place un formulaire de contact par lequel les tiers pourront contacter l'entreprise - Prévoir une politique de communication externe en cas de crise	- **Analyse documentaire**: - Accéder au plan de communication - Voir si le formulaire de contact est simple d'utilisation (onglet déroulant) et facilement accessible - Politique de communication en cas de crise - **Tester:** Consulter les publications et l'onglet réservé à la protection des données sur l'extranet de l'entreprise

CONFORMITE DES TRAITEMENTS					
Composante de contrôle interne	**Finalités ou objectifs de contrôle**	**Points de contrôle**	**Impacts**	**Bonnes pratiques de contrôle interne**	**Techniques d'audit**
Principe de licéité du traitement					
Finalité et qualité de la donnée	- S'assurer que l'entreprise a identifié des traitements et leurs finalités - S'assurer que la donnée est adéquate, pertinente et non excessive au regard de la finalité poursuivie, elle-même légitime et transparente	- Procédure permettant de déterminer la finalité d'un traitement et les données nécessaires à cette finalité - Chaque traitement fait bien l'objet d'une justification de sa finalité '- Pour chaque traitement, qualité des données ; données exactes complètes et mises a jour '- Formulaires de collecte ne contenant que les champs nécessaires	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Limiter le partage en interne de documents contenants des DCP aux seules personnes ayant un besoin d'accès dans le cadre de leurs missions - Mettre en place une liste des données qu'il est possible de collecter et de celles qui ne doivent pas l'être, en fonction des services - Etablir des guides d'entretien qui permettent au DPO d'accompagner un service dans la mise en œuvre d'un traitement (quoi collecter et dans quel contexte) - Encadrer les zones de commentaires: prévoir des cases à cocher ou menus déroulants, vérifier régulièrement pour supprimer, listes de mots prohibés bloquant l'enregistrement du formulaire	- **Analyse documentaire**: - Vérification des formulaires de collecte et de l'existence et exhaustivité de la procédure - Pour quelques traitements en cours de production, demander les documents qui permettent de justifier les finalités et les données collectées Par exemple, pour les RH : regarder rapidement les dossiers du personnel pour s'assurer que des pièces inutiles n'y figurent pas (ex permis de conduire). Pour le service de la communication: aller voir le site internet - **Tester** les zones de commentaires

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Conservation des données personnelles	- S'assurer que l'entreprise a défini des règles de conservation des données et de purge (ou archivage définitif)	- Existence d'une charte de définition et de gestion des durées de conservation prévoyant les modalités de conservation et celles d'archivage (courant, intermédiaire, définitif) Les durées sont issues de cette charte ou adaptées à la finalité du traitement - Le traitement intègre, si possible, la date de fin de conservation (ex pour un projet avec date de fin)	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- La charte a été adaptée et déclinée pour chaque service - Faire un état des lieux de ce qui est sur le terrain - Permettre la suppression des données une fois le délai atteint : mettre en place un logiciel automatisé de suppression (jusque dans les sauvegardes et les archives) - Pour les données sensibles, prévoir des outils d'effacement sécurisés plus sophistiqués qu'une simple suppression - Mettre en place des règles d'accès aux archives en limitant cet accès aux seules personnes qui y ont intérêt - Mettre en place un système de protection physique des archives : badge, détecteur fumée…	- **Analyse documentaire**: - Récupérer un exemple de charte déclinée - Pour un traitement : récupérer un exemple de durée de conservation, sa justification et la procédure associée à la purge

Respect des droits des personnes					
Recueil du consentement	- S'assurer que l'entreprise a recueilli le consentement de la personne préalablement au traitement de ses données dans le cas où le consentement est requis	- Existence d'une procédure de recueil du consentement diffusée en tenant compte des nouvelles arrivées - Par traitement concerné, collecte effective du consentement : existence d'un espace de collecte du consentement, traçabilité du consentement, et de son retrait	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Espace intranet de collecte ou case à cocher dans un contrat: "j'accepte la sollicitation" sur les formulaires en ligne	- **Analyse documentaire** : Vérifier la clarté et la diffusion de la procédure et accéder à la documentation applicable au traitement - **Test applicatif** de recueil du consentement
Droit à l'information	- S'assurer que l'effectivité des droits de la personne concernée est assurée par une information claire et accessible	- Procédure de gestion de l'information des personnes concernées faite au plus tard au moment de la collecte des données - Par traitement, définition des mentions d'informations et de leur mise en œuvre là où c'est nécessaire (contrat, site intranet, e-mail, formulaire de collecte....) - Site de l'entreprise indiquant clairement la manière d'exercer ses droits : page d'accueil ou rubrique vie privée/données personnelles	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Prévoir des moyens permettant de démontrer que l'information a été donnée : case à cocher permettant de certifier que l'individu a été informé, faire signer un document de lecture des informations... - Identifier le ou les meilleurs moyens pour garantir l'information en amont de la collecte des données dont les informations sont amenées à être collectées : panneau d'affichage, mentions site web... - Informer la personne qui viendrait exercer ses droits, en cas de vidéosurveillance	- **Analyse documentaire**: - Vérifier l'existence d'une procédure de gestion de l'information, sa clarté et sa diffusion - Sur un échantillon de traitements, vérifier que les mentions d'information sont dans les contrats de travail des collaborateurs et dans les conditions générales de vente et vérifier leur exhaustivité - Vérifier le site internet de l'entreprise

