FACULTÉ DE DROIT
ET DE SCIENCE POLITIQUE

PROTECTION DES DONNEES PERSONNELLES

L'APPLICATION DU RGPD AU SEIN DES ENTREPRISES D'ASSURANCE

Master II Droit des assurances

Année universitaire 2017 - 2018

Mémoire rédigé par

Marion Cura

Sous la direction de

Anne Pélissier

Professeur des universités

Les opinions exprimées dans ce mémoire sont propres à leur auteur et n'engagent pas l'Université de Montpellier I.

Remerciements

Je tiens à remercier vivement Madame le Professeur Anne Pélissier, d'une part pour la confiance qu'elle m'a accordé lors du choix des élèves intégrant son Master, d'autre part pour son accompagnement, tant pédagogique que moral, au sein de l'année universitaire. Je salue l'admiration qu'elle suscite en nous, son parcours et la qualité de la formation dont nous avons pu bénéficier grâce à elle.

J'adresse également mes remerciements à Madame Mercedes Paraire, pour m'avoir reçue en alternance au sein du service « Direction et Coordination des affaires juridiques Vie » dans l'entreprise Aviva à Bois-Colombes, pour sa disponibilité et sa gentillesse, ainsi que pour les sujets très intéressants sur lesquels elle m'a donné l'occasion de travailler.

Je remercie sincèrement mon équipe du pôle excellence technique vie chez Aviva, Madame Christine Pairamian, Messieurs Christophe Gonnet et Laurent Robert, qui ont répondu à toutes mes questions, m'ont accompagné dans mon intégration, et ont continué à m'épauler toute l'année en entreprise.

Je tiens aussi à remercier tout particulièrement Madame Anne Goliro, de la direction conformité et du contrôle interne chez Aviva, spécialiste en protection des données personnelles, qui a eu la gentillesse de répondre à mes demandes d'éclaircissements sur certains éléments techniques du règlement général sur la protection des données personnelles et de lire mon mémoire.

Enfin, je remercie mes camarades de classe, avec qui j'ai eu la chance de passer la meilleure année dans mes études supérieures, non seulement par la cohésion qui a pu régner tout au long de l'année, mais également pour le soutien dans les travaux de groupe, les échanges au sujet de nos mémoires respectifs, qui n'ont fait que renforcer nos liens, et pour certains d'entre nous, ont créé de réelles amitiés.

Table des matières

Liste des abréviations

AAI ..... Autorité Administrative Indépendante
AERAS ..... s'Assurer et Emprunter avec un Risque Aggravé de Santé
AFP ..... Agence France Presse
APEC ..... Asian-Pacific Economic Cooperation
BCR ..... Binding Corporate Rules
CIL ..... Correspondant Informatique et Libertés
CJUE ..... Cour de Justice de l'Union Européenne
CNIL ..... Commission Nationale de l'Informatique et des Libertés
COFRAC ..... Comité Français d'Accréditation
DPO ..... Data Protection Officer
DPD ..... Délégué à la Protection des Données
EIVP ..... Etude d'Impact sur la Vie Privée
NS ..... Norme Simplifiée
OCDE ..... Organisation de Coopération et de Développement Economiques
ONU ..... Organisation des Nations Unies
PIA ..... Privacy Impact Assessment
PME ..... Petite(s) Moyenne(s) Entreprise(s)
RGPD ..... Règlement Général sur la Protection des Données personnelles
SAFARI ..... Système Automatisé pour les Fichiers Administratifs et le
..... Répertoire des Individus
UE ..... Union européenne

Les articles, lorsqu'ils sont cités sans source, émanent du RGPD.

Introduction : L'historique de la protection des données personnelles

Le règlement général sur la protection des données personnelles touche sans exception toutes les organisations, peu importe le domaine, qui sont susceptibles de connaître les données personnelles des personnes physiques au sein de l'Union européenne. Cette étude s'axe sur son application dans le milieu des assurances.

Ce règlement est perçu comme une véritable révolution en matière de protection des données personnelles. Pourtant, des mesures antérieures ont déjà été mises en place ; la France est d'ailleurs un pays précurseur. Il est cependant important d'observer l'évolution de cette protection pour la comprendre, et pour s'apercevoir à quel point une harmonisation sur le plan européen s'avérait nécessaire, ce qui a été réalisé grâce au règlement.

Section 1 : L'encadrement de la circulation des données personnelles avant le RGPD

Avant le RGPD, la circulation des données personnelles était déjà encadrée, mais la pluralité des règlementations existantes dénotait, malgré une volonté déjà bien affirmée de protéger les citoyens, une certaine désorganisation.

I. La protection des données personnelles d'un point de vue national

A) Les prémices d'une règlementation sur la protection des données personnelles

Dans les années 70, le projet SAFARI émanant du gouvernement, prévoit d'identifier chaque citoyen par un numéro et d'interconnecter sur la base de cet identifiant tous les fichiers de l'administration. Cette idée provoque une vive réaction de l'opinion publique, faisant émerger la volonté du respect de la vie privée et des libertés individuelles.

Le 6 janvier 1978, la loi « Informatique et libertés » annonce les prémices en matière de protection des données personnelles. Elle est considérée comme une étape majeure puisqu'elle permet l'instauration d'une base solide en la matière et reste inchangée pendant plusieurs décennies.

Tout d'abord, cette loi institue la CNIL, première autorité administrative indépendante en France, et principal acteur de la protection des données personnelles ; elle précise les pouvoirs de contrôle et de sanction de cette dernière. Ensuite, elle définit les principes à respecter lors de la collecte, du traitement et de la conservation des données personnelles. Enfin, elle définit les droits des personnes sur leurs données.

B) La CNIL

Les cinq missions de la CNIL sont décrites à l'article 11[1] de la loi « Informatique et libertés », ainsi elle informe toutes les personnes concernées et tous les responsables de traitement de leurs droits et obligations (1) ; elle veille à ce que les traitements de données à caractère personnel soient mis en œuvre (2) ; elle dispose d'un pouvoir de contrôle et de sanction relatif aux responsables des traitements (3) ; elle se tient informée de l'évolution des technologies de l'information (4) ; elle peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application de la loi Informatique et libertés et des dispositions relatives à la protection des données personnelles (5).

Il est à noter que la CNIL est une des rares AAI à disposer d'un pouvoir de sanction.

Finalement, inspirant de nombreux pays, le modèle français a été un pays pionnier en matière de protection des données personnelles.

II. La protection des données personnelles aux niveaux européen et international

A) La protection des données personnelles au niveau européen

La directive 95-46 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 a été transposée en France par la loi du 6 août 2004[2]. Ainsi se forme un socle commun à tous les Etats membres en matière de protection des données personnelles.

[1] La loi dite « Informatique et libertés » a été modifiée le 20 juin 2018, les missions de la CNIL sont passées de quatre à cinq (1° à 5°)

[2] 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

Cette directive prévoit en son article 29 l'institution d'un groupe de travail appelé G29, constitué de membres des autorités de chaque pays, qui est l'équivalent de la CNIL mais au niveau européen ; il s'agit en effet d'un organe consultatif européen indépendant ayant plusieurs missions. Il a un rôle d'harmonisation au niveau de l'UE, et contribue, par ses recommandations, à l'élaboration des normes européennes. Il conseille également la Commission européenne et rend des avis sur le niveau de protection des pays tiers ne faisant pas partie de l'UE, tels que la Norvège ou l'Islande.

En 2000, la Charte des droits fondamentaux de l'Union européenne prévoit en son article 8 la protection des données personnelles.

Le règlement (CE) n°45/2001 a institué une autorité de contrôle indépendante : le contrôleur européen à la protection des données. Cette autorité de contrôle indépendante a pour mission de contrôler et assurer la protection des données personnelles et de la vie privée au sein des institutions et des organes de l'UE en préconisant les bonnes pratiques. Elle joue également un rôle d'expert auprès de la CJUE afin de contribuer à l'interprétation de la législation en matière de protection des données personnelles.

Le Traité de Lisbonne[3], signé le 13 décembre 2007, en accordant de nouveaux pouvoirs au Parlement européen en matière de protection des données, a également permis une clarification du système.

Il est également possible d'ajouter qu'en 2009, l'article 16 du TFUE pose le principe selon lequel toute personne a droit à la protection de ses données à caractère personnel.

B) La protection des données personnelles au niveau international

La Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe, signée le 28 janvier 1981, est le premier texte international à faire directement référence à la protection des données personnelles. Cette Convention a pu être modernisée durant les années suivantes, notamment en 2011, grâce à la reprise de certains concepts importants, qui ont été définis et précisés.

[3] Traité de Lisbonne 2007/C 306/01 modifiant le traité sur l'Union européenne, le traité instituant la Communauté européenne et certains actes connexes, signé à Lisbonne le 13 décembre 2007

L'OCDE, dans une recommandation du 23 septembre 1980, a adopté des lignes directrices sur la protection de la vie privée et les flux transfrontières de données. L'ONU a adopté des lignes directrices similaires par une résolution du 14 décembre 1990, l'accent étant cette fois-ci porté de manière plus importante sur la protection liée aux données sensibles. Ces deux organisations ont ainsi établi de grands principes tels que le consentement de la personne concernée ou bien l'obligation de collecte loyale et licite.

Enfin, sous l'impulsion des autorités de protection des données telle que la CNIL, une résolution a été votée à l'unanimité lors de la 31ème conférence[4] internationale des commissaires à la protection des données. Cette résolution vise à établir un ensemble de principes communs en réaction à l'évolution technologique des dernières années.

Si les sources internationales n'ont pas réellement eu un impact sur le modèle français, elles ont tout de même permis une certaine harmonisation au sein des pays, particulièrement ceux ne faisant pas partie de l'UE.

Section 2 : L'entrée en vigueur du RGPD

L'adoption du RGPD a pour but de créer un ensemble de règles uniformes au sein de l'UE, en renforçant la confiance des organismes et des citoyens dans le numérique.

Initialement, l'idée d'un nouveau cadre règlementaire s'agissant de la protection des données à caractère personnel est née en 2012, du côté de Viviane Reding, alors Commissaire européenne à la Justice, aux Droits fondamentaux et aux Citoyens.

C'est l'affaire Snowden[5] en 2013 qui a donné la réelle impulsion à la mise en place du RGPD. Ce scandale ayant révélé l'espionnage de millions de citoyens a rendu évidente la question de la révision du système de protection des données personnelles et une unification des lois déjà existantes sur les données est apparue politiquement nécessaire. En effet, le respect de la vie

[4] Conférence internationale des commissaires à la protection des données et à la vie privée, Résolution sur des normes internationales de vie privée, 4-6 novembre 2009

[5] Edward Joseph Snowden est un lanceur d'alerte américain, ancien employé de la CIA (Central Intelligence Agency) et de la NSA (National Security Agency) ; il a révélé les détails de plusieurs programmes de surveillance de masse américains et britanniques

privée est un droit fondamental européen, jouissance inaliénable et inviolable de chacun des citoyens.

