Cahiers Techniques 2018

Commission
Systèmes d'Information

Le Règlement Général sur la Protection des Données

(RGPD)

Comment l'entreprise doit-elle protéger les données personnelles ?

En partenariat avec

CGI | Business Consulting

AMRAE L'ASSOCIATION

Version 2 – JUIN 2018

A propos de l'AMRAE

L'AMRAE est l'association française des professionnels de la gestion des risques et des assurances.

L'**A**ssociation pour le **M**anagement des **R**isques et des **A**ssurances de l'**E**ntreprise rassemble plus de 1200 membres appartenant à 750 entreprises françaises publiques et privées.

L'association a notamment pour objectifs de développer la « culture » du Management des Risques dans les organisations et d'aider ses membres dans leurs relations avec les acteurs du monde de l'assurance et les pouvoirs publics. Elle les conseille dans l'appréciation des risques, dans la maîtrise de leurs financements et leurs dépenses d'assurance.

Sa filiale AMRAE Formation, pour répondre aux besoins de formation professionnelle de ses adhérents ou de ceux qui légitimement s'adressent à elle, dispense des formations diplômantes, certifiantes et qualifiantes de haut niveau.

A propos de CGI Business Consulting

CGI Business Consulting anticipe, conçoit et donne vie aujourd'hui aux modèles qui feront l'économie de demain.

Véritables business designers, nous sommes des accélérateurs de stratégies : nous décryptons les dynamiques des marchés afin de capter les opportunités de changement. Nous accompagnons les grands projets de transformation de nos clients dont nous sommes les partenaires privilégiés, leurs **Trusted Advisors**.

Avec plus de 1000 consultants à Paris et en région, CGI Business Consulting est le 3ème acteur du conseil en management en France (source PAC) et fait bénéficier ses clients de plus de 20 ans d'expérience dans l'accompagnement des grands projets de transformation des entreprises. Notre positionnement unique s'appuie sur la présence d'un groupe mondial, l'expertise technologique d'une ESN et l'impact disruptif de nos partenaires : nos clients bénéficient ainsi du meilleur des expertises du marché.

Fondée en 1976, CGI est la cinquième plus importante entreprise indépendante de services-conseils en technologie de l'information (TI) et en management au monde. Grâce à ses quelques 71 000 professionnels établis partout dans le monde, CGI offre un portefeuille complet de services stratégiques en TI et en management, d'intégration de systèmes ainsi que d'impartition de services en TI et en gestion des processus d'affaires. CGI propose une approche unique de proximité avec les clients et le réseau mondial de prestation de services le mieux adapté à leurs besoins. Elle offre également des solutions de propriété intellectuelle exclusives afin de les aider à accélérer l'obtention de résultats et à réaliser la transformation numérique de leur organisation. CGI génère des revenus annuels de 10,8 milliards de dollars canadiens. Les actions de CGI sont inscrites à la Bourse de Toronto (GIB.A) ainsi qu'à la Bourse de New York(GIB). Site Web : www.cgi.com.

Table des matières

Préface

Le 25 mai 2018, un changement de premier ordre s'est opéré dans la **protection de la vie privée et surtout dans la protection de nos données personnelles !**

On entend par donnée à caractère personnel toute donnée permettant d'identifier directement ou indirectement une personne physique comme par exemple le nom, le prénom, le numéro de sécurité sociale, une photographie, des coordonnées bancaires ou bien encore une adresse IP.

Le « Règlement Général sur la Protection des Données » (RGPD ou en anglais « *General Data Protection Regulation* », GDPR) s'applique désormais à toutes les organisations, y compris celles ne se trouvant pas implantée sur le territoire européen :

- Qui réalisent des traitements de données à caractère personnel sur le sol européen,
- Ou qui réalisent des traitements de données à caractère personnel de résidents européens (citoyens européens ou non).

Ce règlement répond à plusieurs nécessités :

- Politique : l'Union Européenne souhaite protéger les données de ses citoyens et de ses résidents, notamment vis-à-vis des GAFAM[1]-,
- Economique : la transformation liée à l'économie numérique nécessite la confiance des citoyens-,
- Humaine : l'Union européenne souhaite préserver la vie privée des personnes de toute atteinte lors du traitement de leurs informations.

Les fuites d'informations personnelles font la « Une » de l'actualité quasiment chaque semaine. Le RGPD vise notamment à prévenir et limiter ce risque. En effet, après avoir fourni des informations personnelles, une personne physique peut voir ses données exploitées par des tiers, voire revendues à d'autres tiers, et elle en perd alors totalement le contrôle.

En grande majorité, les organismes traitant des données personnelles n'apportent pas encore de garanties suffisantes quant à l'exécution concrète des droits de la personne (droit à l'oubli par exemple), ni l'assurance d'un traitement maîtrisé lorsqu'il s'agit par exemple d'éviter :

- Le vol d'informations personnelles de santé, de données bancaires ou d'identité ;
- La divulgation d'informations personnelles compromettant la notoriété.

En confiant à chaque organisation détentrice de données à caractère personnel, la **responsabilité de « sécuriser » celles-ci et en octroyant de nouveaux droits aux personnes concernées**, l'Union Européenne fait de ce risque un **risque d'entreprise**. Les organisations ont donc désormais à gérer des risques d'un genre nouveau, car liés à la vie privée, encore peu ou mal identifiés, et qui peuvent engendrer :

[1] GAFAM : Google, Apple, Facebook, Amazon, Microsoft

- des impacts sur leur image et leur réputation avec des conséquences potentielles graves comme une perte de confiance de leurs clients (ces derniers préférant se tourner vers des organisations leur garantissant une meilleure protection de leurs données) ;
- des impacts financiers significatifs liés aux sanctions (pouvant aller jusqu'à 4% du chiffre d'affaires), aux frais de notification, à une perte de business (liée à la perte de clients), à des dommages et intérêts, à des frais de défense…

Compte tenu de l'importance des impacts de ces risques pour les organisations, le ***Risk manager*** ne peut pas « passer à côté » de ces sujets et doit s'impliquer dans le projet de mise en conformité de son organisation. Il doit s'impliquer en le coordonnant, ou plus simplement en étant partie prenante, et en guidant alors le projet, et la mise en conformité, dans une approche par les risques (afin par exemple d'éviter les impacts les plus importants, de ne pas surinvestir vers une sur-conformité inutile, ou encore, d'être en veille sur l'interprétation et la déclinaison du Règlement). Dans certaines organisations, il pourra se voir nommer ***Data Protection Officer (DPO)***, ou responsable de cette conformité.

Outre le volet risques de la fonction, la mise en œuvre du RGPD impacte également le rôle du Risk manager sur la partie « Assurance ». La souscription d'une police « cyber » permet, par exemple, de couvrir un certain nombre de risques et frais associés, mais également d'apporter des services d'expertise à des organisations ne pouvant, par exemple, se doter d'un service interne dédié à la gestion de crise « cyber ». Dans les années à venir, le maintien de cette conformité va également devenir un enjeu de risques.

Conscients de cette complexité, l'AMRAE et CGI Business Consulting ont choisi de vous accompagner dans votre démarche de prise en compte du RGPD, au travers de ce cahier technique dans sa seconde version (la V1 ayant été publiée début février 2018), en apportant notamment un éclairage sur les questions suivantes :

- Comprendre ce qu'est le RGPD et notamment comment est constitué ce Règlement.
- Quels sont les nouveaux droits introduits ?
- Qui doit-on impliquer dans l'organisation afin de se mettre en conformité ?
- Quel rôle pour le Risk manager dans ce projet ?
- Quelles sont les nouvelles responsabilités ? Quelles fonctions sont impactées ?
- Comment mener à bien son projet « RGPD » et maintenir sa conformité dans le temps ?