				- Par téléphone, prévoir un message automatique avant la suite de la conversation offrant la possibilité de s'opposer à l'enregistrement lors d'une collecte OU donner la possibilité de sélectionner une touche pour plus d'informations sur les mentions	
Exercice du droit d'accès des personnes concernées	-S'assurer que les personnes sont en mesure d'exercer leur droit d'accès dans les cas prévus par le règlement	- Procédure permettant de déterminer comment réceptionner la demande, à qui la transmettre, comment la gérer, qui répond, sous quel forme et dans le délai d'un mois - Exercice du droit d'accès automatisé ou manuel (adresse mail)	- Risque de désorganisation et absence de suivi des demandes - Pas d'interlocuteur désigné - Risque juridique (sanction et risque d'image)	- La procédure définit la bonne gestion du droit d'accès de la personne concernée, et est diffusée - Identifier la personne concernée - Prévoir d'envoyer un accusé de réception après réception de la demande - Automatiser dans les applications concernées l'exercice du droit d'accès pour simplifier la démarche et tenir les délais (espace clients ou applications dédiées en interne) - Dans le cas contraire, mettre en place une adresse internet dédiée aux demandes d'accès (sur le site de l'entreprise)	- A**nalyse documentaire** : - Récupérer la procédure - Vérifier que le registre intègre bien des fonctionnalités permettant de suivre l'exercice des droits et les demandes en cours - Vérifier la clarté des réponses déjà apportées - **Tester** au niveau d'un traitement l'exercice du droit d'accès et vérifier la visibilité de l'adresse permettant à défaut de l'exercer

				- Dans ce dernier cas, désigner un service chargé de recueillir les demandes qui les redistribuera selon la demande en question - Mettre en place un outil de suivi des demandes afin de respecter le délai (ex le registre du DPO peut permettre le suivi de ce délai avec alerte intégrée) - Conserver la copie des démarches effectuées (copies écran, extractions…) - Tenir un journal de l'historique des demandes de droit d'accès (ex dans le registre du DPO)	

Droit de rectification, droit à l'oubli, droit à la limitation du traitement, et d'opposition	-S'assurer que les personnes sont en mesure d'exercer leur droit rectification, droit à l'oubli, droit à la limitation du traitement, et droit d'opposition	- Procédure globale permettant de déterminer comment réceptionner et traiter la demande, à qui la transmettre, comment la gérer, qui répond, sous quel forme et dans le délai d'un mois - Exercice manuel (adresse mail)	- Risque de désorganisation et absence de suivi des demandes - Pas d'interlocuteur désigné - Risque juridique (sanction et risque d'image)	- La procédure définit la bonne gestion des demandes de la personne concernée et est diffusée - Vérifier l'identité de la personne concernée, et définir l'organisation nécessaire à la réponse - Demander des justificatifs préalablement à la rectification : changement de statut pat, domicile. - Envoyer une capture d'écran à la personne concernée après rectification ou un message de confirmation de suppression - Désigner un service en charge de réceptionner les demandes qui les redistribuera au service pour traitement - Par voie électronique, prévoir une adresse mail ou un lien facilement accessible indiquant les éléments à transmettre	- **Analyse documentaire** : - Récupérer la procédure - Vérifier la visibilité de l'adresse mail - Vérifier le suivi des demandes en cours - Vérifier la clarté des réponses déjà apportées - **Rapprochement** au niveau d'un traitement : sélectionner des échantillons de demandes (rectification, effacement...) et les réponses apportées

Droit à la portabilité	- S'assurer que les personnes sont en mesure d'exercer leur droit à la portabilité	- Procédure globale permettant de déterminer comment réceptionner et traiter la demande, à qui la transmettre, comment la gérer, qui répond, sous quel forme et dans le délai d'un mois - Exercice du droit d'accès automatisé ou manuel (adresse mail)	- Risque de désorganisation et absence de suivi des demandes - Pas d'interlocuteur désigné - Risque juridique (sanction et risque d'image)	- La procédure définit la bonne gestion du droit à la portabilité et est diffusée - Vérifier l'identité de la personne concernée (si mode manuel) - Définir la nature des données concernées par la portabilité - Prévoir un système automatisé là où la portabilité est requise (ex B to C : énergie, assurance, banque, télécom...) pour simplifier la démarche et tenir les délais (espace clients ou applications dédiées en interne) - Dans le cas contraire, l'entreprise a mis en place une adresse internet dédiée à l'exercice du droit à la portabilité (sur le site de l'entreprise)	- **Analyse documentaire** : - Accéder à la procédure - Vérifier les réponses déjà apportées - Vérifier la visibilité de l'adresse permettant à défaut d'exercer ce droit - **Tester** pour s'assurer que le registre intègre bien des fonctionnalités permettant de suivre l'exercice de la demande en cours - **Tester** au niveau d'un traitement l'exercice du droit à la portabilité

				- Désigner un service chargé de recueillir les demandes qui les redistribuera selon la demande en question - Envoyer un accusé de réception de la demande - Mettre en place un outil de suivi des demandes afin de respecter le délai (ex le registre du DPO peut permettre le suivi de ce délai avec alerte) - Conserver la copie des démarches effectuées (copies écran, extractions…) - Tenir un journal de l'historique des demandes (ex registre du DPO)	
Obligation de notification	- S'assurer que l'entreprise organise l'obligation de notification de violation de données	- Procédure de notification des violations de données diffusée - Moyen électronique sécurisé pour la notification	- Risque de non-conformité au GDPR : sanction financière et atteinte à la réputation	- Sensibiliser particulièrement sur le sujet puisque la notification doit avoir lieu en tout état de cause - Mettre en place la procédure de communication à la personne concernée après évaluation de la CNIL sur l'impact de la violation - Puisque la loi n'impose pas de délai au sous-traitant, il conviendra de prévoir dans le contrat, les délais de transmission de la violation	- **Analyse**r: accéder à la procédure de communication - Sélectionner les contrats de quelques sous-traitants et vérifier la prise en compte de la notification - Trace de la sensibilisation particulièrement des SI

Transferts & Contrats					
Transferts	- S'assurer de l'encadrement du transferts des données hors UE	- Le registre du DPO identifie pour les traitements concernés par des transferts hors UE, le dispositif permettant de l'encadrer - Le contrat doit préciser le dispositif d'encadrement retenu pour les transferts	- Risque extraterritorial - Risque juridique : sanction financière et risque d'image - Risque d'efficacité	- Mettre en place une cartographie des flux de données - Disposer de BCR pour encadrer les transferts au sein du groupe - Référencer des sous-traitants qui ont leurs propres BCR ou qui ont adopté un dispositif pour le transfert de nature à protéger les données (ex Privacy Shield pour les Etats-Unis...)	- **Analyse documentaire**: - Accéder à quelques contrats - **Rapprochement:** Vérifier que les prestataires retenus ont des clauses contractuelles types signés selon le périmètre du transfert ou des BCR - Vérifier dans le registre que le transfert est bien identifié et que le dispositif d'encadrement y est rattaché (copie de la clause, copie de la certification...)