Trois ans après, le règlement européen n°2016/679 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 voit le jour. Celui-ci s'applique depuis le 25 mai 2018. Le texte abroge la directive de 1995[6], et donc une partie de la loi « Informatique et libertés[7] ». De nombreuses formalités préalables (déclarations, autorisations), notamment auprès de la CNIL, vont disparaître. En contrepartie, la responsabilité des organismes sera renforcée ; ils devront en effet assurer une protection optimale des données en fonction des risques pour les données et libertés des personnes physiques, et être en mesure de la démontrer en documentant leur conformité, et les réévaluer régulièrement[8].

Ce règlement impose donc aux entreprises et administrations de nouvelles obligations, ainsi qu'une modification profonde de leur organisation et de leurs procédures en matière de traitement des données à caractère personnel. Il vise à renforcer l'importance de la protection des données auprès de ceux qui les traitent et à responsabiliser tous les professionnels concernés.

Quels sont les impacts du règlement général sur la protection des données personnelles au sein des entreprises d'assurance en France ?

Ce règlement vient modifier les règles de fonctionnement en matière de protection des données qui existaient auparavant en rappelant d'anciens principes tout en venant en imposer de nouveaux (Chapitre 1), c'est pour cela que l'application en est progressive mais requiert une conformité irréprochable, qui nécessite de nombreuses procédures à mettre en place pour les entreprises d'assurance, impactant sur leur fonctionnement (Chapitre 2).

[6] Directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 « *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* »

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

[8] Le délai maximum étant tous les trois ans, mais l'idéal d'après la CNIL étant une réévaluation annuelle

Chapitre 1 : L'analyse du RGPD

Section 1 : Les enjeux et apports du RGPD

Le RGPD vient rappeler certains principes et pose de nouveaux enjeux pour les responsables de traitement.

I. Le RGPD, des enjeux ambitieux

Le RGPD vient donner un socle commun au niveau européen pour la protection des données à caractère personnel. En effet, la Directive de 1995[9], si elle poursuivait le même objectif, apparaissait plus fragmentée ; on peut ainsi dire qu'on passe de la fragmentation à l'harmonisation avec ce règlement.

Les principes déjà existants sont confirmés, pour cela le règlement reprend certaines notions clés présentes dans la Directive antérieure, telles que les données personnelles[10] ou le responsable du traitement[11]. Les principes fondamentaux sont rappelés, tels que la finalité, la pertinence, la proportionnalité, la confidentialité, la transparence, la durée de conservation, la loyauté ou encore la sécurité. Il faut souligner que les droits des personnes sont indéniablement mis en avant et renforcés, tels que le droit d'accès, le droit d'être informé, de rectification, de limitation et d'opposition, avec l'ajout de nouveaux droits qui sont la portabilité et le droit à l'oubli. Enfin, une architecture institutionnelle est mise en place : les autorités de protection des données nationales coopèrent entre elles.

Un des enjeux est évidemment d'encadrer la circulation des données personnelles et de limiter leur diffusion et leur conservation, afin d'assurer une protection pour les citoyens de l'UE et une uniformisation de l'application des principes de protection des données personnelles dans l'UE.

[9] Directive 95/46/CE sur la protection des données personnelles

[10] Les données personnelles sont toute information se rapportant à une personne physique identifiée ou identifiable

[11] Le responsable de traitement est la personne physique ou morale, l'autorité publique, le service ou autre organisme qui, seul ou conjointement avec d'autres intervenants, détermine les finalités et les moyens du traitement

Les formalités déclaratives à la CNIL en l'absence de CIL sont supprimées, mais apparait cependant un renforcement de la responsabilité des entreprises (*accountability*[12]).

Enfin, une augmentation des sanctions administratives est prévue en cas de non-respect du règlement.

Il s'agira pour l'entreprise d'assurance d'être en conformité au règlement sur tous points de vue, afin de renforcer la confiance des clients pour la protection de leurs données, ce qui passe par un code de conduite par secteur d'activités.

II. Les apports principaux du RGPD

Si le RGPD rappelle certains éléments, il vient consacrer certaines notions, obligations et droits également.

A) Des notions nouvelles

Tout d'abord, la nouveauté principale du RGPD concerne son champ territorial ; en effet, selon l'article 3, « *Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union.* » Les entreprises, pour toutes les personnes physiques dans l'UE susceptibles d'être concernées par la protection des données, sont soumises au règlement, peu importe où se trouve leur siège. De même, les sous-traitants sont également concernés, ce qui n'était pas le cas auparavant.

Il est également possible de souligner que de nouveaux instruments juridiques sont présents pour assurer la conformité, et seront développés ci-après (chapitre 2 - section 1).

De plus, un acteur essentiel apparait dans le RGPD : le comité européen de la protection des données[13]. Il veille à l'application cohérente du règlement. La notion d'autorité chef de file[14] apparaît aussi dans le RGPD, elle coopère avec les autres autorités de contrôle concernées. Des

[12] L'*accountability* désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données

[13] Article 68 : Comité européen de la protection des données

[14] Article 60 : Coopération entre l'autorité de contrôle chef de file et les autres autorités de contrôle concernées

lignes directrices[15] du G29 ont été adoptées à ce sujet. Apparaissent également des mécanismes de contrôle de cohérence[16].

Finalement, une certaine gouvernance européenne s'installe avec ce règlement, ce socle commun permettra aux pays membres d'être sur un même pied d'égalité en matière de protection des données à caractère personnel.

B) De nouveaux droits pour les personnes

Certains droits existaient déjà pour les personnes, comme le droit d'accès[17] de la personne concernée, le droit de rectification[18] ou encore le droit d'opposition[19] au traitement des données. Le RGPD vient cependant consacrer deux nouveaux droits très importants : le droit à l'oubli et le droit à la portabilité.

Concernant le droit à l'oubli[20], si cette notion existait déjà dans le cadre de la convention AERAS[21] depuis peu, il s'entend différemment dans le RGPD. En effet, s'il autorise à ne pas déclarer d'anciennes pathologies sous certaines conditions pour l'un, il prescrit une durée de conservation limitée des données pour l'autre, sur certains fondements juridiques du traitement (consentement et intérêt légitime notamment).

Pour ce qui est du droit à la portabilité des données[22], celui-ci permet, lorsqu'une personne a transmis des données à caractère personnel à une organisation, de demander à récupérer toutes ses données sur un format exploitable, et ainsi pouvoir les transmettre, si elle le souhaite, à une autre organisation, si le traitement est fondé sur le consentement ou sur un contrat.

---

[15] https://www.cnil.fr/sites/default/files/atoms/files/wp244rev01_fr.pdf

[16] Article 63 : Mécanisme de contrôle de la cohérence

[17] Article 15 : Droit d'accès de la personne concernée

[18] Article 16 : Droit de rectification

[19] Article 21 : Droit d'opposition

[20] Article 17 : Droit à l'oubli

[21] Avenant à la Convention AERAS du 2 septembre 2015**,** Loi n°2016-41 du 26 janvier 2016 de modernisation de notre système de santé, Décret n° 2017-173 du 13 février 2017 précisant les modalités d'information des candidats à l'assurance-emprunteur lorsqu'ils présentent du fait de leur état de santé ou de leur handicap un risque aggravé

[22] Article 20 : Portabilité des données

D'autres droits sont également consacrés, tels que le droit à la limitation du traitement[23], ou le droit de ne pas être soumis à une décision automatisée, dont le profilage[24].

C) Des nouvelles obligations pour les entreprises

Auparavant, les entreprises devaient effectuer des déclarations et obtenir des autorisations auprès de la CNIL sur certains traitements à risque[25]. A présent, elles n'ont plus cette contrainte de rendre systématiquement des déclarations et d'obtenir des autorisations, mais en revanche elles doivent être prêtes, à tout moment, à se faire contrôler par la CNIL.

Les obligations nouvelles imposées par le RGPD semblent désormais plus difficiles à satisfaire ; d'une part elles sont renforcées, mais d'autre part il y a un renversement de la charge de la preuve en ce que ce n'est plus aux organismes d'envoyer leurs déclarations ou demande d'autorisation, et à la CNIL de prouver qu'il y a un non-respect quelconque, mais c'est aux entreprises à présent de démontrer qu'elles sont en conformité au régulateur par rapport aux risques et qu'elles effectuent régulièrement des réévaluations[26].

Depuis le 25 mai 2018, les entreprises ont donc un rôle actif dans la démonstration de leur conformité au RGPD ; cette conformité implique de nombreuses obligations, certaines déjà existantes et d'autres nouvelles.

Section 2 : Les principes directeurs de protection des données personnelles

Le RGPD poursuit une volonté d'harmoniser la règlementation au sujet de la protection des données à caractère personnel dans les pays membres de l'UE ; pour cela, différents principes doivent être respectés au sein des entreprises d'assurance françaises, qui sont soumises à ce règlement.

---

[23] Article 18 : Droit à la limitation du traitement

[24] Article 22 : Décision individuelle automatisée, y compris le profilage. – Une décision automatisée est une décision prise à l'égard d'une personne, par le biais d'algorithmes appliqués à ses données personnelles, sans qu'aucun être humain n'intervienne dans le processus. Le profilage est un traitement utilisant les données personnelles d'un individu en vue d'analyser et de prédire son comportement

[25] L'ancien article 25 de la loi dite « Informatique et libertés » prévoyait une autorisation de la part de la CNIL par exemple pour les données sensibles, les numéros de Sécurité sociale, les infractions

[26] Article 24 : Responsabilité du responsable du traitement

I. Le principe d'*accountability*

Originaire des pratiques anglo-saxonnes, le concept d'*accountability* fait son apparition au titre du nouveau règlement, à l'article 24 et au considérant 74, « *il y a lieu d'instaurer la responsabilité du responsable du traitement pour tout traitement de données à caractère personnel qu'il effectue lui-même ou qui est réalisé pour son compte* ». Ainsi, la CNIL traduit ce principe comme « *l'engagement responsable* », qui oblige les entreprises à mettre en œuvre des mécanismes et des procédures internes en fonction des risques sur la vie privée, permettant de démontrer le respect des règles relatives à la protection des données, et par conséquent leur conformité au règlement.

A) La priorité donnée à l'anticipation

Si le régime juridique antérieur relevait principalement des formalités préalables, en effet l'article 22 de la loi informatique et liberté de 1978 prévoit, sauf cas particuliers, *« les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés* », le RGPD vient renverser la charge de la preuve en supprimant cette obligation de déclaration si les traitements ne constituent pas un risque réel pour les personnes concernées. Il impose en revanche que l'entreprise puisse, à tout moment, démontrer sa conformité en cas de contrôle par une autorité de contrôle nationale. Désormais, c'est donc en amont du traitement des données que le responsable devra documenter ses actions pour être en conformité au RGPD tout au long de la vie du traitement. La priorité est accordée à l'anticipation, c'est un changement profond de logique, qui suscite pour l'entreprise une philosophie d'autorégulation.