François Beaume
vice-Président de l'AMRAE

Hervé Ysnel
vice-Président CGI Business Consulting
Responsable des offres Cybersécurité et gestion des risques

Le Cahier technique que vous avez en main a été rédigé par les experts RGPD de CGI Business Consulting : Anthony Augereau (Directeur), Amaury Cothenet (Manager), Jean Olive (Directeur), Hervé Ysnel (vice-Président), ainsi que les membres de la practice « Security and Risk Management » de CGI Business Consulting.

Ce cahier technique a été relu, corrigé et amélioré par : Sophie Mauvieux (Administrateur AMRAE et membre de son Comité Scientifique Permanent), François Beaume (vice - Président AMRAE), Hélène Dubillot (Bureau Permanent de l'AMRAE, Directrice de la coordination scientifique), Marie-Christine Vittet (Data Risk manager, membre de la commission Systèmes d'Information), Bruno Rasle (Délégué Général de l'AFCDP).

[AVERTISSEMENT] L'objet de ce document est d'apporter un éclairage sur les évolutions de la règlementation européenne en matière de protection des données à caractère personnel. Le contenu de ce document n'a pas fait l'objet d'une analyse juridique et n'a pas valeur de conseil juridique. Il ne s'agit pas d'un commentaire du texte du Règlement Général sur la Protection des Données (RGPD). Il a été rédigé par des spécialistes de la gestion des risques, conformité et cybersécurité.
Il appartient à chacun de procéder au contrôle des lois et règlements applicables à son secteur d'activité, en se faisant, le cas échéant, accompagner par ses conseils juridiques.

1. Le Règlement Général sur la Protection des Données

Grâce aux progrès effectués dans les technologies de traitement de données, les entreprises peuvent désormais collecter et analyser les informations personnelles beaucoup plus facilement. Ces progrès ont offert une diversité de possibilités aux entreprises mais introduit également des risques.

Le traité sur le fonctionnement de l'Union Européenne définit, en son article 288, qu'un règlement est un acte juridique contraignant pour celles et ceux à qui il s'applique. Un règlement est applicable dans tous les pays de l'Union Européenne sans transposition en droit national, donc de manière homogène et au même moment dans tous les Etats membres.

Dans ce contexte, le Règlement Général sur la Protection des Données (RGPD – aussi nommé « Règlement » dans ce document), en vigueur depuis le 24 Mai 2016, a été introduit pour mieux protéger les individus de ces risques. Ce 25 mai 2018, le RGPD remplacera la précédente directive européenne 95/46/CE relative à la protection des données. Le RGPD fixe des principes clés qui déterminent comment traiter les données personnelles. L'ensemble de ces principes apporte une approche juridique uniforme sur la confidentialité des données dans l'Union Européenne. Il est applicable au responsable de traitement ou au sous-traitant établi sur le territoire de l'Union ou, si cela n'est pas le cas, aux personnes concernées par le traitement, qui se trouvent sur le territoire de l'Union.

Responsable de traitement : personne (physique ou morale), autorité publique, service ou organisme qui détermine les finalités et les moyens nécessaires relatifs à un traitement de données à caractère personnel (ex. directeur de l'entité où le traitement est mis en œuvre, et dont il porte la responsabilité).

Sous-traitant : personne (physique ou morale), l'autorité publique, service ou organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Le caractère extraterritorial du RGPD s'impose à tous les organismes, y compris ceux qui sont établis en dehors de l'espace européen, dès lors qu'ils procèdent au traitement de DCP.

Son domaine d'application est très large car il vise à la fois les données collectées par une organisation à « l'extérieur » (auprès de clients ou prospects par exemple), ainsi que les **données internes de ses collaborateurs**. Ces données sont accessibles en ligne au sein du Système d'Information (ex. base de données client),

mais elles sont également présentes dans des **bases et documents sauvegardés ou archivés**.

Le RGPD s'inscrit, pour la France, dans la lignée de la Loi Informatique et Libertés (LIL - promulguée en France en 1978 puis révisée en 2004 et en 2016), des avis et délibérations élaborés par la CNIL, de la Directive européenne 95/46 « Protection des données personnelles », de la LCEN (Loi pour la Confiance dans l'Economie Numérique) et du « Paquet Telecom » :

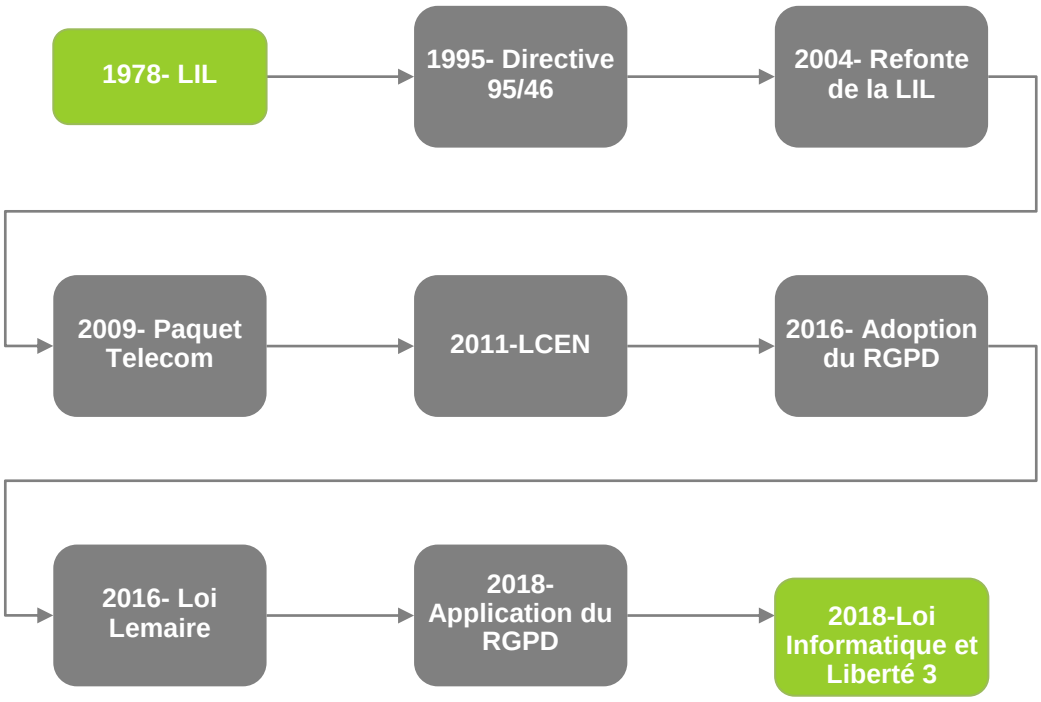


Figure 1 : Chronologie (non exhaustive) de l'évolution de la réglementation européenne et française

Le Règlement laisse aux Etats membres une marge de manœuvre concernant une cinquantaine de paramètres, pour lesquels chaque Etat peut légiférer de manière souveraine.

L'Autriche et l'Allemagne ont été les premiers Etats membres de l'UE à avoir adopté une législation nationale adaptée au RGPD, et ce dès juillet 2017. En France, le texte définitif vient d'être adopté par le Parlement et validé par le Conseil Constitutionnel dans une décision datant du 12 juin 2018.