Contrats	S'assurer que les traitements confiés à un ST font l'objet d'une contractualisation	- Une clause spécifique à la protection des données personnelles est intégrée au contrat - Identification des ST - Le ST met en place des règles permettant de garantir la sécurité et la confidentialité des données ainsi que la destruction des données à l'issue de la mission - Registre et DPO (si cas de désignation obligatoire) pour les ST	- Risque juridique : sanction financière et risque d'image	- La clause de protection doit traiter le cas RT à ST et RT à RT (les périmètres de responsabilité de chaque RT devront être précisément indiqués dans le contrat) - La clause mentionne les obligations du ST, et les garanties à prendre (Sécurité, gestion des données...), -Prévoir une clause de confidentialité et de réversibilité - Prévoir la possibilité de réaliser un audit des sous-traitants - Limiter l'accès aux données strictement nécessaires à l'exercice de sa mission et s'assurer qu'elles ne sont pas utilisées pour une autre finalité -Le contrat prévoit les conditions dans lesquelles les données doivent être soit détruites soit restituées a l'issue du contrat - Prévoir la validation des sous-traitants de 2ème niveau par le RT	- **Analyse documentaire :** **-** Vérifier l'existence de la clause spécifique (son exhaustivité) - **Rapprochement**: Pour un traitement, sélectionner un échantillon de contrats et la manière dont la clause a été intégrée et adaptée

Privacy by design/ privacy by default					
Privacy by design/ privacy by default	- S'assurer que l'entreprise prend en compte la protection des données dès la conception du produit ou service et la décline pendant le traitement	- Existence de l'application d'une méthodologie de privacy by design/default	- Risque juridique - Risque d'efficacité	- Disposer d'une méthodologie de privacy by design qui assure l'instruction d'un traitement, sa conformité et sa contribution à l'accountability - La méthodologie doit permettre d'identifier la présence de données sensibles et de déterminer les mesures de sécurité appropriées, l'existence de transferts hors UE et de les encadrer avec le dispositif approprié, d'identifier les traitements à risque (qui pourraient exclure une personne d'un droit) - Prévoir un pack de formation des chefs de projets et des DPO à ces concepts - Lorsque nécessaire, la méthodologie privacy by design doit permettre de déclencher un DPIA	- **Analyse documentaire**: - Vérifier l'existence et l'exhaustivité de la méthodologie - **Rapprochement**; Pour un projet en cours de conception, vérifier la manière dont la méthodologie est déroulée et les livrables associés

Analyse d'impact					
Analyse d'impact	- S'assurer que l'entreprise réalise une étude d'impact vie privée pour les traitements à risque	- Existence et application d'une méthodologie de DPIA - Cartographie des traitements ayant fait l'objet d'un DPIA ou devant faire l'objet d'un DPIA	- Risque juridique - Risque d'efficacité	- S'appuyer sur des experts externes pour réaliser les DPIA - Disposer d'une méthodologie pour laquelle les DPO et les RSSI ont été formés : la méthodologie doit prévoir la notification à l'autorité de contrôle pour avis en cas de risque résiduel trop élevé - Etablir la liste des traitements identifiés par le G29 comme devant faire l'objet d'un DPIA et la relier aux traitements concernés en interne	- **Analyse documentaire:** **-** Vérifier l'existence et l'exhaustivité de la méthodologie - Récupérer la cartographie - **Rapprochement**: Pour un projet en cours, de conception, vérifier la manière dont la méthodologie est déroulée et les livrables associés

Contrôle de la CNIL					
Contrôle de la CNIL	- S'assurer que l'entreprise est organisée pour répondre aux contrôles de l'autorité de contrôle	- Procédure qui prévoit la manière d'agir et qui formalise les bonnes pratiques à adopter avec des contrôleurs - L'entreprise a désigné des personnes lors des contrôles CNIL et a établi la liste de ces personnes	- Réalisation du contrôle rendue plus difficile et relations plus délicates avec l'autorité de contrôle -Risque d'entrave au contrôle	- S'assurer que l'accueil est sensibilisé à la protection des données personnelles: demandes de réclamations ou contrôles - Informer l'accueil de ce qu'est la CNIL et comment agir face aux contrôleurs - La liste des personnes doit être présente à l'accueil - Prévoir un responsable des lieux qui coordonne le contrôle et sollicite les personnes qui y participent - Prévoir dans la procédure que le responsable des lieux vérifie la lettre de mission : agents, date, périmètre - Prévoir d'appeler rapidement la CNIL pour vérifier qu'il s'agit bien un contrôle officiel	- **Analyse documentaire** sur les bonnes pratiques et la procédure - **Interview** de l'accueil pour tester son aptitude face au contrôle - **Rapprochement**: Si des contrôles ont été faits: voir les documents produits lors de ces contrôles : prise de note (main courante), REX et si cela a été intégré dans la procédure

				- Accompagner les contrôleurs dans les locaux - Prévoir une personne pour la prise de note (car PV contradictoire de la CNIL) - S'assurer que le responsable des lieux est sensibilisé en amont pour connaitre les droits de la CNIL en termes de contrôle : quels documents peuvent être demandés... - Faire appel à un expert éventuellement pendant la procédure de contrôle (avocat…) - Faire un retour d'expérience suite à un contrôle CNIL pour permettre des améliorations	