B) Un principe englobant de nombreuses mesures

Ce principe d'*accountability* induit donc de nouvelles obligations à la charge du responsable de traitement. Premièrement, le responsable du traitement doit respecter les règles relatives à la protection des données (article 5[27]). Ensuite, il est tenu de rédiger des procédures simples et transparentes (article 12[28]) concernant l'application de ces principes et l'exercice des droits

[27] Article 5 : Principes relatifs au traitement des données à caractère personnel

[28] Article 12 : Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée

conférés aux personnes. Les informations délivrées aux personnes concernées (Articles 12[29], 13[30] et 14[31]) doivent être conformes aux exigences du règlement, c'est-à-dire concises, transparentes, compréhensibles et aisément accessibles pour les personnes concernées. De plus, il devra respecter les principes de *privacy by design* et *privacy by default* (article 25[32]) ; le *privacy by design* désigne le fait que le respect de protection des données doit être pris en compte dès la conception d'un produit ou d'un service technologique, et le *privacy by default* s'axe sur le traitement des données lui-même, c'est-à-dire que l'entreprise doit ainsi garantir par défaut le plus haut niveau de protection des données. Par ailleurs, le responsable de traitement est soumis à une obligation de documentation (article 35[33]) signifiant l'élaboration d'un travail préparatoire conséquent. Enfin, il doit tenir un registre interne (article 30[34]) qui recense toutes les activités de traitement. Il englobe donc le registre de traitement, l'étude d'impact sur la vie privée, la notification des violations de données à la CNIL et la nomination d'un délégué à la protection des données, qui seront abordées lors de la section suivante (Chapitre 2, Section 1 : Les mesures devant être mises en place par les entreprises d'assurance).

Les entreprises d'assurance devront donc mettre en œuvre des mesures techniques et organisationnelles pour s'assurer de l'application des principes de protection des données personnelles. En effet, il faudra être en mesure de démontrer que les traitements respectent les principes précités et que les mesures mises en œuvre sont réexaminées et actualisées si nécessaire.

Les responsables de traitement doivent donc adopter une véritable démarche de responsabilisation et d'éthique, puisqu'elles deviennent de véritables acteurs de la régulation des données personnelles.

[29] Article 12 : Transparence des informations et des communications et modalités de l'exercice des droits de la personne concernée

[30] Article 13 : Informations à fournir lorsque les données à caractère personnel sont collectées auprès de la personne concernée

[31] Article 14 : Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée

[32] Article 25 : Protection des données dès la conception et protection des données par défaut

[33] Article 35 : Analyse d'impact relative à la protection des données

[34] Article 30 : Registre des activités de traitement

II. Le principe de finalité

Ce principe contient deux sous-principes : le traitement doit être légal, loyal et transparent, et la finalité doit être limitée.

A) L'exigence de loyauté, légalité et transparence du traitement

Le traitement doit être loyal, légal et transparent ; avant toute collecte et utilisation de données personnelles, le responsable de traitement doit précisément définir l'objectif poursuivi par la mise en place du traitement. Ces objectifs, appelés aussi « finalités », doivent respecter les droits et libertés des individus, notamment l'information sur la finalité. Il va de soi que l'objectif est légitime et compatible avec les missions de l'organisme.

Ainsi, l'entreprise d'assurance pourra se poser les questions suivantes avant toute collecte et utilisation de données personnelles : quel est le fondement juridique du traitement (consentement, contrat, intérêt légitime, obligation légale) ? Est-il légitime au regard des missions et des droits et libertés des personnes ?

B) Une finalité limitée

La finalité du traitement doit être respectée ; il existe une interdiction de traiter ultérieurement les données d'une manière incompatible avec la finalité initiale. Des données collectées dans un but précis, ne peuvent être utilisées dans un cadre différent de celui pour lequel elles ont été recueillies.

Ces données doivent être utilisées selon « l'attendu raisonnable de la personne[35] », c'est-à-dire en fonction de ce à quoi elle peut raisonnablement s'attendre sur l'utilisation de ses données lorsqu'elle les délivre.

III. Le principe de pertinence des données

Deux sous-principes sont inclus dans le principe de pertinence des données : celui de la minimisation et celui de l'adéquation des données.

[35] En ce sens, l'avis WP 217, « *notion of legitimate interests of the data controller* », relatif à la directive 95/46/EC, version anglaise uniquement, https://cnpd.public.lu/content/dam/cnpd/fr/publications/groupe-art29/wp217_en.pdf

A) La minimisation des données

Seules les données strictement nécessaires à la réalisation de l'objectif poursuivi peuvent être collectées. Il faut veiller au caractère sensible de certaines données, c'est-à-dire celles qui concernent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

B) L'adéquation des données

Il faut que les données soient adéquates et pertinentes au regard de l'objectif du traitement. Pour les catégories particulières de données, le traitement par défaut est interdit.

Pour les contrats d'assurance chez les entreprises d'assurance, les traitements de données de santé, du numéro de sécurité sociale, de données d'infractions / condamnations doivent être conformes aux modalités décrites au sein du « Pack de conformité Assurance[36] ». Ces données doivent être exactes, et si possible tenues à jour.

Au sein des entreprise d'assurance, les points d'attention doivent être portés sur le fait que les données ne peuvent servir que pour les finalités définies au moment de leur collecte et des processus permettant la mise à jour de ces données doivent être mis en œuvre. Il ne faut pas collecter certaines catégories de données telles que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophique ou l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

De plus, concernant les données de santé, données d'infraction et numéro de sécurité sociale, il est nécessaire de limiter la collecte et les accès au plus strict nécessaire et de respecter le cadre règlementaire du secteur de l'Assurance, notamment en termes de confidentialité. Enfin, ces données ne peuvent être utilisées dans le cadre de la prospection commerciale.

[36] Ce Pack comprend en particulier la NS-16 (contrat), AU-031 (Numéro SS) et AU-032 (données d'infraction) du site de la CNIL

IV. Le principe de conservation limitée

Les données personnelles collectées ne peuvent être conservées *ad vitam æternam* par les entreprises, elles ne peuvent les garder qu'un temps.

A) L'encadrement de la durée de conservation des données

La durée de conservation des données doit être définie. Effectivement, les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une « *durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont traitées*[37] ».

Cette durée dépend non seulement des différents objectifs, mais elle doit aussi tenir compte des éventuelles obligations légales à conserver certaines données, comme par exemple les délais de prescription du code des Assurances. La conservation d'une même donnée personnelle peut varier en fonction des objectifs poursuivis.

Ces données sont donc conservées pendant une durée limitée. Pendant la durée du contrat, les données sont stockées dans un premier temps en base d'archives courante. Puis, à compter du dénouement du contrat, elles sont transférées dans un deuxième temps sur une base d'archives intermédiaire, où seules certaines personnes habilitées peuvent y accéder, car elles y ont un intérêt, notamment en cas de contentieux ou pour répondre à une demande de l'Administration fiscale. Enfin, elles sont totalement supprimées ou anonymisées[38]. Elles peuvent également être classées dans une base d'archives définitives, mais les entreprises d'assurances ne sont pas concernées.

L'inconvénient est que la durée de conservation n'est pas toujours précisée ou encadrée règlementairement, il appartient donc aux entreprises d'assurance de juger par elles-mêmes du temps de conservation nécessaire. Pour les clients, le délai de conservation en base d'archives courante dure tout au long du contrat. Ensuite, les données passent en base d'archives intermédiaire à compter du dénouement du contrat. Le dénouement du contrat s'entend par l'évènement mettant fin à celui-ci, par exemple un décès ou un rachat total du souscripteur en matière d'assurance vie. Le délai de conservation en base d'archives intermédiaire est de trente

[37] Article 5.1.e) : Principes relatifs au traitement des données à caractère personnel

[38] Considérant 26

ans[39] à compter du décès de l'assuré en matière d'assurance vie par exemple, mais il peut totalement varier, parfois il peut être de deux ans ou de dix ans à compter du dénouement du contrat, et peut s'élever à plus de cent ans, en partant de la souscription du contrat pour certaines compagnies. L'idéal serait que la CNIL fournisse un chiffre indicatif pour les compagnies d'assurance selon les types de contrats, afin de permettre un alignement sur ces durées de conservation qui sont à l'heure d'aujourd'hui totalement disparates.

En matière de données de santé, s'il n'y a pas de conclusion de contrat, la conservation est de deux ans en base d'archives courante et trois ans en base d'archives intermédiaire à des fins probatoires[40]. Les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur son état de santé physique ou mental passé, présent ou futur[41].

B) Les points d'attention

La conservation des données doit être limitée pour une durée nécessaire, tout en respectant la protection des données personnelles. Pour cela, il faut définir et documenter les règles de conservation des données. Chaque entreprise est *a priori* libre de décider du délai de conservation en base d'archive courante et en base intermédiaire, mais si celui-ci paraît trop long au regard des finalités poursuivies, elle devra fournir les justifications nécessaires auprès du régulateur si elle est interrogée, et s'expose, en cas de dérive, à des sanctions. De plus, les données conservées en base d'archives intermédiaire doivent uniquement permettre de faire valoir un droit en justice[42], un tri doit donc être effectué lors du transfert de la base active à la base intermédiaire, pour ne garder que les données indispensables, ce qui peut être très lourd administrativement.

---

[39] Article L114-1 du Code des assurance : « *pour les contrats d'assurance sur la vie, (…) les actions du bénéficiaire sont prescrites au plus tard trente ans à compter du décès de l'assuré* »

[40] En ce sens, NS-016 de la CNIL, « *Passage, gestion et exécution des contrats d'assurance* », https://www.cnil.fr/fr/declaration/ns-016-passationgestion-et-execution-des-contrats-dassurance

[41] Article 4, 15° : Définitions, « *données concernant la santé* » et considérant 35

[42] Par exemple, chez Aviva, pour un contrat d'assurance vie, après un rachat total, l'assuré était décédé ; un héritier désigné en tant que bénéficiaire, trouvant le contrat plusieurs années après a voulu demander le règlement du capital décès. Si aucune donnée n'avait été conservée afin de pouvoir justifier du premier versement, Aviva aurait alors dû effectuer le versement des fonds une seconde fois

Il est également recommandé de prévoir des logiciels d'archivage si nécessaire, ainsi que des logiciels de purge ou d'anonymisation de ces données au sein des entreprises d'assurance, afin de garantir l'effacement ou la non identification automatique des données du client lorsque le délai de conservation est écoulé.

V. Le principe de sécurité

En 2017, la CNIL a effectué 341 contrôles pour vérifier la conformité des entreprises afin de sécuriser les données[43]. Elle reçoit chaque semaine un à deux signalements concernant des failles de sécurité ; ce chiffre ne fera qu'augmenter avec l'entrée en vigueur du RGPD, c'est pourquoi les entreprises doivent avoir une vigilance accrue en la matière.

A) Une mesure préventive

Les données doivent être traitées de façon à garantir une sécurité appropriée afin d'empêcher notamment un traitement non autorisé ou illicite, et la perte, la destruction ou les dégâts d'origine accidentelle.