D'autres textes règlementaires européens ou français sont associés au RGPD, et apportent des compléments ou des spécificités liées à un domaine d'application, parmi lesquels (cf. annexe pour plus de détails) :

- La Loi pour la Confiance dans l'Economie Numérique (LCEN) – Texte français ;

- La Directive e-Privacy – Texte européen ;
- La Loi pour une République numérique – Loi Lemaire – Texte français.

1.1 Structure du Règlement

Le RGPD est composé de 88 pages, 173 considérants et 99 articles répartis en 11 chapitres. Le contenu des articles est le résultat de consensus et de compromis entre les Etats membres. En conséquence, le texte final a dû parfois être édulcoré et son interprétation délicate, nécessite la lecture des considérants associés.

Figure 2 : les 11 chapitres du Règlement Général sur la Protection des Données

Il est structuré autour de neuf principes clés, présentés ci-après et détaillés tout au long de ce document :

Figure 3 : Principaux points du Règlement Général sur la Protection des Données

1.2 Principes clés du RGPD

Ce chapitre a pour objet de faire le lien entre les principes fondamentaux identifiés dans le chapitre précédent et les articles concernés au sein du RGPD. Chaque article fera l'objet d'une description succincte. Cette première approche des articles clés du Règlement sera précisée ultérieurement tout au long du document.

- **Sécurité du traitement** : L'accent est mis sur l'obligation d'un niveau de sécurité adéquat lors du traitement des Données à Caractère Personnel (DCP). Un certain nombre de mesures pourront être envisagées telles que la pseudonymisation, l'anonymisation (cf. méthodes classiques d'anonymisation paragraphe 5.10) ou le chiffrement.

  L'article 32 du RGPD définit notamment l'obligation, pour l'organisation, de sécuriser le traitement des données à caractère personnel.

  A cet égard, **le responsable de traitement des DCP** (Cf. Glossaire), qui détermine les finalités du traitement des DCP et la manière dont les traitements seront mis en œuvre (ex : Une personne morale : l'entreprise, ou une personne physique : le directeur/responsable du service concerné), doit s'assurer que les mesures techniques et organisationnelles mises en place sont appropriées et garantissent un niveau de sécurité adapté. Pour ce faire, le responsable de traitement a souvent besoin de s'appuyer sur des compétences spécifiques internes (ex : Direction des risques, Direction Juridique/Conformité, Direction sécurité, DSI …) ou externes, notamment pour mener l'analyse d'impact relative à la protection des données (Cf. paragraphe 5.10) et mettre en place les mesures nécessaires.

  Il doit également assurer la disponibilité, l'intégrité, la confidentialité et la résilience des données manipulées lors du traitement.

  Il est également responsable de la traçabilité des actions, qui permettront à l'organisation de prouver sa conformité au Règlement.

- **Nécessité de notification** et de **communication** en cas de violation des données : le Règlement introduit un certain nombre d'obligations dans le cas où une violation de données personnelles est constatée par l'organisation : obligations de notifications à l'autorité de contrôle (CNIL en France) et aux personnes concernées par cette violation. Ces notions sont explicitées plus en détail au chapitre 5.4 du présent document.

- **Le droit des personnes** sur leurs données personnelles : les personnes concernées voient leurs droits s'élargir et les conditions d'utilisation de leurs données personnelles explicitées. Les articles sur le droit des personnes concernées sont détaillés dans le chapitre 2 du présent document, et sont définis dans les articles 15, 16, 17, 18, 20, 21 et 22 du RGPD.

  Le RGPD s'inscrit dans la continuité des réglementations nationales existantes. Ainsi, en France, il fait suite à la Loi Informatique et Libertés de 1978 (LIL). Des droits, tels que les droits d'information et de transparence (Art. 12 du RGPD), d'accès (Art. 15 du RGPD), de rectification (Art. 16 du RGPD), d'opposition (Art. 21 du RGPD) sont réaffirmés, renforcés ou précisés dans le RGPD.

  De nouveaux droits sont développés par le RGPD, tels que le droit à l'effacement (article 17) et le droit à la limitation du traitement (article 18). Le droit à la portabilité des données (article 20) a quant à lui été créé.

- **Data Protection Officer (DPO) ou Délégué à la Protection des Données (DPD):** L'article 37 du RGPD crée une nouvelle fonction au sein de l'organisation, le Data Protection Officer (DPO), qui aura pour mission de veiller au respect de la bonne application du règlement. De ce fait, il sera le point de contact privilégié des autorités sur ce sujet. Il devra, en outre, créer et tenir à jour un registre des traitements des DCP. Enfin, il a pour rôle de conseiller et de sensibiliser les différents acteurs de l'organisation, impliqués dans les traitements des DCP.

  Lorsqu'un Correspondant Informatique et Libertés (CIL) a été nommé dans l'organisation, celui-ci voit parfois son rôle évoluer pour devenir DPO (même si cette évolution n'est pas systématique compte tenu de l'évolution de l'enjeu). Cette nouvelle fonction peut aussi être attribuée à différents acteurs au sein de l'entreprise comme le Risk manager, la direction juridique, la conformité, le contrôle interne, la DSI, etc. Le G29 a précisé dans un guide de bonnes pratiques[2] les activités que peuvent mener les DPO, sans enfreindre leur obligation d'indépendance.

- **Privacy by design & by default** : Le Règlement, dans l'article 25, définit un certain nombre d'obligations quant à la mise en œuvre, par l'entreprise, d'une démarche de protection des données, dès la conception d'une nouvelle solution et par défaut. Cette démarche repose sur plusieurs grands principes :

[2] https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

- ✓ la protection de la sphère privée (dès la conception),
- ✓ la pseudonymisation des données (dès que possible),
- ✓ la minimisation des données, c'est-à-dire collecter des données adéquates et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (ne pas prendre des informations qui ne seraient pas vraiment « utiles » au traitement) ,
- ✓ la définition d'une durée de conservation adaptée à la durée de traitement,
- ✓ un stockage des données centralisé, accessible uniquement par les personnes ayant besoin de les connaître,
- ✓ la prise en compte de la « *privacy* » dans la durée de vie complète des données.

- **Sanctions** : Différentes amendes et sanctions sont prévues en fonction de la nature du manquement au RGPD par le responsable de traitement et/ou son sous-traitant. Les conditions d'application de ces amendes et sanctions sont explicitées plus en détail au chapitre 3.2.
-

  Privacy Impact Assessment (PIA) ou Analyse d'Impact relative à la Protection des Données (AIPD) : Cette notion de PIA est abordée à l'article 35 du RGPD. Une analyse est nécessaire lorsqu'un traitement de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées. Le PIA consiste à vérifier, d'une part, la proportionnalité du traitement au regard des finalités (est-il cohérent face à l'enjeu ?) et l'impact sur les droits et libertés (quels risques pour les personnes ?), et d'autre part, à évaluer les mesures de sécurité prises pour traiter les risques associés (les garanties prises sont-elles suffisantes pour maîtriser le traitement ?). L'analyse d'impact est décrite plus en détail au chapitre 5.9.

- **Accountability** : Les responsables de traitement doivent être en capacité de prouver la bonne prise en compte des exigences du RGPD. Les obligations contractuelles entre l'organisation et les sous-traitants sont renforcées. Le responsable du traitement et le sous-traitant doivent tenir un **registre de traitement** complet recensant l'ensemble des traitements de données mis en place et démontrer leur conformité au Règlement.