SECURITE INFORMATIQUE					
Composante de contrôle interne	**Finalités ou objectifs de contrôle**	**Points de contrôle**	**Impacts**	**Bonnes pratiques de contrôle interne**	**Techniques d'audit**
Politique	- S'assurer que l'entreprise dispose d'une politique sécurité groupe et, le cas échéant, d'une charte informatique à jour qui prévoit les comportements des collaborateurs	- Une politique permet d'organiser la sécurité des SI - La politique est à jour et exhaustive	- Risque de mise en péril des SI - Risque financier et risque d'image - Risque opérationnel	- Diffuser des fiches thématiques ou politiques thématiques de sécurité, qui détaillent des éléments spécifiques tels que la politique mots de passe	- **Analyse :** - Vérifier l'existence et la pertinence de la politique groupe et analyser les fiches thématiques éventuelles:- vérifier la clarté des fiches thématiques et leur caractère synthétique - Vérifier la diffusion de la politique et sa visibilité sur l'intranet du groupe
	- S'assurer que la politique et la charte font l'objet d'une diffusion	- Connaissance en interne de son existence et accessibilité	- Une méconnaissance de la politique entraine la mise en péril des SI - Risque financier et risque d'image - Risque opérationnel	- Diffuser régulièrement à titre de piqûre de rappel les exigences de sécurité - Donner un point de contact aux collaborateurs pour les accompagner dans l'application - Utiliser des réseaux interne, outils collaboratifs et newsletters	- **Analyse**: - Obtenir trace de leur diffusion

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Identification et authentification	- S'assurer que l'entreprise met en œuvre des mesures sécures d'authentification afin d'assurer la confidentialité des accès, la disponibilité des ressources et l'intégrité des données	- Fichiers de journalisation - Pour chaque utilisateur, identité numérique unique et identification obligatoire avant tout accès informatique	- Usurpation d'identité et risque de fuite de données - Atteinte à la confidentialité des données, à la disponibilité des ressources et à l'intégrité des données	- Adapter le niveau d'authentification en fonction de la sensibilité des données - Limiter les tentatives d'accès et historiser les tentatives - Mettre en place une politique de mot de passe : nombre et nature de caractères, changement régulier de mot de passe (par exemple trimestriellement) - Etablir une procédure de renouvellement de mot de passe en cas de perte et obligation de changement du MDP - Vérifier que les logiciels ne permet pas un enregistrement automatique des mots de passe - Prévoir le verrouillage des sessions automatique en cas de non utilisation pendant une certaine durée - Mettre en place un horodatage : date et heure de la dernière connexion au moment de la connexion à un compte	- **Interrogation des fichiers** : - Vérifier que chaque application est protégée par un système d'identification et d'authentification - **Tester** et vérifier le niveau de sécurité des mots de passe - Vérifier que l'application ne déconnecte après un temps sans utilisation

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Gestion des habilitations / privilèges[90]	- S'assurer que l'entreprise a mis en place un mécanisme de définition des niveaux d'habilitation et d'un contrôle des accès	- Profils d'habilitations - Suivi des départs des salariés ayant un accès aux DCP ou le fait qu'un salarié ne soit plus habilité à accéder à un local ou à une ressource - Application du principe de moindre privilège (accès aux ressources avec le minimum de privilèges pour conduire ses actions)	- Risque d'accès et d'actions non autorisées par une personne ayant des responsabilités ou habilitations incompatibles sur les DCP	- Mettre en place une politique de contrôle des accès et la mettre à jour - Limiter les accès aux DCP aux personnes en ayant besoin dans le cadre de leur fonction - Prévoir la procédure à l'arrivée/départ d'une personne ayant un accès légitime aux DCP - Identifier clairement les personnes ayant un accès aux DCP et identifier les hauts privilèges et les justifier - Mettre en place un tableau de suivi des habilitations - Classifier les informations afin savoir où sont les données sensibles et les protéger en matière d'habilitation - Faire des revues régulières d'habilitations (voir qui à accès à quoi et si c'est légitime)	- **Analyse documentaire**: - Accéder à la politique des accès et la procédure à l'arrivée/départ - Vérifier le tableau de suivi et trace des mises à jour éventuelles - **Rapprochement** : Accéder aux profils d'habilitation et s'assurer que leur gestion permet l'application du moindre privilège - vérifier pour quelques habilitations si les accès sont justifiés par la fonction de la personne (fiches de poste) - Vérifier que les tentatives d'accès sont suivies : demander un historique - Vérifier que le traçage des accès est sécurisé voir crypté

[90] Les privilèges sont les droits (modification, suppression…) accordés en fonction de l'habilitation

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
				- Réaliser une revue annuelle des privilèges pour identifier et supprimer les comptes non utilisé - Journaliser les informations liés aux privilèges -Tracer les accès pour suivre les activités des utilisateurs, les anomalies et événements liés à la sécurité.	
Recensement des applications	- S'assurer que l'entreprise recense ses applications	- Document permettant de connaitre en temps réel les applications régulièrement mis à jour	- Risque d'efficacité : mise en péril des SI	- Mise en place d'une cartographie des systèmes applicatifs - Mettre en place une collaboration entre les services pour récupérer les informations les plus justes possibles - Le document prévoit les applications contenants des DCP et trace les services les plus à risques et notamment les services traitements de données sensibles	- **Analyse documentaire**: cartographie des applications et accéder au document qui recense les applications contenant des DCP - **Interview** du RSSI sur comment la cartographie est rempli et mise à jour, et interroger sur la mise en œuvre de la collaboration

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Protection des données	- S'assurer que l'entreprise prévoit des systèmes de protection des données	- Architecture informatique sécurisée - Procédés de protection des données : chiffrement et segmentation des données (entre les applications)	- Virus -Vol de donnée ou de détournement de donnée	- Mettre en place un système d'information adéquat et non désuet - Installer des pare-feux par ordinateur et des antivirus - Mettre à jour les systèmes de sécurité des données et prévoir un suivi des mises à jour - Installer les patchs et correctifs logiciels - Procédés adaptés à la sensibilité des DCP (chiffrement, anonymisation ou pseudonymisation des données) - Encadrer l'utilisation des outils personnels dans le cadre de l'activité professionnelle (ex ne pas brancher le téléphone personnel sur l'ordinateur professionnel) - Audit des applications (en cas de nouvelle application)	- **Analyse documentaire:** **-** Accéder au suivi des mises à jour et des nouvelles installations de sécurité - Accéder à la procédure encadrant l'utilisation des outils personnels - Réaliser des **tests** d'intrusion