En fonction des risques sur les droits et libertés des personnes concernées, des mesures techniques ou organisationnelles appropriées doivent être mises en œuvre, afin de garantir l'intégrité et la confidentialité.

Pour les traitements représentant un risque élevé pour les droits et libertés des personnes concernées, il convient de réaliser et documenter une étude d'impact sur la vie privée.

En effet, certains traitements présentent des caractéristiques spécifiques ou nécessitent des mesures particulières. Le recueil de données concernant la santé en fait partie. Pour ce type de données personnelles, une analyse approfondie de la loi informatique et libertés et du règlement est nécessaire pour évaluer et déterminer les mesures à mettre en œuvre. Par exemple, des informations renforcées envers le client seront nécessaires ainsi que son consentement ou son autorisation préalable, une étude sur la protection des données (PIA) est obligatoire et devra être prévue afin de renforcer la sécurité juridique et technique du traitement.

[43] Par exemple, en février 2017, la CNIL, après vérification de conformité, a prononcé une sanction de 100 000 euros à l'encontre de la société Darty pour ne pas avoir suffisamment sécurisé les données de certains clients ayant effectué une demande en ligne de service après-vente

B) L'appel à la sous-traitance

Avec le RGPD, les sous-traitants doivent prendre en compte les principes de protection des données personnelles. Ainsi, ils doivent garantir la sécurité des données traitées[44], et ont une obligation d'assistance, d'alerte et de conseil, notamment sur l'étude d'impact et la violation des données. Désormais, ils ont également l'obligation de tenir un registre[45], et des sanctions[46] peuvent leur être appliquer.

Lorsqu'une compagnie d'assurance fait appel à la sous-traitance, sa responsabilité est susceptible d'être engagée ; l'entreprise doit donc sélectionner un sous-traitant présentant des garanties suffisantes sur le respect des principes de protection des données personnelles. En matière de contractualisation, il faut prévoir et adapter les clauses de protection des données personnelles au contexte de la prestation.

VI. Le principe de respect des droits des personnes

Environ 15% des mises en demeure de la CNIL concernent la défense des droits des personnes.

A) Un large panel de droits

Tout d'abord, le droit d'information incombe au responsable de traitement pour les personnes concernées. En effet, pour être loyale et licite, la collecte des données personnelles doit s'accompagner d'une information claire et simple.

De plus, le consentement doit être requis ; il doit être libre, éclairé et explicite. Cette demande de consentement est formulée en des termes clairs et simples, et est préalable à la collecte des données. Ce consentement est souvent matérialisé par une case à cocher, que ce soit sur papier ou en ligne. Il est notamment requis en cas de collecte de catégories particulières de données, de réutilisation des données à d'autres fins, d'utilisation de cookies pour certaines finalités et pour les mineurs de moins de quinze ans[47], celui des parents est demandé. Avec le RGPD, le

[44] Article 32 : Sécurité du traitement

[45] Article 30, 2° : Registre des activités de traitement

[46] Article 83, 3° : Conditions générales pour imposer des amendes administratives

[47] Le RGPD indique seize ans, mais avec la loi dite « Informatique et libertés », modifiée le 20 juin 2018, cette « majorité numérique » est abaissée à quinze ans

consentement peut désormais être retiré librement. De plus, la preuve du consentement incombe au responsable de traitement.

Parmi les droits des personnes, il y a également le droit d'accès. La personne concernée a le droit d'obtenir la copie de l'ensemble de ses données faisant l'objet d'un traitement. Par exemple, elle pourra contacter l'entreprise d'assurance pour récupérer une copie, et ils ne pourront s'y opposer.

Par ailleurs, le droit de rectification permet à une personne concernée d'obtenir du responsable de traitement la rectification des données qui sont inexactes.

Les personnes ont également un droit d'opposition. C'est-à-dire qu'il est possible de s'opposer à un traitement fondé sur l'intérêt légitime, y compris le profilage, à moins que le responsable de traitement ait des motifs légitimes et impérieux.

Enfin, le droit à la limitation de traitement permet d'obtenir de la part du responsable de traitement l'interruption du traitement dans différents cas : l'exactitude des données est contestée par la personne, le traitement est illicite et la personne demande la limitation, les données sont nécessaires à l'exercice ou la défense d'un droit en justice.

Le droit à la portabilité a aussi été consacré ; il permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers, si ces données sont nécessaires au contrat ou basées sur le consentement.

B) Les points d'attention pour les responsables de traitement

L'ensemble des mentions d'information est à revoir car le RGPD implique des changements, à la fois sur la façon de s'informer et il nécessite aussi des informations supplémentaires.

La mise en œuvre des différents droits des personnes est à intégrer impérativement lors de la conception du nouveau traitement.

Par exemple, au sein des compagnies d'assurance, pour l'organisation de la réponse aux demandes d'exercices des droits, il faut se demander quel service gère les demandes. Le délai de réponse doit être respecté ; comme il est dit « *dans les meilleurs délais* », il faut considérer qu'il y a 1 mois maximum. Le processus de réponses est à organiser et formaliser. Si le

demandeur a plusieurs contrats de types différents[48], vie et dommage, gérés par des services différents, il faut être capable de compléter l'ensemble des données.

Il convient d'attirer également l'attention sur le droit à l'oubli ; les entreprises d'assurance doivent définir, pour tout nouveaux traitement, la durée de conservation et les processus d'archivage, de purge ou d'anonymisation.

VII. Le principe du transfert hors UE

Les responsables de traitements et les sous-traitants peuvent transférer certaines données hors de l'UE, à condition d'assurer un niveau de protection des données suffisant. Le RGPD élargit la gamme d'outils juridiques qui permettent d'encadrer ces transferts.

A) La possibilité du transfert

Le transfert des données personnelles hors de l'UE est possible, sous réserve que le RGPD soit respecté. Tout d'abord, il peut se faire mais seulement dans les pays adéquats (Annexe 1).

De nombreux outils juridiques de transfert peuvent être utilisés ; certains ne nécessitent pas d'autorisation préalable de la CNIL, alors que d'autres le requièrent.

Au préalable, il est conseillé aux organismes de prendre une décision d'adéquation (article 45[49]). Il s'agit d'effectuer un examen global de la législation en vigueur dans un Etat, avant de décider du transfert des données personnelles.

S'il n'y a pas de décision d'adéquation, le transfert de données peut tout de même être possible, grâce à des « garanties appropriées » (article 46[50]). Ces garanties sont constituées pour la plupart par des décisions d'autorités de contrôle.

[48] Par exemple, chez Aviva, des personnes ont demandé à récupérer leurs données personnelles. Le problème étant qu'Aviva vie et Aviva (dommages) sont deux entités distinctes, avec des logiciels de traitement et de gestion des données différents. Il a donc fallu récupérer les données auprès des différents services concernés, ce qui a pris un certain temps et aurait pu être sujet à des sanctions à cause du délai important de réponse. Depuis, des personnes ont été nommées dans les services pour être responsables de la collecte de ces données en cas de demande de la part du client, et un logiciel spécifique a été mis en place.

[49] Article 45 : Transferts fondés sur une décision d'adéquation

[50] Article 46 : Transferts moyennant des garanties appropriées

Certains mécanismes de transfert de données ne nécessitent pas l'autorisation préalable de la CNIL, et d'autres ne peuvent être mis en œuvre sans cette autorisation (Annexe 2).

Parmi ces outils, certains existaient déjà et restent valables pour transférer des données personnelles en dehors de l'UE, telles que les clauses contractuelles types émanant de la Commission européenne, ou les BCR[51], qui doivent être connues et maitrisées, et prévoir des règles contraignantes pour les entreprises responsables de traitement ou leurs sous-traitants, quel que soit leur pays d'implantation, ainsi que pour tous leurs salariés. Ces BCR constituent une alternative aux Clauses Contractuelles Types, puisqu'elles permettent d'assurer un niveau de protection suffisant aux données transférées hors de l'UE.

Il est possible de préciser que l'APEC a adopté une sorte d'équivalent des BCR ; il s'agit d'élaboration de règles internationales en matière de protection de la vie privée (*Cross Border Privacy Rules*), ce qui montre l'importance de cet outil.

D'autres de ces mécanismes ont été instaurés par le RGPD, comme celui de certification approuvée comportant l'engagement des pays hors UE d'appliquer les garanties appropriées, ou un code de conduite respectant l'application des garanties adéquates également.

B) La nécessité du transfert

Par dérogation, le transfert peut s'avérer nécessaire à certaines conditions. Par exemple, à la sauvegarde de la vie de la personne concernée, ou à la sauvegarde de l'intérêt public. Également, s'agissant du respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice.

Le transfert peut également être nécessaire à l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci. De plus, il peut s'avérer indispensable à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable de traitement et un tiers. Par exemple, en matière de contrat d'assistance rapatriement.

[51] Les « *Binding Corporate Rules* », constituent un code de conduite, définissant la politique d'une entreprise en matière de transfert de données personnelles et permet de garantir une protection adéquate pour les transferts depuis l'UE vers des pays tiers à l'UE au sein d'une même entreprise ou d'un même groupe

Chapitre 2 : Les conséquences du RGPD

Section 1 : Les mesures devant être mises en place par les entreprises d'assurance

Il apparait nécessaire pour les entreprises d'organiser le pilotage et la gouvernance de cette conformité dans l'entreprise.

I. La mise à jour des informations en matière de collecte de données

Les articles 12, 13 et 14 du RGPD prévoient une information transparente pour les personnes dont les données sont collectées. Si elle existait déjà avec la loi Informatique et Libertés, elle est renforcée avec le RGPD.

A) Les cas nécessitant une information

Les personnes concernées doivent être informées en cas de collecte directe mais aussi en cas de collecte indirecte des données.

Les collectes directes de données sont celles recueillies directement auprès des personnes par les organismes responsables de traitement, par exemple par un formulaire ou lors de la souscription d'un contrat, et lorsqu'elles sont recueillies via des dispositifs de sécurité, comme les vidéosurveillances ou les systèmes de géolocalisation.

Lorsque les données ne sont pas recueillies directement auprès des personnes, il s'agit de la collecte indirecte. Par exemple, leurs données peuvent être récupérées auprès de partenaires commerciaux ou de sources accessibles au public.

L'information doit se faire, dans le cadre de la collecte, au moment du recueil des données pour la collecte directe, et aussitôt que possible en matière de collecte indirecte, sachant qu'au plus tard elle doit se faire dans le délai d'un mois (sauf exception). Elle doit aussi être faite en cas de modification substantielle ou d'évènement particulier, tel qu'un changement dans les modalités d'exercice des droits.

B) Les informations à délivrer

Malgré l'entrée en vigueur du RGPD, certaines choses ne changent pas. Le responsable du traitement de données doit délivrer l'identité et les coordonnées de l'organisme ; les finalités de la collecte ainsi que le caractère obligatoire ou facultatif du recueil des données doivent être précisés. Les destinataires ou les types de destinataires des données sont mentionnés. La durée de conservation des données ou les critères permettant de la déterminer, ainsi que les droits dont bénéficient les personnes concernées sont également donnés. De plus, la personne doit être informée si ses données sont susceptibles d'être transférées hors UE, et les garanties associées.