<u>Obligations des responsables de traitement de DCP et de leurs sous-traitants :</u>

L'article 24 du Règlement requiert de la part du **responsable de traitement** (personne, autorité publique, service ou organisme qui détermine les finalités et les moyens nécessaires relatifs à un traitement de données à caractère personnel) qu'il soit en mesure de démontrer que le traitement effectué est conforme au RGPD. Le responsable de traitement s'appuie pour cela sur l'ensemble des mesures mises en

œuvre, soit par lui directement, soit par des sous-traitants qui devront présenter les garanties suffisantes en matière conformité au RGPD (cf. chapitre 5) et de protection des droits des personnes (cf. chapitre 2).

Obligation de génération de preuve à la charge de l'entreprise :

L'article 5 modifie profondément les modalités de génération de la preuve. Sous la Loi Informatique et Libertés de 1978, la charge de la preuve incombait soit à la personne concernée par le traitement de la DCP, soit à l'autorité de contrôle (ex : CNIL). Il leur incombait de démontrer que le traitement de la donnée personnelle n'était pas conforme à ce qui était exigé. **Le RGPD transfère désormais la charge de la preuve à l'organisation traitant des données personnelles. Elle** devra être en mesure de démontrer, lorsqu'on lui en fera la demande, que les modalités du traitement sont conformes au Règlement.

L'organisation devra **prouver qu'elle a mis en œuvre toutes les mesures nécessaires** à la protection des données personnelles qu'elle avait en sa possession (Cf. 3.1 Principe de Responsabilité/Accountability).

- **Licéité et consentement :** L'exigence de licéité est introduite à l'article 5 du Règlement. D'après le premier paragraphe de cet article, toute donnée à caractère personnelle doit être « traitée de manière licite, loyale et transparente au regard de la personne concernée ». La notion de licéité est précisée dans le premier paragraphe de l'article 6 du RGPD. Le respect d'au moins une condition, parmi les conditions citées ci-dessous, est nécessaire afin d'être en conformité avec le critère de licéité :

  - ✓ **Le consentement de la personne** (Art. 6.1.a et Art. 7) : Principe clé permettant de démontrer la licéité du traitement. La demande de consentement écrite doit être présentée sous une forme qui la distingue clairement des autres questions et surtout, « sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples ». Ex : consentement pour traiter les données à des fins d'envoi de newsletter par mail via une case à cocher et non pré-remplie. (Par ex : « Oui, j'accepte que mes données soient récoltées et traitées par l'AMRAE pour les buts ayant été déclarés. »)

  - ✓ **L'exécution d'un contrat** (Art. 6.1.b du RGPD) : Le traitement est considéré comme licite lorsqu'il est nécessaire dans le cadre d'un contrat ou dans celui de l'intention de fournir un contrat. Ex : traitement des données de salariés pour que l'employeur puisse procéder à leur rémunération.

  - ✓ **L'obligation légale** (Art. 6.1.c du RGPD) : Le traitement est considéré comme licite s'il est effectué conformément à une obligation légale à laquelle le responsable de traitement est soumis. Ex : traitement des données relatives aux rémunérations de leurs salariés par les employeurs pour pouvoir les communiquer à la sécurité sociale ou à l'administration fiscale.

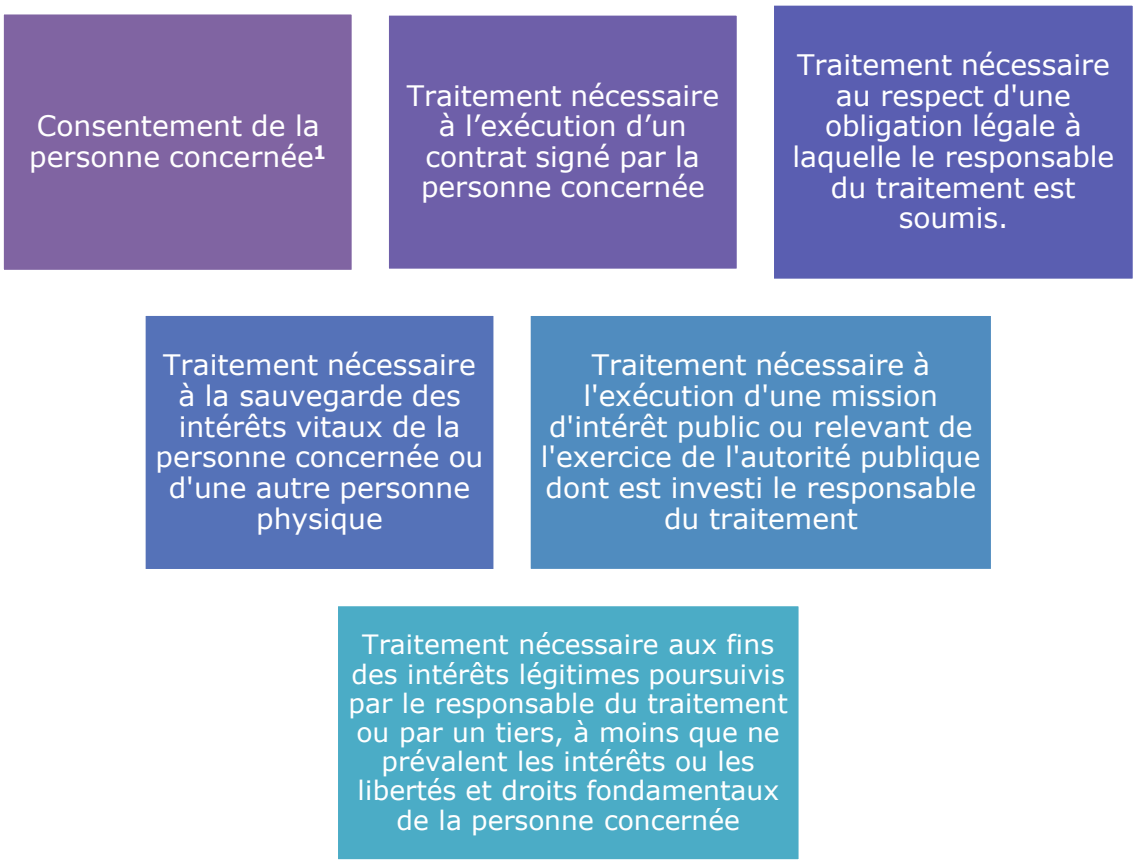
- ✓ **La sauvegarde des intérêts vitaux** (Art. 6.1.d du RGPD): Le traitement trouve son fondement juridique quand l'intérêt vital de la personne concernée, ou d'une autre personne physique, est en jeu. Ex : traitement de données aux urgences d'un hôpital.

- ✓ **L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique** (Art. 6.1.e du RGPD) : Le traitement est licite s'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique.

- ✓ **L'intérêt légitime** (art. 6.1.f du RGPD) : Le traitement est licite s'il trouve son fondement dans l'intérêt légitime poursuivi par le responsable de traitement, à moins que ne prévalent les intérêts ou les droits et libertés fondamentaux de la personne concernée. Le G29 a publié un document précisant les modalités d'application de cette base légale[3].
- ✓ Ex : traitement de données à des fins de prévention contre la fraude.