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Sécurité physique	- S'assurer que l'entreprise met en place des moyens de protection des locaux où sont traitées des DCP afin de protéger l'intégrité des données	- Protection des accès aux salles de l'extérieur vers l'intérieur et à l'intérieur de la zone - Existence d'une politique de maintenance	- Perte partielle ou totale des données - Risque de vol des données	- Protéger les serveurs de manière physique : caméras et alarmes, portillon de sécurité et SAS accessibles par des dispositifs d'authentification (carte par exemple) - Revoir régulièrement les accès limités aux SAS ou locaux contenants des DCP et tenir un tableau de bord de ces accès - Entretenir la climatisation des locaux où sont stockées et traitées des DCP - Prévoir des moyens de protection contre les catastrophes naturelles (prévoir un générateur de secours en cas coupure électrique ou des sites de secours, faux plancher contre les inondations...) - Mettre en place de la maintenance	- **Observations physiques**: Se déplacer sur le site : - Vérifier l'organisation des salles et le paramétrage des serveurs - Vérifier la sécurité physique des supports contenants des données personnelles: PC verrouillées, antivols…. - **Analyse documentaire** : - Vérifier l'existence d'une cartographie des installations/applications comportant des DCP - Demander les comptes rendus de maintenance - Vérifier l'existence de process de gestion de crise

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Sécurité des flux et accès à distance	- S'assurer que les flux sont sécurisés	- Protocoles de sécurisation des flux	- Risque d'atteinte à la sécurité de la donnée si des fichiers sont captés lors de leur transfert	- Adapter le niveau de sécurisation des flux à la sensibilité des données - Utilisation du VPN pour les accès distants et chiffrement des données - Encadrer le télétravail	- **Analyse :** - Vérifier l'existence d'une cartographie des flux et des accès à distance - Obtenir le suivi les utilisateurs de VPN

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Sauvegarde et continuité d'activité	- S'assurer que l'entreprise met en place des mesures de sauvegarde et de continuité de l'activité	- Système de sauvegarde des données et procédure associée - Existence d'un PCA	- Perte partielle ou totale des données	- Mettre en place une procédure de sauvegarde intégrant la destruction des sauvegardes une fois le délai de conservation ou d'archivage atteint - Redonder ses sites (avoir plusieurs sites : en réplication à chaud (copie en permanence) ou réplication à froid (réalisation de la copie à une fréquence définie), - Effectuer régulièrement des sauvegardes - Selon le volume de données, prévoir des sauvegardes incrémentales (n'enregistre que les modifications par rapport à une précédente sauvegarde) ou complètes à une fréquence moindre - Sécuriser le stockage des supports de sauvegarde - Réaliser des tests régulier de la continuité d'activité	- **Analyse**: - Accéder à la procédure de sauvegarde - Demander les comptes rendus de test de continuité d'activité - **Tester** le PCA, et tester la procédure de sauvegarde

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Gestion de crise/ gestion des failles de sécurité	- S'assurer que l'entreprise a un système de réaction suite à une faille de sécurité	- Existence d'un processus de gestion de crise - Système de supervision des SI	- Crise non contrôlée : impact financier et risque d'image - Risque juridique	- Prévoir une procédure de gestion des failles permettant de préserver les preuves de l'évènement, qualifier et corriger, réunir les bons interlocuteurs - Mettre en place des équipes spécialisées comme des centres de supervision de sécurité pour détecter en temps réel les tentatives d'attaque envers les SI - Inclure un volet sécurité au sein de chaque projet - Sensibiliser le service informatique à la transmission rapide de l'intrusion (si des DCP risque d'être atteintes) pour permettre au RT de procéder à l'obligation de notification	- **Analyse**: accéder à la procédure de gestion des failles - Vérifier s'il y a des astreintes - **Interview** avec le RSSI et rencontrer les équipes spécialisées - Interroger le service informatique pour évaluer sa compétence de l'obligation de notification et obtenir éventuellement trace de la sensibilisation

Composante de contrôle interne	Finalités ou objectifs de contrôle	Points de contrôle	Impacts	Bonnes pratiques de contrôle interne	Techniques d'audit
Maintenance/ Support à distance	- S'assurer que l'entreprise fournit un support/assistance sécurisé à ses collaborateurs	- Suivi des opérations de maintenance - Sécurisation de la connexion lors du support - Script de support	- Risque de fuite des données - Impact opérationnel	- Enregistrer les opérations de maintenance - Tableau de bord de suivi des accès à distance - Configurer les outils de manière à recueillir le consentement de l'utilisateur avant la prise en main à distance (par exemple en cliquant sur une icône ou en répondant à un message s'affichant à l'écran) - Permettre à l'utilisateur de pouvoir constater si la prise en main à distance est en cours et quand elle se termine (affichage d'un message à l'écran) - Envoyer une confirmation par mail à la personne à la résolution de la panne - Tenir un suivi des accès à distance - Chiffrer les données de manière sécurisée avant envoi en maintenance externe de toute ressource informatique ou a minima faire signer un engagement de confidentialité au tiers prenant en charge le support	- **Analyse**: - Vérifier l'existence d'une cartographie des incidents rencontrés - Accéder au suivi des opérations de maintenance et de supports à distance - **Tester** le support

CONCLUSION

La clé de la mise sous contrôle de la conformité est une gouvernance fine et bien orchestrée, intégrant les notions de transversalité, de coopération, de complémentarité entre acteurs et de priorisation des actions.

Au regard des aspects techniques du règlement à maitriser, des travaux d'adaptation à réaliser d'ici mai 2018, beaucoup d'entreprises en particulier pourraient ne pas parvenir à mettre en place ces changements seules. Inévitablement se posera la question de l'accompagnement externe notamment pour réaliser les diagnostics, les revues de conformité voir pour la conduite des missions d'audit sur les traitements et l'avancement des travaux.

CONCLUSION GENERALE

Le GDPR est un texte complexe, difficilement abordable à la fois par les entreprises et par les citoyens. Sa mise en œuvre, nous l'avons démontré, ne sera pas « chose aisée ». Il n'est donc pas étonnant de relever une méconnaissance de ce texte.