Le RGPD instaure de nouvelles exigences s'agissant des informations à délivrer. Les personnes doivent être informées de la base juridique du traitement, c'est-à-dire ce qui autorise légalement le traitement. Elles doivent également savoir qu'elles ont le droit d'introduire une réclamation auprès de la CNIL. Enfin, elles doivent recevoir les coordonnées du DPO de l'organisme, ou à défaut de désignation, d'un point de contact sur les questions de protection des données personnelles.

Les entreprises doivent donc veiller à ce que la totalité des informations soient transmises, de manière aussi concise, simple et précise que possible. Elles doivent réussir à concilier ce nombre relativement important d'informations à transmettre avec la nécessité d'être le plus clair et concis possible, pour ne pas créer la confusion chez les personnes profanes.

II. La création d'un registre de traitement

La tenue d'un registre de traitement est prévue par l'article 30 du RGPD ; il doit pouvoir être communiqué à la CNIL lorsqu'elle le demande, pour pouvoir exercer sa mission de contrôle des traitements de données.

A) Une cartographie des traitements essentielle

Grâce au registre des traitements, il est possible d'identifier les différentes actions à mener pour se conformer aux obligations présentes et futures, puis les classer en fonction des risques que font peser les traitements sur les droits et libertés des personnes concernées.

Afin de mesurer l'impact du RGPD sur les traitements de données à caractère personnel que l'entreprise réalise, il faut recenser de manière précise l'ensemble des traitements réalisés en interne et en externe, par des sous-traitants ou des délégataires de gestion.

L'élaboration de ce registre est intéressante pour les entreprises, car c'est un moment où elles s'interrogent et revoient leurs traitements ; il s'agit d'élaborer une cartographie des traitements mis en œuvre au sein de l'entreprise en matière de collecte, traitement et conservation des données à caractère personnel. Ce registre se constitue en trois étapes : il faut d'abord recenser les informations disponibles dans l'entité au sujet des finalités de traitement et des types de données collectées, puis élaborer la liste des traitements grâce notamment à un tableau de suivi des activités de l'entreprise et des fiches de registre par activité. Enfin, il faut identifier et analyser les risques pouvant peser sur les traitements de données mis en œuvre et élaborer un plan d'action de mise en conformité au RGPD.

La CNIL a mis sur son site un modèle de registre de base[52], dont les entreprises peuvent s'inspirer. Toutefois, il leur est conseillé de l'enrichir avec des mentions complémentaires, pour en faire un outil plus global de pilotage de la conformité.

La tenue du registre doit se faire sous forme écrite, aucune obligation sur le format n'est imposée par le RGPD. Celui-ci peut donc être constitué sous format papier ou électronique.

B) L'utilité de ce registre

D'une part, ce registre est une obligation du RGPD, pour les entreprises responsables de traitement et pour les sous-traitants ; la seule exception est si l'entreprise a moins de 250 salariés, sauf le cas où le traitement est à risque, non occasionnel ou s'il s'agit de données sensibles, où elle devra également tenir un registre.

D'autre part, il est essentiel pour comprendre les flux de données. Ainsi, il est possible de distinguer les catégories de données personnelles traitées, leur finalité, leur temps de conservation et la façon dont elles sont sécurisées, quelles sont les personnes qui y ont accès et celles qui sont en charge de leur contrôle, mais également avec qui elles sont partagées ; c'est la notion de destinataire des données[53].

[52] https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

[53] Article 4, 9° : Définitions, « destinataire »

L'idée selon la CNIL de ce registre est d'en faire un véritable outil de pilotage et de conformité du RGPD. Ce registre doit pouvoir être communiqué à la CNIL lorsqu'elle le demande, pour pouvoir exercer sa mission de contrôle des traitements de données.

III. L'instauration de politiques internes (*policy*)

Le RGPD implique la nomination de personnes spécialisées et capables d'anticiper certains évènements pouvant porter préjudices à la protection des données à caractère personnel des citoyens concernés.

A) Une organisation nécessaire à la protection des données personnelles

Afin de garantir un niveau optimal de protection des données personnelles, il convient de mettre en place des procédures internes garantissant la protection des données à tout moment, en prenant compte des évènements pouvant survenir au cours de la vie d'un traitement. Par exemple, un changement de prestataire ou une faille de sécurité.

Il parait indispensable de former des personnes destinées spécialement à ce traitement. Des formations internes spécifiques à suivre pour les personnes ou collaborateurs traitant les données devraient être proposées, et être obligatoires pour certains d'entre eux.

B) Une procédure nécessitant une rigueur d'application

Cette organisation implique dans un premier temps de sensibiliser et d'organiser la remontée d'information avec les collaborateurs, dans un deuxième temps de prendre en compte cette protection dès la conception d'un traitement ou d'une application (mesures d'informations, durée de conservation, sécurité…). Dans un troisième temps, de traiter les réclamations et demandes des personnes concernées par l'exercice de leurs droits. Dans un dernier temps, d'anticiper les violations de données, notamment en prévoyant, dans certains cas, une notification à l'autorité de la protection des données et aux personnes concernées.

Les entreprises travaillant avec des sous-traitants doivent ajouter ou mettre à jour des clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, confidentialité et protection des données traitées.

IV. L'élaboration d'analyses de risques et analyses d'impact pour certaines données sensibles

L'article 35 du RGPD dispose que lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, il faut mener et documenter une analyse d'impact. Ces analyses d'impact (PIA ou EIVP) doivent impérativement être menées avant la mise en œuvre du traitement.

A) Un instrument juridique fortement conseillé

Une PIA contient une description du traitement étudié et de ses finalités, une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités, et une évaluation des risques pour les droits et libertés des personnes concernées. Ces analyses d'impact sont obligatoires pour les données sensibles, et fortement conseillées dans tous les cas de traitement de données personnelles. Neuf critères[54] sont donnés par le G29, dans ses lignes directrices pour les opérations de traitement qui nécessitent une PIA du fait d'un risque inhérent élevé.

Ces analyses sont mises en œuvre par le responsable de traitement ou le sous-traitant, qui doit prendre conseil auprès du DPO s'il en a été désigné un, et demander l'avis des personnes concernées par le traitement ou leurs représentants lorsque c'est approprié. Le responsable de traitement peut également avoir recours, si besoin, à des experts, des avocats, des techniciens ou sociologues. Il ne sera pas lié par les avis recueillis et pourra décider de ne pas les suivre, mais il devra alors en documenter les raisons.

A titre d'exemple, sont concernés les cas qui entrainent des effets juridiques importants à la suite d'une décision, lorsqu'il s'agit de traitement de certaines données à grande échelle (par exemple, pour un hôpital en matière de données de santé), ou lorsqu'il s'agit d'une surveillance systématique de zone accessible au public.

[54] WP 248, « *Lignes directrices concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement est « susceptible d'engendrer un risque élevé » aux fins du règlement (UE) 2016/679* », https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

B) Le contenu de ces analyses

Ces PIA reposent sur deux piliers : une partie juridique, sur la nécessité et la proportionnalité concernant les principes fondamentaux, se traduisant comme une obligation de résultat, et une partie technique par rapport aux risques sur la sécurité des données, étant une obligation de moyen.

Ces analyses d'impact doivent *a minima* contenir une description du traitement et ses finalités, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ; une évaluation de la nécessité et la proportionnalité des opérations par rapport aux finalités ; une évaluation des risques pour les droits et libertés des personnes concernées ; les mesures envisagées pour faire face aux risques et assurer la sécurité des données à caractère personnel, ainsi que limiter les risques sur les libertés et la vie privée des personnes concernées.

En somme, cette EIVP doit apporter la preuve du respect du règlement. Le G29 rappelle que la réalisation d'impact doit être entendue comme un processus continu tout au long de la vie du traitement et non comme une mesure ponctuelle. Ainsi, cette étude contribue à construire des traitements de données respectueux de la vie privée et permettent de démontrer la conformité du traitement au RGPD.

Le secteur de l'assurance est particulièrement concerné, car les décisions peuvent avoir des effets importants sur les personnes (par exemple, en matière de fraude). Pour les entreprises d'assurance dont les données de santé collectées sont nombreuses, il est nécessaire de mettre en place des analyses d'impact pour ce type de données. Ainsi, en cas de contrôle de la CNIL, il sera possible de montrer cette documentation pour prouver que tout a été mis en œuvre pour prévenir les risques. En pratique, cette étude servira à décrire les mesures mises en place pour prévenir et limiter les risques, et si l'entreprise les jugent satisfaisantes.

V. La nomination d'un délégué à la protection des données personnelles

Le DPO conseille et accompagne les organismes qui le désignent dans leur conformité ; ce statut a été créé par le règlement.

A) Les cas de désignation

La désignation d'un *data protection officer*, en français délégué à la protection des données est obligatoire seulement dans trois cas : s'il s'agit d'un organisme public, ou bien si l'activité de l'entreprise amène à effectuer un suivi régulier et systématique des personnes à grande échelle, ou à traiter des données dites « sensibles » ou relatives à des condamnations pénales et infractions. Cependant, même si l'obligation ne s'impose pas formellement à l'entreprise concernée, il est fortement recommandé de désigner une personne en interne ou en externe chargée de s'assurer de la mise en conformité au RGPD.

Le DPO pourra être recruté par les entreprises en interne, mais aussi en externe, notamment pour les PME, pour ceux qui peuvent avoir une telle qualité, comme les avocats ou les commissaires aux comptes.

Dans la pratique, il est possible d'avoir un DPO mutualisé pour plusieurs entreprises, mais celui-ci doit être facilement accessible en cas de besoin.

Si d'apparence il s'agit d'un nouveau métier, une activité similaire existe déjà : le CIL. Reste à voir si les personnes exerçant cette profession pourront revêtir la casquette de DPO également, ou si des formations seront nécessaires.

B) Le rôle du délégué à la protection des données personnelles

Le délégué à la protection des données a un rôle très étendu en matière de conformité de protection des données au sein de l'entreprise. Ses missions principales sont d'informer et conseiller le responsable de traitement ou le sous-traitant, de contrôler le respect du règlement, de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution, mais aussi de coopérer avec l'autorité de contrôle.

Ainsi, il doit dans un premier temps s'informer sur le contenu des nouvelles obligations imposées par le règlement et les lois locales, sensibiliser ses supérieurs hiérarchiques et l'organisation sur l'impact de ces nouvelles données, aider à réaliser l'inventaire des traitements de données à disposition dans l'entreprise, et enfin piloter la conformité en continu.

Dans un second temps, le DPO va donner des conseils à l'entreprise d'une part, et sera l'interlocuteur de la CNIL d'autre part, notamment en cas de consultation pour un risque élevé

(PIA), ou en cas de violation de données. Ses décisions ne sont ni contraignantes, ni obligatoires. Il informe en interne sur la règlementation, et toute une équipe, en fonction de la taille de l'entreprise, veille à l'application de la règlementation, des risques et de la nouvelle conduite à tenir.