[3] http://www.dataprotection.ro/servlet/ViewDocument?id=1086

Le traitement est considéré comme licite si au moins une des six conditions suivantes est respectée :



Conditions rendant le traitement licite

[1]La notion de consentement est définie à l'article 4 paragraphe 11 du RGPD comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».
Point d'attention : des modalités particulières sont en vigueur concernant les mineurs de moins de 16 ans. En outre, un consentement ne peut être considéré comme librement consenti dans le cas d'un déséquilibre dans le rapport de force entre la personne et le responsable de traitement.

Figure 4 : La licéité de traitement : les critères

1.3 Autorité de contrôle indépendante

La notion d'autorité de contrôle compétente est définie au sein de l'article 55 du Règlement. Selon cet article : « Chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie conformément au présent Règlement sur le territoire de l'État membre dont elle relève ». Ce point était déjà prévu dans la Directive de 1995, aussi de nombreux pays possédaient déjà leur autorité de contrôle avant l'adoption du RGPD.

L'autorité de contrôle d'un Etat membre veille au respect du RGPD, non seulement par les organisations présentes sur son territoire, mais aussi par celles qui traitent des données personnelles d'européens en dehors du pays (ex. hors de l'union européenne). En outre, elle est en charge des litiges concernant les traitements des données personnelles réalisés par les entreprises, associations, organismes publics, …

L'autorité de contrôle dispose donc d'un pouvoir national. En France, dans la continuité du dispositif existant, **la CNIL conserve son statut d'autorité de contrôle nationale.**

Le Règlement ne prévoit pas la création d'une autorité de contrôle supranationale (Actuellement, l'ENISA est pressentie pour faire office d'autorité Européenne). Néanmoins, certains traitements sont transfrontaliers et nécessitent la désignation d'une autorité de chef de file. Un traitement transfrontalier est définit par le paragraphe 23 de l'article 4 du RGPD comme : « un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres ; ou qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres ».

Afin de répondre à ce cas particulier, le Règlement définit, dans son article 56, la notion d'autorité chef de file :

« Sans préjudice de l'article 55, l'autorité de contrôle de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant est compétente pour agir en tant qu'autorité de contrôle chef de file concernant le traitement transfrontalier effectué par ce responsable du traitement ou ce sous-traitant, conformément à la procédure prévue à l'article 60 ».

L'autorité chef de file est donc désignée conformément à l'emplacement géographique du siège social de l'entreprise ou sur le site où sont réalisés la plupart des traitements. Elle assure la fonction d'autorité de contrôle pour l'ensemble des traitements réalisés par l'entreprise. Elle est l'unique interlocuteur du responsable de traitement.

1.4 Précisions apportées par la version modifiée au 25 mai 2018 de la Loi Informatique et Libertés (LIL 2018)

Le 25 mai 2018, la nouvelle version de la LIL a transposé entièrement le RGPD dans la législation française. Cette transposition a permis aux députés et sénateurs de préciser les marges de manœuvres laissées par le RGPD. Après quelques divergences entre les deux chambres, c'est finalement le texte établi par l'Assemblée Nationale qui constitue en majorité la version finale de la Loi. Les principales discordances portaient sur l'immunité des collectivités territoriales aux sanctions financières et le chiffrement de bout en bout notamment. Ces mesures, proposées par le Sénat, n'ont pas été retenues.

En pratique, voici les principaux changements apportés par la LIL 2018 qui pourraient concerner les entreprises :

- **L'âge de la majorité** : La LIL 2018 fixe à 15 ans l'âge à partir duquel la base légale d'un traitement reposant sur le consentement est valide. C'est-à-dire qu'à partir de 15 ans, un individu peut donner son consentement librement. En dessous de cette limite, un consentement conjoint entre le mineur et son responsable légal est nécessaire. De plus, les mineurs de plus de quinze ans peuvent empêcher l'accès aux personnes exerçant l'autorité parentale à leurs données récoltées dans le cadre médical notamment lors d'une étude, évaluation ou un diagnostic. (Art. 59 de la LIL modifiée 2018).

- **L'action de groupe** : elle a été renforcée par le texte de loi. Les personnes concernées par une violation de données pourront obtenir la réparation des préjudices moraux et matériels subis, en plus d'obtenir la cessation du traitement. (Art. 43 de la LIL modifiée 2018). Ainsi, un groupe de personnes pourra intenter un procès aux entreprises en cas de non-conformité au RGPD, avec des sanctions cibles dissuasives pour une organisation.

- **Données à caractère particulier** : Le RGPD n'autorise le traitement de données à caractère particulier (données biométriques, origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de ces dernières) que sous certaines conditions précises. Cependant, la Loi Informatique et Libertés modifiée 2018 fournit des exceptions supplémentaires permettant de traiter des données à caractère particulier. De ce fait, les données biométriques, strictement nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans les missions des travailleurs, peuvent être traitées. Les données publiques disponibles dans les jugements et toutes les données anonymisées par un procédé conforme aux recommandations de la CNIL pourront également être manipulées. (Art. 8 de la LIL modifiée 2018)

- **Collectivités territoriales** : aucune aide financière ou exonération des sanctions pécuniaires n'est prévue comme le Sénat le suggérait. Cependant, l'Assemblée Nationale a expressément demandé à la CNIL de fournir des guides adaptés aux besoins des collectivités territoriales. De plus, ces dernières auront la possibilité de se doter d'un service unifié afin d'associer leurs traitements de données pour faciliter la mise en conformité au RGPD et partager la charge financière induite.

Ensuite, la LIL 2018 prévoit que l'autorité de contrôle compétente, la CNIL, puisse prononcer, après une procédure contradictoire, l'une ou plusieurs des mesures suivantes en cas de manquement à l'exercice d'un droit de la part d'un responsable de traitement :

- « Un rappel à l'ordre ;
- Une injonction de mettre en conformité le traitement avec les obligations résultant de la loi française ou du RGPD ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie d'une astreinte dont le montant ne peut excéder 100 000 euros par jour ;
- A l'exception des traitements qui intéressent la sûreté de l'Etat ou la Défense, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du règlement (UE) 2016/679 ou de la présente loi ;
- Le retrait d'une certification ou l'injonction, à l'organisme concerné, de refuser ou de retirer la certification accordée ;
- La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;
- Le retrait de la décision d'approbation d'une règle d'entreprise contraignante ;
- […] Une amende administrative ne pouvant excéder 10 millions d'euros ou […] 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux paragraphes 5 et 6 de l'article 83 du règlement (UE) 2016/679, ces plafonds sont portés respectivement à 20 millions d'euros et 4 % du chiffre d'affaires. »

D'autres ajouts ont également été effectués concernant la réglementation des traitements mis en œuvre par les tribunaux notamment. La version modifiée de la Loi Informatique et Libertés (LIL 3) a été validée par le Conseil Constitutionnel dans une décision du 12 juin 2018.

2. Un renforcement du droit des personnes sur leurs données personnelles

[RAPPEL] Le contenu de ce document n'a pas fait l'objet d'une analyse juridique et n'a pas valeur de conseil juridique. Il a été rédigé par des spécialistes de la sécurité informatique et de la gestion des risques.

2.1 Introduction aux droits des personnes sur leurs données personnelles dans le RGPD

Le Règlement Général sur la Protection des Données (RGPD) renforce le droit des personnes à disposer de leurs données personnelles en leur apportant des garanties supplémentaires à celles acquises par la loi Informatique et Libertés (LIL du 6 août 2004 - révisée) et la loi pour une république numérique (dite « Lemaire ») du 7 octobre 2016.