Néanmoins pour faire une synthèse très générale de son application, il me parait intéressant de mettre l'accent sur un point majeur sur lequel les entreprises doivent principalement agir pour que le règlement prenne ses racines en profondeur au sein de l'organisation concernée : instaurer une collaboration entre les acteurs de l'entreprise et une coopération entre parties prenantes.

Ainsi la démarche d'audit sera une aide en se centrant notamment sur trois axes d'investigation clés ;

Ainsi, au-delà des aspects méthodologiques, techniques ou juridiques, **la sensibilisation parait être le premier point sur lequel l'entreprise se doit d'agir le plus tôt possible**. La protection des données est à la portée de tous puisque c'est la mauvaise utilisation ou une divulgation par erreur qui porte atteinte aux droits et liberté des individus. D'autre part, cette sensibilisation doit avoir lieu à tous les niveaux hiérarchiques pour prendre en compte le « chainage des responsabilités » et en premier lieu, l'implication du Comex est essentielle.

Par ailleurs, **le DPO apparait comme le « pivot » dans cette vaste organisation** autour de la mise en conformité au GDPR, mais son rôle est voué à l'échec s'il ne s'inscrit pas dans une notion d'équipe. Les difficultés, nous l'avons évoqué, sont telles que, seul, le DPO ne sera pas en capacité d'atteindre les objectifs du GDPR quels qu'ils soient.

La clé de la réussite est de **mettre en place une « communication collaborative » sur l'avancement du projet de mise en conformité au GDPR.**

Des questions restent néanmoins encore en suspens. Le niveau de protection des citoyens sera-t-il plus élevé comme l'affirme le règlement ? La réponse dépendra surtout de la capacité des entreprises à s'approprier l'ensemble de la réglementation.

A l'heure actuelle, le baromètre GDPR sur la maturité des entreprises françaises de mai 2017[91], a permis de démontrer que la maturité des entreprises est relativement faible au regard des travaux réalisés. Mais ce baromètre a surtout pu démontrer que les entreprises ne travaillent pas collectivement. La cause principale est le manque de communication qui peut être expliqué par le fait que l'exécutif lui-même n'est pas impliqué, or c'est grâce à lui que des

[91] Baromètre GDPR, Synthèse du sondage n°1 Brainwave GRC, « La maturité des entreprises françaises face au Règlement Général sur la Protection des Données », mai 2017

actions de sensibilisation de l'ensemble de l'organisation peuvent être organisées. La synthèse du sondage parle même d'une épée de Damoclès pour les entreprises face à la complexité du cadre à venir. Toutefois, il est à noter que la désignation à venir d'un DPO représente un élément encourageant permettant d'apporter un cadre à la communication interne.

Le prochain questionnaire du baromètre est actuellement ouvert, il permettra d'apprécier, nous l'espérons, une belle progression dans ce vaste projet de mise en conformité.

BIBLIOGRAPHIE

I- OUVRAGES

- DESGENS-PASANAU G., *Le correspondant « Informatique et Libertés*, LexisNexis, 2013
- EYNARD J., *Les données personnelles : quelle définition pour un régime de protection efficace ?*, Editions Michalon, 2013
- FOREST D., *Droit des données personnelles*, Lextenso éditions, 2011
- MATTATIA F., *Le droit des données personnelles*, Editions Eyrolles, 2e éd., 2016
- GROSJEAN A., *Enjeux européens et mondiaux de la protection des données personnelles*, Editions Larcier, 2015

II- ARTICLES, CHRONIQUES & DOCTRINE

- ATAYA G., « L'auditeur face au chantier du GDPR », Ouverture sur le Monde, N°008, 4e trimestre 2016
- BARRAU L. et TESSONNEAU A., « Protection des données personnelles et risques juridiques », *Les enjeux des données numériques*, n°147, avril 2013, p. 25BISEUL X., « La conformité, un avantage compétitif », Zdnet, juin 2017
- DESJARDINS C., « Données personnelles : six conseils pour lancer son chantier GDPR », Les échos, février 2017
- FAILLET C., « Le data-driven marketing, qu'est-ce que c'est ? », l'Observatoire Influencia, novembre 2015
- FERRANDON P., « Pourquoi une gouvernance de la donnée ? », JDN, septembre 2016
- GRIGUER M., « Conformité Informatique et Libertés : l'étude d'impact ou l'approche par les risques », Cahiers pratiques, n°4, juillet 2015
- MERMILLIOD C., « Le vol de données et son impact sur l'image des entreprises », Les échos, janvier 2016
- MOURIER E., « Le GDPR comme tremplin vers une gouvernance des données gagnant-gagnant », Les Echos, décembre 2016
- RENARD I., « L'audit et la législation sur les données personnelles ne font pas bon ménage », Droit et informatique La revue, mai 2007
- SCHMIDT S., « Les 3 V du big data : volume, vitesse et variété », JDN, mai 2012
- SOENEN P., « Anticiper la conformité au nouveau Règlement Général sur la protection des données », Tribune Libre, n°008, 4e trimestre 2016
- VALLEE M., « Une éthique des données personnelles doit être le fondement du marketing « data driven » », Les Echos, avril 2016

III- DOCUMENTS DE TRAVAIL

- **Textes de loi**

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Directive 95/46/CE 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
- Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
- Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE
- LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique

- **Travaux divers**

Travaux CNIL

- Les guides de la CNIL
    - Pia-1, La méthode : comment mener une étude d'impact sur la vie privée, juin 2015
    - Pia-2, L'outillage : modèles et bases de connaissances de l'étude d'impact sur la vie privée, juin 2015
    - Pia-3, Les bonnes pratiques : mesures pour traiter les risques sur les libertés et la vie privée, 2012
    - Guide CNIL, La sécurité des données personnelles, Edition 2010
    - Guide CNIL, Les transferts de données à caractère personnel hors Union Européenne, novembre 2012
    - Guide CNIL du Correspondant Informatique et Libertés, 2011

- Fiches CNIL
    - Fiche n°2 CNIL « Personnes habilitées, sous-traitants, destinataires des données et tiers autorisés », juillet 2014
    - Fiche n°9 « L'information des personnes », juillet 2014
    - Fiche n°10 CNIL « Sécurité des données », juillet 2014