VI. La notification des violations des données personnelles

Selon l'article 33 du RGPD, lorsqu'il a connaissance d'une violation de données ayant un risque élevé pour la personne concernée, le responsable de traitement doit le notifier au plus tôt à la CNIL, dans un délai de 72 heures maximum.

A) Les cas de désignation

La violation de données est définie comme une « *violation de la sécurité entrainant, 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* » (point 12 de l'article 4 du RGPD).

Le responsable du traitement ou le sous-traitant doit rapidement déterminer si la violation de données est susceptible d'engendrer un risque, afin de pouvoir le notifier à l'autorité de contrôle et aux personnes concernées lorsque c'est nécessaire, dans les délais impartis.

Trois cas peuvent être déterminés : en premier lieu, il n'y a pas besoin de notification s'il n'y a pas de risque. Par exemple, un salarié se fait voler une disque dur externe avec des données chiffrées protégées inexploitables, et une copie existe. En deuxième lieu, cas où le risque est tempéré, dans ce cas il faut faire une notification à la CNIL. Par exemple, ce sera le cas d'un piratage de serveur, le rendant indisponible, donc empêchant aux clients de recevoir la newsletter d'une entreprise. La notification à l'autorité suffit. Enfin, si le risque est élevé, une notification aux personnes concernées sera nécessaire. Par exemple, une fuite d'une liste d'abonnés ayant un contrat d'assurance, ou encore l'attaque d'une plateforme de vente en ligne et la publication des données (login, mot de passe, historique d'achat).

B) L'évaluation de la nécessité de notifier

La difficulté réside dans l'évaluation de la gravité et la probabilité de survenance des conséquences de la violation. C'est finalement du cas par cas, c'est pourquoi il parait opportun

de réaliser des tests ou des mises en situation pour voir qui doit intervenir, à quel moment, et comment réagir face à ce type d'évènement. En effet, il faut prendre en compte les circonstances spécifiques de la violation, la nature, le volume et la sensibilité des données ; le nombre et types de personnes concernées (par exemple, mineur ou patient) ; les possibilités d'identification des personnes ; les caractéristiques du responsable de traitement et enfin la gravité des conséquences potentielles (si le risque peut entrainer des dommages physiques, matériels ou un préjudice moral).

La mise en place de cette procédure de réaction vive et efficace est compliquée à mettre en œuvre au sein des entreprises d'assurance, car elle implique de faire travailler ensemble des personnes qui n'ont pas l'habitude de se côtoyer, et le temps assez court pour notifier à la CNIL la violation des données nécessite un véritable travail d'exercices en amont afin de réagir au mieux et au plus vite. Ce temps commence à courir à compter de la prise de connaissance de la violation ; par exemple, les autorités considèrent que si une personne informe le responsable du traitement qu'elle a reçu un faux email de sa part contenant des données à caractère personnel la concernant, cette information ne fera que suggérer qu'une violation de données a eu lieu ; si après une première investigation, des indices révélant un accès non autorisé aux données sont recueillis, le responsable du traitement sera alors considéré comme ayant pris connaissance de l'incident.

La notification à l'autorité de contrôle[55] devra contenir une description de la violation des données, le nom et coordonnées du délégué à la protection des données ou personne en charge de l'organisation, une description des mesures prises ou envisagées et une description des conséquences éventuelles.

S'agissant de la notification à la personne concernée[56], elle est similaire à celle faite aux autorités de contrôle, à la différence que la description de la nature de la violation doit être faite en termes simples.

Le responsable de traitement doit documenter toutes les violations de données, qu'elles aient fait l'objet d'une notification ou non. Lorsqu'il décide de ne pas notifier la violation, il doit motiver cette décision.

[55] Article 33 : Notification à l'autorité de contrôle d'une violation de données à caractère personnel

[56] Article 34 : Communication de la personne concernée d'une violation de données à caractère personnel

Section 2 : Les impacts réels au sein de l'organisation des procédures pour les entreprises d'assurance

Les entreprises d'assurance doivent tout mettre en œuvre pour être conformes au RGPD de manière exhaustive et aussi tôt que possible.

I. Les chantiers en principe déjà en cours

Les entreprises doivent, depuis le 25 mai, être en conformité au niveau des nouvelles obligations imposées par le RGPD.

Le registre de traitement doit être élaboré, et être tenu à jour en continu. Un système d'archivage et de purge des données personnelles est en principe mis en place, avec une procédure adéquate. Les informations des personnes concernées doivent avoir été modifiées et renvoyées ; d'ailleurs il est à noter que normalement beaucoup de mails concernant la « mise à jour du RGPD » ont été reçus par les particuliers, ils proviennent de toutes sortes d'entreprises[57], pas uniquement en matière d'assurance, puisque le règlement touche toutes les entreprises susceptibles d'être concernées par la protection des données personnelles, c'est-à-dire qui font la collecte d'informations personnelles à un moment donné de leur processus. Il doit y avoir un renforcement de la sécurité sur les traitements des données sensibles, telles que les données de santé, ce qui impose à plusieurs services de travailler sur le sujet. De plus, lors de la prospection commerciale, le consentement doit être requis au préalable.

En matière de sous-traitance, une révision de l'ensemble des contrats doit être faite en 2018, et les plus risqués devraient avoir été révisés impérativement avant l'entrée en vigueur du RGPD, pour garantir juridiquement les traitements.

Enfin, les nouvelles obligations imposées par le règlement doivent être mises en œuvre, tel que le *Privacy by design, by default* et l'approche par les risques pour les personnes concernées. Les équipes doivent savoir comment mener des EIVP pour les traitements à risque. Un DPO doit avoir été nommé également, si cela est nécessaire.

[57] Par exemple : Google, Etam, Foodora, Uber, Sfr, Spotify…

Toutes ces obligations doivent déjà être bien ancrées au sein des entreprises d'assurance[58].

II. Les chantiers à lancer impérativement avant 2019

Bien que deux années ont été laissées aux entreprises pour préparer la mise en application du RGPD, certaines mesures demandent, en plus du temps, de la pratique pour observer les difficultés concrètes qu'elles peuvent susciter.

Un réel développement de la culture du règlement et plus généralement de protection des données est à inculquer par tous les acteurs. Pour cela, une bonne communication, des formations complètes et des moyens de sensibilisations sur le sujet sont à mettre en œuvre. Tout cela ne pourra s'effectuer qu'avec le temps et l'expérience.

En outre, une profonde transformation de la gouvernance de la protection des données se dessine à l'horizon. En effet, chaque département traitant des données personnelles est responsable de la mise en œuvre des principes de ces dernières et de l'application du RGPD. Chaque référent à la protection des données doit être identifié, et ces référents doivent mettre en application les principes de protection pour le périmètre de leur ligne fonctionnelle ; ce qui impose de délimiter leur périmètre. Reste à savoir combien de référents au RGPD doit contenir chaque entreprise, et comment se définit le périmètre, par direction ou autrement ? Il s'agit d'une véritable problématique d'organisation, qui ne se résoudra qu'avec le temps, et sera unique à chaque entreprise, en fonction de sa manière de fonctionner[59].

Enfin, le DPO, chef d'orchestre de la conformité, doit contrôler le respect du règlement et du droit national en matière de protection des données. Pour cela, il faut informer et conseiller le responsable de traitement ainsi que les employés, conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution. De plus, il faut coopérer avec l'autorité de contrôle et être le point de contact avec cette dernière.

[58] Chez Aviva, le registre de traitement a été mis en place, un DPO a été nommé en décembre 2017, et les contrats avec les sous-traitants ont été mis à jour. Le suspense repose encore sur l'EIVP, puisqu'il n'y en a pas encore eu d'élaborer à ce jour

[59] Au sein d'Aviva, un référent est nommé par pôle (Annexe 3)

Quoiqu'il en soit, il est vivement conseillé aux entreprises d'être irréprochables au sujet de la conformité, pour éviter d'être exposées aux sanctions prévues par le Règlement.

Section 3 : Vers une régulation plus contentieuse de la protection des données

Les sanctions renforcées par le RGPD conduisent à des conséquences pratiques facilitant le contentieux.

I. Des sanctions renforcées

En cas de non-respect du RGPD, les responsables de traitement et leurs sous-traitants s'exposent à des sanctions administratives importantes (Article 83[60]).

L'avertissement par écrit est la sanction la plus douce, mais il peut également être rendu public. Les autorités de protection[61] peuvent prononcer un avertissement ou mettre en demeure l'entreprise, mais elles peuvent également limiter de façon temporaire ou définitive un traitement. Il leur est également possible d'ordonner de satisfaire aux demandes d'exercice des droits des personnes, ou d'ordonner la rectification, la limitation ou l'effacement des données.

Ensuite, des amendes administratives peuvent être prononcées, elles sont de deux sortes. Le premier échelon s'élève à 2% du chiffre d'affaires annuel mondial ou 10 millions d'euros, la plus élevée des deux options étant retenue ; la sanction s'appliquera en cas d'absence de protection des données dès la conception et par défaut de sécurité des données, en cas d'absence de notifications des violations de données, ou encore s'il y a absence de registre de traitement. Également si les règles de désignation du DPO ne sont pas respectées. Le second échelon s'élève à 4% du chiffre d'affaires annuel mondial ou 20 millions d'euros, le montant le plus élevé et donc le plus sévère étant de nouveau retenu dans ce cas ; cette sanction aura vocation à s'appliquer lorsqu'il y aura une violation des droits fondamentaux des personnes.

Pour autant, Isabelle Falque-Pierrotin, la présidente de la CNIL, a affirmé aux entreprises qu'elle ferait preuve de souplesse en matière de contrôle après l'entrée en application du RGPD, lors d'un entretien en février dernier pour le quotidien les échos : « *le 25 mai ne sera pas une*

[60] Article 83 : Conditions générales pour imposer des amendes administratives

[61] G29 et CNIL

date couperet annonciatrice d'une pluie de sanctions » ; ainsi, une sorte de moratoire pour les nouveaux principes à respecter est accordé.

Cependant, cette déclaration n'est pas synonyme de laxisme de la part de la CNIL, telle en est la preuve pour la société Optical Center, qui a été sanctionnée[62] au mois de juin avec une amende de 250 000 euros pour un défaut de sécurité sur son site internet permettant à un tiers d'accéder à des données personnelles de clients.

II. Les conséquences pratiques

Le RGPD instaure de nombreuses nouveautés, qui vont mettre un certain temps à se mettre en place, et qui vont inévitablement engendrer certains contentieux, qui étaient inhabituels jusqu'à la date de mise en application du règlement.

Tout d'abord, l'obligation des notifications des failles sécurité prévu à l'article 33 va modifier les sources d'information des régulateurs et orienter leur approche. Ainsi, il faudra être prévenant.

De plus, l'introduction d'actions collectives va faciliter la structuration et l'expression des plaignants, même si le règlement renvoie à la loi nationale (article 80[63]). Des plaintes collectives ont d'ailleurs déjà été déposées le 28 mai contre les GAFAM[64], à l'initiative de l'association de défense des internautes « La Quadrature du Net ».