Ainsi, sur les 6 droits présents dans le Règlement (accès, rectification, effacement, limitation, portabilité, opposition – Cf. Chapitres 2.3 à 2.8 du présent cahier technique), le droit à la portabilité (Art. 20) est une nouveauté tandis que les autres ont été réaffirmés (Art. 15 et 16), ou sensiblement modifiés (Art. 18, 20, 21, 22). Les organismes sont tenus d'informer les personnes concernées de l'existence de ces droits de manière « concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ».

A titre d'illustration, voici un exemple de mention d'information conforme au RGPD, fourni par la CNIL sur son site internet :[4]

Vos droits :

Vous pouvez accéder aux données vous concernant ou demander leur effacement. Vous disposez également d'un droit d'opposition, d'un droit de rectification et d'un droit à la limitation du traitement de vos données (cf. cnil.fr pour plus d'informations sur vos droits).

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter gestionpersonnel@abcd.fr.

(NB : si la société ABCD avait un DPO, elle indiquerait :

Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter notre DPO.

- *Contacter notre DPO par voie électronique : dpo@abcd.fr*
- *Contacter notre DPO par courrier postal :*

Le délégué à la protection des données
Société ABCD
Rue la Transparence
96 000 CONFIANCE)

Figure 5 : Mention d'information

[4] Vous pouvez retrouver des exemples de mentions d'informations à l'adresse suivante : https://www.cnil.fr/fr/rgpd-exemples-de-mentions-dinformation

2.2 Quelles sont les personnes concernées par ces droits ?

La protection offerte par le Règlement s'applique à toutes les personnes physiques qui se trouvent sur le territoire de l'Union, indépendamment de leur nationalité ou bien dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union (cf. article 3 du RGPD).

2.3 Droit d'accès (Art. 15)

Présentation

L'article 15 du RGPD réaffirme, pour une personne, le droit d'accès à ses Données à Caractère Personnel (DCP), déjà présent dans la Loi Informatique et Libertés à l'article 39.

Chaque personne a le droit d'être informée par le responsable du traitement, des modalités de traitement de ses données et, le cas échéant, d'y accéder et de les connaître.

Ainsi les personnes peuvent demander (Art. 15) à tout moment :

- Quelles sont les **finalités** des traitements dont leurs DCP font l'objet,
- Quelles sont les **catégories** de DCP utilisées,
- Quels sont les **destinataires** (i.e. à qui sont communiquées les DCP) et/ou quelle est la source des données (d'où proviennent- elles ?),
- Quelle est la **durée** de conservation prévue pour ces DCP,
- Si une prise de décision automatisée est appliquée à leur cas dont le **profilage** et l'existence des droits qui lui sont accordés.

Le responsable de traitement est quant à lui soumis à **une obligation d'information** lorsqu'il collecte des données personnelles, que ce soit directement auprès des personnes concernées ou bien indirectement (Art. 13 & 14).

Par ailleurs, **toute personne concernée pourra demander une copie gratuite de ses données**, que le responsable de traitement devra lui fournir dans un format lisible et d'usage courant dans les meilleurs délais (**au plus tard dans un délai d'un mois après la demande**).

En pratique…

Opérationnellement, le RGPD apporte peu de modifications pour les organisations ayant déjà mis en place un processus permettant de répondre au droit d'accès prévu dans la LIL française. Il suffit d'adapter ce processus pour inclure les nouvelles exigences du RGPD en termes de droit d'accès.

Le régulateur précise, au paragraphe 4 de l'article 15, que le droit d'obtenir une copie des données ne doit pas porter « atteinte aux droits et libertés d'autrui ». Il incombe donc au responsable du traitement de s'assurer de l'identité du requérant. En effet, l'obtention par ce biais d'une copie des données d'autrui (ex. en se faisant passer pour elle) porterait directement atteinte à ses droits et libertés.

2.4 Droit de rectification (Art. 16)

Présentation

L'article 16 du RGPD réaffirme également le droit à la rectification de ses DCP déjà abordé dans la LIL française (Art. 40), et apporte peu de nouveautés par rapport à celle-ci. Cependant, la directive 2016/680 précise certains aspects : ce droit doit s'exercer « sans contrainte », « sans délai ou frais excessifs ».

2.5 Droit à l'effacement (ou « droit à l'oubli ») (Art. 17)

Présentation

En France, l'article 40 de la Loi Informatique et Libertés, prévoyait déjà que toute personne physique, justifiant de son identité, pouvait exiger du responsable d'un traitement que soient effacées les données à caractère personnel la concernant, quand elles étaient soit :

- Inexactes,
- Incomplètes,
- Equivoques,
- Périmées,
- Ou dont la collecte, l'utilisation, la communication ou la conservation étaient interdites.

Désormais, il est plus simple pour une personne physique d'obtenir ce droit à l'effacement ou à l'oubli dans des délais raisonnables.

Cependant celle-ci ne pourra pas user de ce droit si le responsable de traitement justifie qu'une conservation des données est légitime et notamment nécessaire à des fins d'archivage dans l'intérêt général. Par exemple, à des fins scientifiques, statistiques et historiques, ou pour des motifs d'intérêt public (ex : santé publique), ou bien pour respecter une obligation légale à laquelle il est soumis.

Quelles sont les personnes concernées ?

Dans la mesure où les conditions pour faire usage de son droit sont respectées, toute personne peut demander l'effacement de ses données, à la condition de prouver son identité, pour ne pas nuire à une personne tierce.

Cependant, les documents liés aux employés, factures, et autres documents devant être légalement conservés ne pourront être supprimés (cf. §1.2 conditions de licéité du traitement).

En pratique…

A la demande de la personne concernée, le responsable du traitement est tenu, dans les meilleurs délais, avec un mois au maximum, d'effacer les données à caractère personnel.

Néanmoins, le régulateur a prévu une obligation pour le responsable du traitement de mettre en œuvre des « moyens raisonnables y compris d'ordre techniques » (Art. 17, paragraphe 2) pour permettre l'exercice de ce droit.

Il est cependant difficile d'interpréter la notion de « moyens raisonnables » et de savoir ce qu'attend l'autorité de contrôle sur ce point. Il est donc préférable de prévoir des processus de transmission et d'effacement au sein de l'organisation ainsi que chez ses sous-traitants.

2.6 Droit à la limitation du traitement (Art. 18)

Présentation

Cet article est la continuité de l'article 40 de la Loi Informatique et Libertés et prévoit la limitation temporaire des traitements dans quatre cas très spécifiques :

- Lorsque la personne concernée conteste l'exactitude d'une donnée, le temps que le responsable du traitement puisse contrôler cette exactitude.
- Si le traitement est illicite mais que la personne concernée s'oppose à l'effacement de la donnée (ex : elle constitue un élément de preuve dans le cadre d'une action en justice).

- Lorsqu'elles ne sont plus nécessaires à l'organisation mais que la personne concernée a besoin de ses données pour la constatation, l'exercice ou la défense de ses droits en justice.
- Le temps nécessaire à l'examen du caractère fondé d'une demande d'opposition due à la situation particulière de la personne (Art. 21 du RGPD), c'est-à-dire le temps de procéder à la vérification des intérêts légitimes du responsable de traitement (ex. profilage nécessaire à une mission d'intérêt public).

Le considérant 67 du Règlement précise que le choix technique pour limiter le traitement est à la charge du responsable de traitement et peut inclure :

- Un déplacement temporaire des données vers un autre système ;
- Un verrouillage des données les rendant inaccessibles ;
- Un retrait temporaire de données publiées sur un site internet.