- « Livres blanc »
    - Livre Blanc, Business&Decision, « GDPR, En route vers la conformité », avril 2017
    - Livre Blanc Deloitte, « GDPR, par où commencer ? », janvier 2017
    - Livre blanc Devoteam « Plan d'action GDPR : Objectif conformité », 3 janvier 2017

- La CNIL en bref, 2016
- CNIL, Règlement européen sur la protection des données : ce qui change, 28 février 2017
- CNIL, Rapports entre l'entreprise et la CNIL : quelles évolutions avec le RGPD ?, rédigé par Clémence SCOTTEZ

Travaux réglementaires

- Avis 4/2007 du Groupe de travail « article 29 » à la Commission sur le concept de donnée à caractère personnel
- Avis 1/2010 sur les notions de «responsable du traitement» et de «sous-traitant»
- Assemblée nationale sur les incidences des nouvelles normes européennes en matière de protection des données personnelles sur la législation française, enregistré à la Présidence de l'Assemblée nationale le 22 février 2017
- Recommendations for a privacy impact assessment for the European Union, PIAF 11-2012

Travaux cabinets & entreprises

- Deloitte, Enjeux Cyber, La face cachée de la cybersécurité, 2016
- EY, « protection des données personnelles : les nouveaux enjeux du règlement européen (GDPR), 2 février 2017.
- Gartner, EU privacy Will Impact Delivery of Your Data Security Product Marketing Messages, 10 mars 2017
- PwC, « Gouvernance des données, mieux maitriser vos données », brochure

Autres travaux

- Baromètre GDPR, Synthèse du sondage n°1 Brainwave GRC « La maturité des entreprises françaises face au Règlement Général sur la Protection des Données », Mai 2017
- CIGREF, Economie des données personnelles, les enjeux d'un business éthique, octobre 2015
- Data protection audit manual, juin 2001
- IIA, GTAG (Guide pratique d'audit des technologies de l'information), « Le management et l'audit des risques d'atteinte à la vie privée », juin 2006

IV- SOURCES ELECTRONIQUES

- Site Web CIL CNRS
  http://www.cil.cnrs.fr/CIL/spip.php?article2707
- Site web de la CNIL
  https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article38
- Site web de l'ANSSI
  http://www.ssi.gouv.fr/
- Site web Deloitte
  https://www2.deloitte.com/fr/fr.html
- Site Légifrance
  https://www.legifrance.gouv.fr/
- Site IIA
  https://na.theiia.org/Pages/IIAHome.aspx

GLOSSAIRE

Règlementation données personnelles

Accountability : Principe de responsabilisation du responsable de traitement qui devra documenter l'ensemble des activités mises en œuvre pour assurer la conformité au règlement dans le but de pouvoir démontrer à tout moment sa conformité et plus particulièrement en cas de contrôle de la CNIL.

Analyse d'impact : Aussi appelée DPIA (Data Protection Impact Assessment). Prévu à l'article 35 du règlement, il s'agit de réaliser une analyse d'impact par traitement et donc d'en étudier les risques afin de pouvoir adapter la protection. Cette analyse est obligatoire en cas de risque élevé pour les droits et libertés des personnes.

BCR : Règles contraignantes d'entreprise qu'une multinationale peut adopter. Elles permettent de porter les transferts internationaux de données personnelles entre les entités du groupe.

CNIL : Commission Nationale de l'Informatique et des Libertés. C'est une autorité administrative indépendante française dont le rôle est de veiller à la protection des droits et libertés des individus face au développement de l'informatique.

Donnée à caractère personnelle : L'article 4 du règlement la définit comme toute information relative à une personne physique identifiée ou identifiable, c'est à dire qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale .

Donnée sensible : Information qui concerne l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle.

DPO : Acronyme qui désigne le Data Protection Officer ou Délégué à la Protection des Données (DPD). Il s'agit de la personne chargée de la protection des données et de la règlementation applicable au sein d'une entreprise. Il remplacera le CIL à compter de l'application du règlement. Ses nouvelles missions sont détaillées à l'article 38 et 39 du règlement.

GDPR (General Data Protection Regulation) : Terme anglais utilisé pour désigner le Règlement Européen sur la Protection des Données qui sera le nouveau cadre légal renforçant la protection des données. D'application directe à compter du 25 mai 2018, il entrainera l'abrogation de la directive de 1995 et une importante adaptation de la loi Informatique et Libertés de 1978.

Personne concernée : Personne à laquelle se rapportent les données qui font l'objet du traitement.

Privacy by design : Définit à l'article 25 du GDPR, le concept signifie protection des données dès la conception, c'est la mise en œuvre des mesures techniques et organisationnelles appropriées dès la conception du produit (par ex du logiciel) pour permettre une conformité au règlement le plus tôt possible.

Privacy by default (protection des données par défaut) : C'est la mise en œuvre par le responsable de traitement de mesures techniques et organisationnelles appropriées afin de traiter les seules données nécessaires au regard de la finalité du traitement.

Responsable de traitement : Personne qui va déterminer à quoi va servir le traitement (finalités) et la manière dont on va atteindre l'objectif fixé (moyens). Le règlement a introduit la notion de responsables conjoints de traitement dans un cas ou plusieurs responsables de traitement détermineraient ensemble les finalités et les moyens d'un traitement.

Sous-traitant : Prestataire de service qui s'engage contractuellement à exécuter un travail pour le compte du responsable de traitement qui n'a pas le temps ou les moyens de faire lui-même.

Traitement de données à caractère personnel : Tout procédé utilisé sur les données personnelles en vue de les collecter, de les enregistrer, de les organiser, de les modifier ou de les transférer.

Informatique et Sécurité

Anonymisation : Processus consistant à supprimer tout caractère identifiant à un ensemble de données.

Base de données : Outil permettant de stocker et d'organiser des données et de les rendre facilement accessibles.

Big Data ou données massives : il n'existe pas de définition universelle du big data. Il désigne un ensemble de données très volumineux qui nécessitent, pour pouvoir être traitées, l'utilisation d'outils puissants, les outils classique de gestion de bases de données ne pouvant le permettre. Le Big Data pose aujourd'hui de nombreuses interrogations face à la protection des données personnelles.