La possibilité d'échanger des informations avec les autres autorités et de mener des opérations conjointes de contrôle si le droit de l'État membre l'autorise est une importante nouveauté (article 62[65]).

En outre, la faculté de poursuivre le régulateur en cas d'absence de réponse à une plainte est une incitation forte à la réactivité (article 78[66]). En effet, si la CNIL ne répond pas dans les trois mois suivants la plainte, il est possible d'exercer un recours juridictionnel. Il faut toutefois tempérer en différenciant « répondre » et « traiter » la plainte ; le régulateur pourra simplement

[62] Délib. CNIL n° SAN-2018-002, 7 mai 2018 : JO, 7 juin

[63] Article 80 : Représentation des personnes concernées

[64] Acronyme pour les « géants du net » : Google, Apple, Facebook, Amazon et Microsoft

[65] Article 62 : Opérations conjointes des autorités de contrôle

[66] Article 78 : Droit à un recours juridictionnel effectif contre une autorité de contrôle

répondre par un accusé de réception et annoncer qu'il va traiter la plainte sans pour autant le faire dans les trois mois ; tant qu'il y a un retour, ce sera conforme au règlement.

L'ouverture d'actions à l'encontre du responsable de traitement mais aussi du sous-traitent augmente les possibilités de recours (article 82[67]) et tend donc vers un accroissement du contentieux. En effet, « *toute personne ayant subi un dommage matériel ou moral du fait d'une violation du présent règlement a le droit d'obtenir du responsable de traitement ou du sous-traitant réparation du préjudice subi* ». D'ailleurs, le 28 juin dernier, le porte-parole de la CNIL, interrogé par l'AFP, a annoncé que depuis l'entrée en vigueur du RGPD, la CNIL a enregistré « près de 1000 plaintes », soit une hausse « de plus de 100% » par rapport à la même période l'année dernière.

Comme vu précédemment, le pouvoir de sanction est considérablement accru : jusqu'à 20 millions d'euros d'amende ou 4% du chiffre d'affaires annuel mondial.

Enfin, la CNIL prévoit la délivrance de certification par des organismes agréés par elle ou accrédités par le COFRAC pour justifier de la conformité au RGPD des entreprises, et mettra fin progressivement à son activité de labellisation.

[67] Article 82 : Droit à réparation et responsabilité

Conclusion

Le RGPD touche beaucoup de secteurs et est au cœur de l'actualité en matière de protection des données personnelles. C'est un chantier très large, et il implique beaucoup de mutations, que ce soit au niveau du personnel, des traitements, des procédures, ou encore des preuves de conformité. Les acteurs de l'assurances doivent désormais s'accommoder des contraintes auxquelles est soumis le traitement des données personnelles de leur clientèle, mais ils peuvent enfin trouver un référentiel règlementaire plus adapté aux nouveaux modèles d'assurance que la collecte des telles données permettra justement de développer.

De manière générale, grâce à ce texte, il est possible d'affirmer que la Commission européenne souhaite trouver un point d'équilibre entre le renforcement du niveau de protection des données à caractère personnel pour assurer la confiance de l'ensemble des personnes présentes sur le territoire de l'UE et l'expansion du numérique. De plus, la CNIL se voit investie de nouveaux pouvoirs, afin d'accompagner, mais aussi de contrôler les responsables de traitement dans la mise en place des procédés permettant d'associer les personnes concernées à la transmission et la conservation de leurs données personnelles.

Ce règlement marque une évolution certaine en matière de droits numériques pour les citoyens européens, et constitue un défi juridique majeur pour les entreprises d'assurance qui devront se conformer aux exigences de ce dernier et garantir une protection adéquate. La mise en place de ce règlement s'adosse donc à une politique nationale plus ambitieuse, et il faudra plusieurs années afin de pouvoir apprécier dans quelle mesure la vie privée aura pu se concilier avec l'ère numérique.

Pour autant, il ne marque pas un aboutissement, puisque dans la continuité de la protection des données à caractère personnel, le 10 janvier 2017, la Commission européenne a publié sa proposition de règlement E-Privacy, dont l'objectif est d'abroger la directive 2002/58 du 12 juillet 2002[68] et d'harmoniser la législation des États membres en matière de confidentialité des communications électroniques. De plus, la loi du 20 juin 2018 relative à la protection des

[68] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

données personnelles vient déjà adapter la loi Informatique et libertés du 6 janvier 1978 au « paquet[69] » européen de protection de données.

Ce nombre croissant de règlementations en matière de protection des données personnelles démontre que, dans l'ère du numérique, il est nécessaire de faire face à une adaptation lente et compliquée du droit pour une évolution très rapide de la technologie. Ainsi, peut-être faudrait-il s'attendre à voir progressivement émerger un droit de l'Homme numérique. Quoiqu'il en soit, l'objectif reste le même : trouver un équilibre entre les intérêts des acteurs économiques et la protection des données personnelles des utilisateurs.

[69] Ce paquet comprend le RGPD et la directive relative à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données » du 27 avril 2016

Bibliographie et autres sources

Articles :

- « *Défaut de sécurité du site internet : Optical center sanctionnée d'une amende de 250 000 euros par la CNIL* », Elnet.fr, 19 juin 2018
- « *Dépôt des plaintes collectives contre les GAFAM !* », la Quadrature du Net, 28 mai 2018
- « *La Cnil accompagne les entreprises dans leur transition vers le RGPD* », Liaisons sociales Quotidien, L'actualité, 19 avril 2018, n°17555
- « *Prise d'effet du Règlement Général sur la Protection des Données : quelles conséquences pour le secteur de l'assurance ?* », Responsabilité civile et assurances, Mai 2018, n°5, alerte 13
- « *RGPD. Données personnelles : le nombre de plaintes à la CNIL a explosé* », site Ouest-France, 29 juin 2018
- E. BRAUN, « *Le RGPD, cette loi sur les données personnelles à laquelle il faut vous intéresser* », Le Figaro, 25 avril 2018
- F. CHALTIEL, « *La protection des données personnelles. A propos de l'entrée en vigueur du règlement général de protection des données* », Petites affiches, 4 juin 2018, n°111, p.6
- F. MATTATIA, *« La mise en œuvre du RGPD au prisme du risque juridique* », Revue Lamy Droit de l'Immatériel, 1er août 2017, n°140
- G. BORDIER, « *Le chantier majeur du RGPD* », Semaine Sociale Lamy, 19 mars 2018, n°1807
- J-L. SAURON et S.HAMON, « *Le projet de loi sur la protection des données mérite-t-il bien son nom ?* », Gaz. Pal., 23 janv. 2018, n°3, p.15
- L. GRYNBAUM, « *RGPD, un changement opportun pour les assureurs* », Argus de l'assurance, 14 juin 2018
- M. DARY et V. LICHET, « *Prospection commerciale et données personnelles : le RGPD bouleverse-t-il les pratiques ?* », Revue Lamy droit des affaires, 1er juin 2018, n°138
- O. DUFOUR, « *La Cnil au défi du RGPD* », Petites affiches, 2 mai 2018, n°087-088, p.4
- P. BOUCHER, « *Safari ou la chasse aux Français* », Le Monde, 21 mars 1974

Conférences :

- Cabinet Fromont Briens, Conférence RGPD, « *Quels impacts pour les acteurs RH ?* », 3 mai 2018, Lyon
- Aviva, « *Le RGPD, le big bang de la protection des données personnelles* », 24 mai 2018, Auditorium, Bois-Colombes

Directives et règlements :

- Parlement européen et Conseil, Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractères personnel et à la libre circulation de ces données, 24 octobre 1995
- Parlement européen et Conseil, Règlement (CE) n°45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, 18 décembre 2000
- Parlement européen et Conseil, Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), 12 juillet 2002
- Parlement européen et Conseil, Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), 27 avril 2016
- Parlement européen et Conseil, Directive (UE) 2016/680 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, 27 avril 2016
- Commission européenne, Projet de Règlement E-Privacy, 10 janvier 2017

Lois et décret :

- Décret n°2005-1309 pris pour l'application de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, 20 octobre 2005, version consolidée au 19 mars 2009
- Loi n°78-17 relative à l'informatique, aux fichiers et aux libertés, 6 janvier 1978
- Loi n°2018-493 relative à la protection des données personnelles, 20 juin 2018

Films :

- BERNET David*, Democracy*, 2015
- STONE Oliver*, Snowden*, 2016

Document et guides pratiques en ligne :

- Commission Nationale de l'Informatique et des Libertés, « *RGPD : par où commencer* », https://www.cnil.fr/fr/rgpd-par-ou-commencer
- Commission Nationale de l'Informatique et des Libertés, « *RGPD : se préparer en 6 étapes* », https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes
- Commission Nationale de l'Informatique et des Libertés, *« Le registre des activités de traitement* », https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement
- Commission Nationale de l'Informatique et des Libertés, « *Le délégué à la protection des données (DPO)* », https://www.cnil.fr/fr/le-delegue-la-protection-des-donnees-dpo
- Commission Nationale de l'Informatique et des Libertés, *« Passation, gestion et exécution des contrats d'assurance* », NS-016, https://www.cnil.fr/fr/declaration/ns-016-passationgestion-et-execution-des-contrats-dassurance
- « *Comment identifier les données ou informations, les traitements et les personnes, soumis à la règlementation relative à la protection des données personnelles ?* », Le Lamy droit du numérique (Guide), 4069
- « *Qu'entend-on par « données personnelles » ?* », Le Lamy droit du numérique (Guide), 4070
- Commission Nationale de l'Informatique et des Libertés, « *Règlement européen sur la protection des données : ce qui change pour les professionnels* », 15 juin 2016,

https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

- G29, « *Lignes directrices concernant la désignation d'une autorité de contrôle chef de file d'un responsable du traitement ou d'un sous-traitant* », 13 décembre 2016, https://www.cnil.fr/sites/default/files/atoms/files/wp244rev01_fr.pdf
- Commission Nationale de l'Informatique et des Libertés, « *Les BCR (règles internes d'entreprise)* », 6 novembre 2017, https://www.cnil.fr/fr/les-bcr-regles-internes-dentreprise
- Commission Nationale de l'Informatique et des Libertés, « *DARTY : sanction pécuniaire pour une atteinte à la sécurité des données clients* », 9 janvier 2018, https://www.cnil.fr/fr/darty-sanction-pecuniaire-pour-une-atteinte-la-securite-des-donnees-clients
- F. CHAFIOL, S. TUBERT, S. LAPEYRE ET A. BLANC, « *M-4 : Notification des violations de données à caractère personnel* », Blog August Debouzy, 14 février 2018, https://www.august-debouzy.com/fr/blog/1110-notification-des-violations-de-donnees-a-caractere-personnel
- Commission Nationale de l'Informatique et des Libertés, « *Bilan 2017, l'effet RGPD : une année de préparation active de la transition, doublée d'une très forte attente des particuliers et des professionnels* », 10 avril 2018, https://www.cnil.fr/fr/bilan-2017-leffet-rgpd-une-annee-de-preparation-active-de-la-transition-doublee-dune-tres-forte
- Commission Nationale de l'Informatique et des Libertés, *« Les enjeux pour 2018 (1) : accompagner les professionnels dans leur transition au règlement jusqu'au 25 mai et après* », 10 avril 2018, https://www.cnil.fr/fr/les-enjeux-pour-2018-1-accompagner-les-professionnels-dans-leur-transition-au-reglement-jusquau-25
- Commission Nationale de l'Informatique et des Libertés, « *Conformité RGPD : comment informer les personnes et assurer la transparence ?* », 14 mai 2018, https://www.cnil.fr/fr/conformite-rgpd-information-des-personnes-et-transparence
- Commission Nationale de l'Informatique et des Libertés, « *Transferts de données hors UE : ce qui change avec le règlement général sur la protection des données (RGPD)* », 24 mai 2018, https://www.cnil.fr/fr/transferts-de-donnees-hors-ue-ce-qui-change-avec-le-reglement-general-sur-la-protection-des-donnees
- Commission Nationale de l'Informatique et des Libertés, « *Limiter la conservation des données* », 28 mai 2018, https://www.cnil.fr/fr/limiter-la-conservation-des-donnees