Si le responsable de traitement vient à lever la limitation, il doit préalablement informer la personne concernée de cette action.

En pratique…

Il est supposé que la majorité des demandes viendront de personnes se plaignant :

1. de l'intérêt légitime du traitement ;
2. du service rendu en souhaitant faire valoir leurs droits devant les juridictions.

Il est donc nécessaire d'avoir un **processus opérationnel** et fonctionnel, écrit et partagé, afin de ne pas se voir reprocher, en plus de la plainte initiale, l'impossibilité pour l'organisation de faire valoir les droits des personnes concernées par ces traitements (ou un délai trop long pour répondre aux

2.7 Droit à la portabilité des données (Art. 20)

Présentation

Ce droit prévoit que la personne concernée puisse récupérer les données personnelles fournies (dans le cadre d'un consentement ou d'un contrat) à un responsable de traitement, et les réutiliser à d'autres fins, sans que le premier ne puisse s'y opposer.

Ce droit n'impacte pas les autres droits découlant du RGPD (droit à l'effacement, à l'opposition…). La portabilité n'entraîne pas automatiquement le droit à l'effacement et n'altère pas non plus la durée initiale de rétention des données. Ainsi, la

personne concernée peut exercer ses droits, tant que le responsable continue de traiter ses données personnelles.

Ce droit a été initialement prévu pour faciliter l'accès aux données à des nouvelles entreprises (start-up, télécoms …). Par exemple, un assuré pourrait demander à son assureur d'exporter ses données (contrat, ...), en vue de demander à une société qui compare les contrats, de lui indiquer les assureurs présentant de meilleures garanties, ou de meilleurs tarifs.

Les données personnelles concernées

La Commission Nationale de l'Informatique et des Libertés (CNIL) précise que les données considérées comme « fournies par la personne concernée » sont :

- « Les données déclarées activement et consciemment par la personne concernée, telles que des données fournies pour créer un compte en ligne (ex. adresse électronique, nom d'utilisateur, âge) » ;
- « et les données générées par l'activité de la personne concernée, lorsqu'elle utilise un service ou un appareil (par exemple : les données brutes collectées par des compteurs communicants, les achats enregistrés sur une carte de fidélité, l'historique des recherches faites sur internet, les relevés de compte bancaire, les courriels envoyés ou reçus, etc.). »

Les données personnelles exclues du droit à la portabilité

Ce droit ne s'applique pas sur « les données personnelles dérivées, calculées ou inférées » créées par l'organisme à partir des données fournies par la personne concernée. Ainsi, si l'organisme dessine le profil d'une personne à partir des données personnelles qu'elle a fournies, alors ces « nouvelles » données seront exclues du droit à la portabilité puisqu'elles n'ont pas été transmises par la personne concernée.

La CNIL précise que les données traitées par les établissements financiers, dans le cadre de la lutte contre le blanchiment, ne sont pas concernées par le droit à la portabilité. De même, que les données des employés traitées par les employeurs sur la base d'un intérêt légitime ou d'obligations légales.

En pratique…

Le G29 (voir Glossaire) recommande de proposer gratuitement et directement aux personnes de pouvoir télécharger leurs données fournies initialement sur un format traditionnel afin de faciliter leur portabilité.

Néanmoins ce service ne permettra pas à des personnes d'exiger l'obtention des données qui n'ont pas été fournies directement à l'organisme, par exemple, les données générées à la suite d'un profilage.

Il est probable que des demandes de portabilité auront principalement lieu afin de changer de fournisseur, donc de responsable de traitement, en cas de mécontentement (par exemple, suite à un refus d'indemnisation, …).

La réponse à une demande de portabilité

Une exigence importante de ce droit est l'interopérabilité, ou l'obligation de fournir les données dans un « format structuré, couramment utilisé et lisible par machine ».

Le G29 propose que la personne puisse avoir la possibilité de télécharger ses données directement en ligne. Dans tous les cas, le moyen de récupérer les données personnelles doit être aisément utilisable et permettre une transmission sécurisée. Ainsi, l'organise est tenu de simplifier l'accès au droit à la portabilité.

2.8 Droit d'opposition (Art. 21 & 22)

Présentation

Ce droit est présenté dans deux articles distincts du RGPD : l'article 21 relatif au droit d'opposition et l'article 22 traitant du droit de refuser les décisions individuelles automatisées.

Le droit d'opposition existe déjà dans la Loi Informatique et Libertés du 6 janvier 1978 modifiée (Art. 38). Sur ce point, le droit français est plus contraignant que le nouveau règlement car il impose aux personnes concernées de justifier d'un « intérêt légitime ».

Cas d'opposition d'un traitement de données :

Cas d'opposition	Référence	Conséquences
Une personne concernée a le droit de s'opposer pour des raisons tenant d'une situation	Article 21 du RGPD – paragraphe 1 (Article 6, paragraphe 1,	Le responsable de traitement ne traite plus les données à moins qu'il démontre qu'il

particulière à un traitement des données personnelles (ou la personne concernée est un enfant)	points f))	existe des motifs légitimes pour le traitement et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée.
Dans le cas où le traitement est licite et nécessaire (pour une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement par exemple), les personnes devraient avoir le droit de s'opposer au traitement de données en rapport avec leur situation personnelle lorsqu'elles en font la demande.	Article 21 du RGPD – paragraphe 1 (Article 6, paragraphe 1, points e))	
Il est également possible pour la personne concernée d'exercer son droit d'opposition pour des traitements effectués, par exemple, à des fins de prospection y compris le profilage dans la mesure où il est lié à une telle prospection.	Article 21 – Paragraphe 2,3	Les données personnelles ne sont plus traitées à ces fins

En pratique…

Le droit d'opposition doit être clairement notifié à toute personne physique au moment de la collecte de ses données personnelles, de façon décorrélée de toute autre communication.

Généralement, l'exercice de ce droit peut se traduire par la possibilité de la personne concernée d'un désabonnement (en cliquant sur les un lien « se désabonner ») si elle ne souhaite pas ou plus que ses données soient conservées pour des traitements (par exemple, la réception de la publicité par mail).

Par ailleurs, le consentement donné initialement doit pouvoir être retiré à tout moment par la personne concernée au obligeant le responsable à arrêter le traitement de ses données personnelles (Cas où la base légale du traitement repose sur le consentement). Il faut donc prévoir que la personne physique puisse décocher cette case, ou prévoir un processus simple et sans délai excessif pour qu'elle puisse exercer son droit de retrait

3. La responsabilité portée par l'entreprise

3.1 Principe de Responsabilité/Accountability

Une des modifications introduites par le législateur via le règlement européen 2016/679 est la notion d'« accountability »/« responsabilité ».

Cette notion se retrouve à l'article 5 paragraphe 2 du RGPD : « Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité) ».