Biométrie : Système d'identification des individus grâce à leurs caractéristiques physiques.

Chiffrement : Aussi appelé cryptage, procédé cryptographique qui permet de garantir la confidentialité d'une information.

Data-driven marketing : ou « Marketing éclairé par les données », consiste à structurer et analyser les données dans le but de comprendre les comportements des consommateurs et de répondre à leurs attentes.

Data mining : Ensemble de techniques permettant de manière automatique d'établir des relations complexes à partir d'un volume important de données.

Objet connecté : Objet équipé de capteurs permettant de faire passer des informations grâce à la connexion à un réseau plus large (internet des objets).

Opt in : Politique de collecte des données personnelle nécessitant le consentement préalable de l'individu.

Opt out : Politique de collecte des données personnelle basé sur le consentement implicite de la personne.

Privacy Child : Mécanisme d'auto-certification reconnu par la Commission européenne pour les entreprises établies aux États-Unis, offrant un niveau de protection adéquat aux données à caractère personnel transférées depuis l'UE vers des entreprises établies aux États-Unis.

Profilage : Utilisation des profils consommateurs à des fins marketing et commerciales.

Prospection commerciale : Action de recherche de nouveaux clients.

Pseudonymisation : Processus consistant à remplacer un identifiant ou plus généralement des données personnelles par un pseudonyme.

Sécurité logique : Utilisation de logiciels pour assurer la sécurité des données.

Sécurité physique : Utilisation de protections permettant de contrôler les accès aux données ou de se prémunir contre tout risque de catastrophe naturelle.

ANNEXES

Annexe n°1 : Articles complémentaires

Dérogation au principe du consentement : Art 7 de la loi 78-17 (repris par l'article 6 du GDPR)

1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:
a) la personne concernée a **consenti au traitement de ses données à caractère personnel** pour une ou plusieurs finalités spécifiques;
b) le traitement est **nécessaire à l'exécution d'un contrat** auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;
c) le traitement **est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis;
d) le traitement est **nécessaire à la sauvegarde des intérêts vitaux de la personne concernée** ou d'une autre personne physique;
e) le traitement est **nécessaire à l'exécution d'une mission d'intérêt public** ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;
f) le traitement est **nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers**, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant..

Exceptions au principe d'interdiction attaché aux données sensibles : Article 8.2 de la loi n°78-17 (repris par l'article 9 du GDPR)

1. « Les traitements pour lesquels **la personne concernée a donné son consentement exprès**, sauf [exception légale] ;
2. Les traitements **nécessaires à la sauvegarde de la vie humaine** mais auxquels la personne concerné [est dans l'incapacité juridique ou matérielle de consentir] ;
3. Les **traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical**
- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme,
- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité

- et qu'ils ne portent que sur des données non communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
4. **Les données à caractère personnel rendues publiques par la personne concernée** ;
5. Les traitements **nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice** ;
6. Les traitements **nécessaires aux fins de suivi médical des personnes** ;
7. Les **traitements statistiques réalisés organismes statistiques légalement habilités** ;
8. Les traitements **nécessaires à la recherche, aux études et évaluations dans le domaine de la santé** (chapitre IX de la loi n°78-17) ;
9. Les traitements justifiés par **l'intérêt public** et autorisés par la CNIL ;
10. Les traitements de santé gérés par des organismes ou les services chargés d'une mission de service public visant à **répondre en cas de situation d'urgence à une alerte sanitaire**

Cas de désignation obligatoires du DPO : Art. 37 du GDPR

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:
a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;
b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement 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; ou
c) 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.

La notion de « grande échelle » apparaissait floue, c'est pourquoi le G29 est venu donner son interprétation. Il recommande de prendre en compte les facteurs suivants :

- le nombre de personnes concernées ;
- le volume de données et/ou le spectre des catégories de données ;
- la durée ou la permanence de l'activité de traitement ;
- l'étendue géographique de l'activité de traitement.

Ainsi, le G29 apporte une large interprétation étendant au maximum les cas de désignation.

Cas droit à l'effacement des données : Art 17 GDPR

1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du

traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:
a) les données à caractère personnel ne sont **plus nécessaires au regard des finalités** pour lesquelles elles ont été collectées ou traitées d'une autre manière;
b) la personne concernée **retire le consentement sur lequel est fondé le traitement**, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;
c) la personne concernée **s'oppose au traitement** en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;
d) les données à caractère personnel ont fait l'objet d'un **traitement illicite**;
e) les données à caractère personnel doivent être effacées **pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre** auquel le responsable du traitement est soumis;
f) les données à caractère personnel ont été **collectées dans le cadre de l'offre de services de la société de l'information** visée à l'article 8, paragraphe 1.

Annexe n°2 : Modèle de fiche à porter au registre

Modèle de fiche à porter au registre	
Traitement n°1	Application de gestion des CIL
Nom et adresse du responsable du traitement :	Commission Nationale de l'Informatique et des Libertés, 8 rue Vivienne - CS 30223, 75083 Paris
Date de mise en oeuvre :	20/10/2005
Finalité principale :	Gestion des Correspondants Informatique et Libertés[1]
Détail des finalités du traitement	▪ Instruction des désignations ; ▪ Actualisation du profil des CIL ; ▪ Edition de la liste des CIL.
Service chargé de la mise en œuvre	Service des Correspondants Informatique et Libertés
Fonction de la personne ou du service auprès duquel s'exerce le droit d'accès	Service des Correspondants Informatique et Libertés
Catégories de personnes concernées par le traitement	Les correspondants informatique et libertés (ci-après CIL), c'est-à-dire les personnes désignées dans les conditions prescrites par le titre III du décret n° 2005-1309 du 20 octobre 2005, pris pour application de la loi « informatique et libertés », et qui assurent les missions définies à l'article 22 de la loi précitée.

[1] Pour information, le détail des informations relatives aux CIL, tel que leurs coordonnées (numéros de téléphone, l'adresse e-mail…), sont traitées dans une autre application ayant notamment pour objet la gestion des usagers en contact avec la CNIL.