Traités :

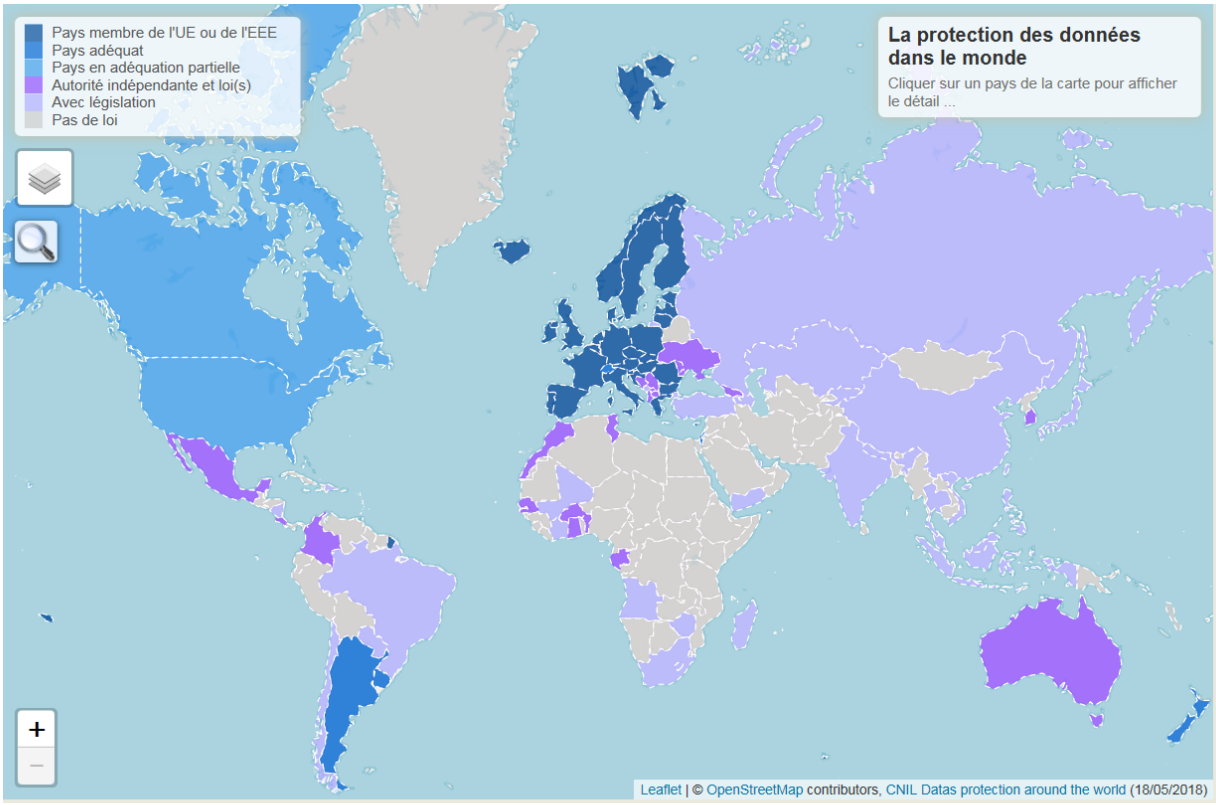
- Traité de Lisbonne modifiant le Traité sur l'Union Européenne et le Traité instituant la Communauté Européenne, 2007/C 306/01, 17 décembre 2007
- Traité sur le fonctionnement de l'Union européenne (version consolidée), C 115/47, 9 mai 2008

Vidéos Youtube :

- Chaîne Agence MCM, « *GEM : protection des données personnelles* », [vidéo en ligne], 3 novembre 2016, (consulté le 20 mai 2018), 31 min, https://www.youtube.com/watch?v=krgeTIx22jM
- Chaîne Cookie Connecté, *« RGPD/GDPR : on répond à vos questions avec la CNIL* », [vidéo en ligne], 5 février 2018, (consulté le 3 mai 2018), 15 min, https://www.youtube.com/watch?v=OUMGp3HHel4
- Chaîne Leo Guillot, « *RGPD : Êtes-vous Prêt Pour le 25 Mai ? On Fait le Point Ensemble* », [vidéo en ligne], 13 mai 2018, (consulté le 20 mai 2018), 24 min, https://www.youtube.com/watch?v=_bPRBDD7SUo

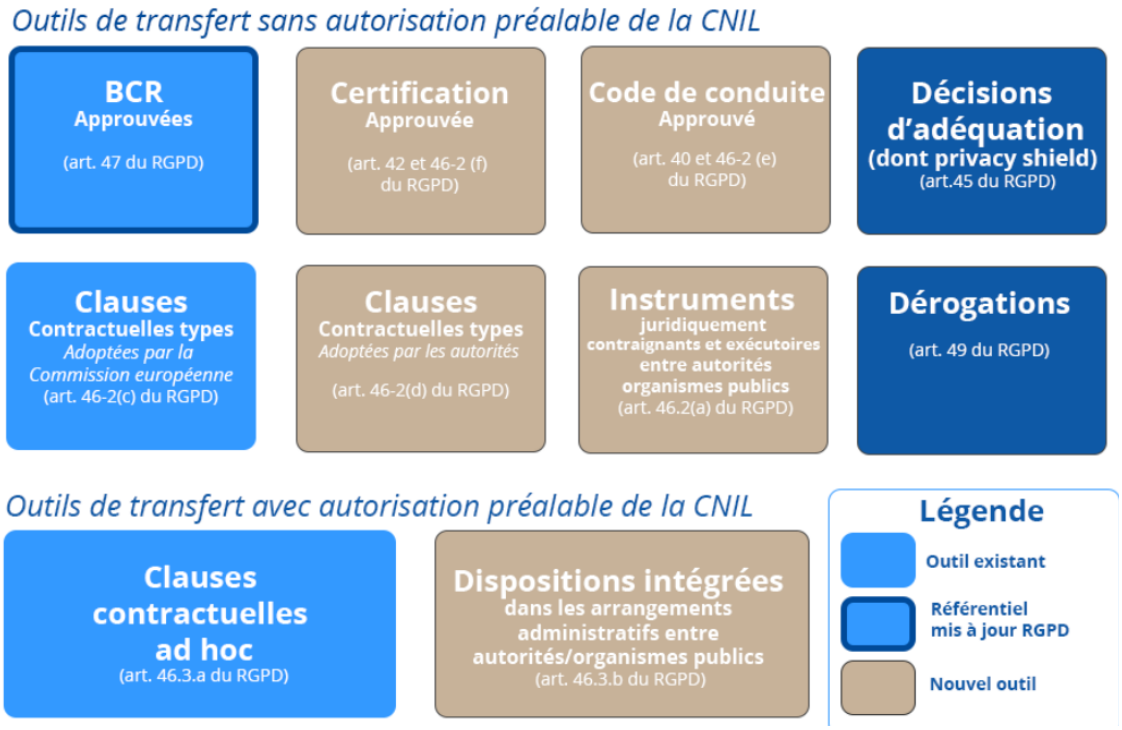
ANNEXES

Annexe 1 : La protection des données dans le monde



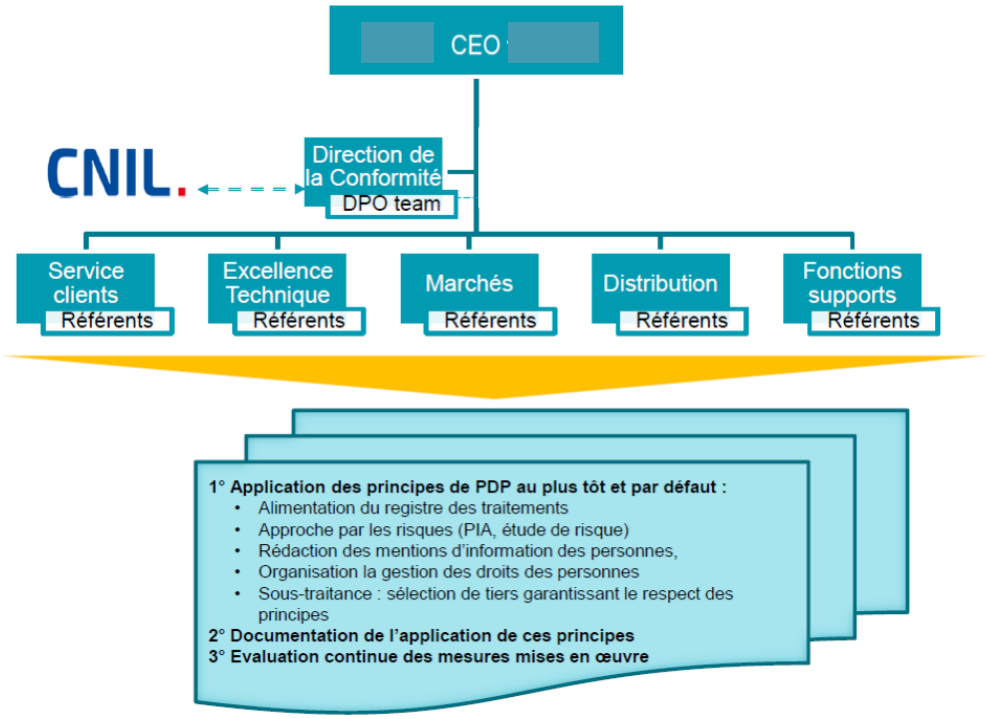
Source : Site de la CNIL, https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Annexe 2 : Les outils juridiques permettant le transfert des données hors UE



Source : Site de la CNIL, https://www.cnil.fr/fr/transferts-de-donnees-hors-ue-ce-qui-change-avec-le-reglement-general-sur-la-protection-des-donnees

Annexe 3 : Gouvernance cible



Source : Aviva

PDP : Protection des Données Personnelles