Le responsable du traitement est garant de la conformité aux six principes présentés au paragraphe 1 de l'article 5 du RGPD qui sont :

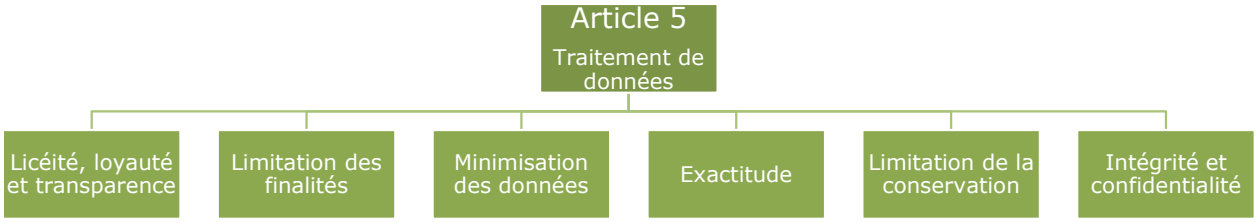


Figure 6 : Six points clés à respecter pour le responsable de traitement (« Accountability »)

Le responsable de traitement doit pouvoir assurer et être en capacité de démontrer sa conformité de tous les traitements de l'organisation à l'ensemble du RGPD.

En effet, en abandonnant le système de la déclaration systématique et préalable à la CNIL, et en demandant maintenant aux entreprises ou organismes de **se porter garants,** et d'**être en capacité de démontrer, sur demande, qu'elles respectent la conformité au réglement,** le RGPD introduit en filigrane, et sans le définir, un processus d'« auditabilité ».

Pour les entreprises, **l'auditabilité** s'appuie sur trois piliers :

- La documentation,
- Les contrôles
- Les preuves.

Les points majeurs sur lesquels l'organisation devra se concentrer pour démontrer sa conformité sont :

- La documentation sur les traitements des DCP :
  - Registre des traitements, analyses d'impacts relatives à la protection des données, transferts de données hors UE.
- L'information relative aux personnes :
  - Mentions d'information, procédure de recueil des consentements, procédure d'exercice des droits.

- Les contrats avec les sous-traitants (article 28 du RGPD) :
    - Obligations, matrice des responsabilités ;
    - Les procédures internes et les preuves associées.

Avec ce processus d'auditabilité, le RGPD (Art. 40, 41, 42 et 43) encourage l'élaboration de codes de conduite et de certifications qui faciliteront la démonstration de la conformité en cas de contrôle.

3.2 Amendes et Sanctions

Le RGPD mentionne en son article 79 que les personnes concernées, si elles estiment que des droits conférés par le Règlement sont violés, peuvent intenter des actions devant les juridictions de leur Etat ou de l'Etat membre dans lequel le responsable du traitement ou son sous-traitant disposent d'un établissement. Les personnes concernées peuvent également donner mandat à un organisme, une organisation ou une association à but non lucratif pour les représenter et faire valoir leurs droits. A ce titre, en France, l'Assemblée nationale a adopté le principe des actions de groupes (« class action ») dans la nouvelle version de la Loi Informatique et Libertés.

En cas de dommage en raison de manquements au RGPD, la personne concernée peut obtenir réparation du préjudice de la part du responsable de traitement ou du sous-traitant. Ces derniers peuvent être tenus responsables du dommage causé et faire l'objet de sanctions administratives.

Le Règlement prévoit, à l'article 58, paragraphe 2, points « a » à « h, » un premier volet de mesures « correctrices ». Ces mesures ont plusieurs niveaux, notamment l'avertissement, l'injonction de mise en conformité, le retrait de certification, l'effacement des données ou encore la suspension des flux de données. L'article 83 prévoit également des amendes administratives dont le montant varie selon les manquements constatés. Cet article laisse aussi aux Etats membres la possibilité de compléter les sanctions, en particulier pour les violations, et rappelle que la fixation de l'amende doit tenir compte d'éléments aggravants et atténuants.

En pratique…

En pratique, en France, rien ne change, sauf le montant des amendes (et donc le risque supporté en cas de non-conformité).

En effet, le texte de loi français relatif à la protection des données personnelles datant de mai 2018 (Loi Informatique et Libertés 3) et validé par le Conseil Constitutionnel le 12 juin 2018, prévoit que l'autorité de contrôle puisse prononcer, après une procédure contradictoire, l'une ou plusieurs des mesures suivantes en cas de manquement à l'exercice d'un droit :

1. « Un rappel à l'ordre ;
2. Une injonction de mettre en conformité le traitement avec les obligations résultant de la loi française ou du RGPD ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie d'une astreinte dont le montant ne peut excéder 100 000 euros par jour ;
3. A l'exception des traitements qui intéressent la sûreté de l'Etat ou la Défense, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du règlement (UE) 2016/679 ou de la présente loi ;
4. Le retrait d'une certification ou l'injonction, à l'organisme concerné, de refuser ou de retirer la certification accordée ;
5. La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;
6. La suspension totale ou partielle de la décision d'approbation d'une règle d'entreprise contraignante ;
7. […] Une amende administrative ne pouvant excéder 10 millions d'euros ou […] 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux paragraphes 5 et 6 de l'article 83 du règlement (UE) 2016/679, ces plafonds sont portés respectivement à 20 millions d'euros et 4 % du chiffre d'affaires. »

Les amendes administratives de l'article 83, en fonction des obligations non respectées, sont répertoriées dans le tableau ci-après.

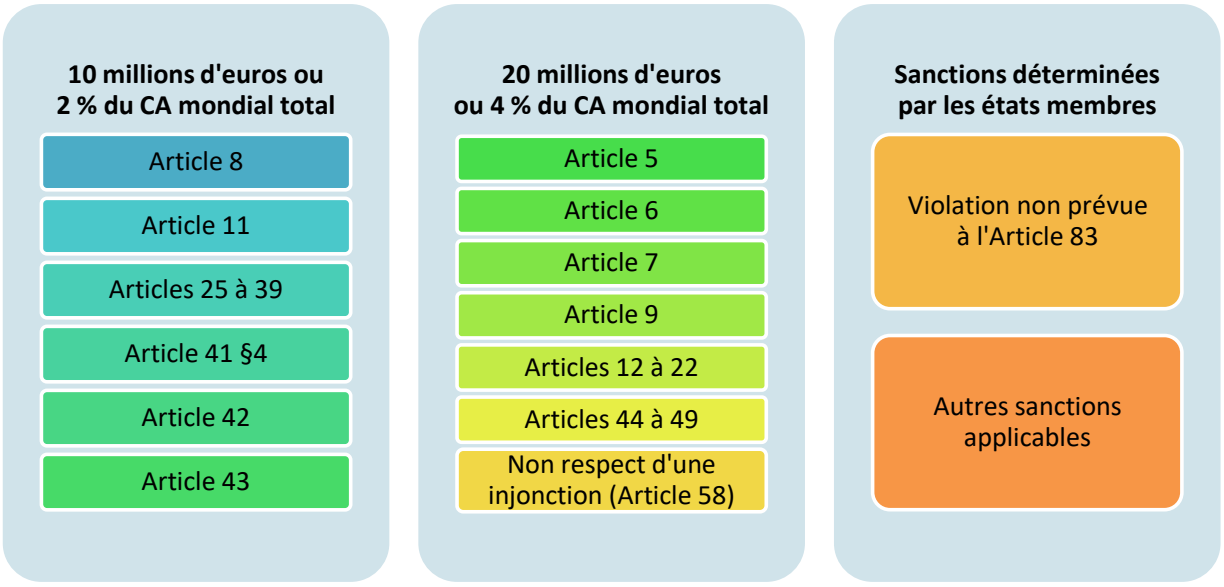


Figure 7 : Tableau de synthèse concernant les amendes administratives en cas de non-respect du RGPD

L'article 83, paragraphe 2, points « a » à « k », mentionne des éléments dont l'autorité devra tenir compte pour fixer les amendes administratives.

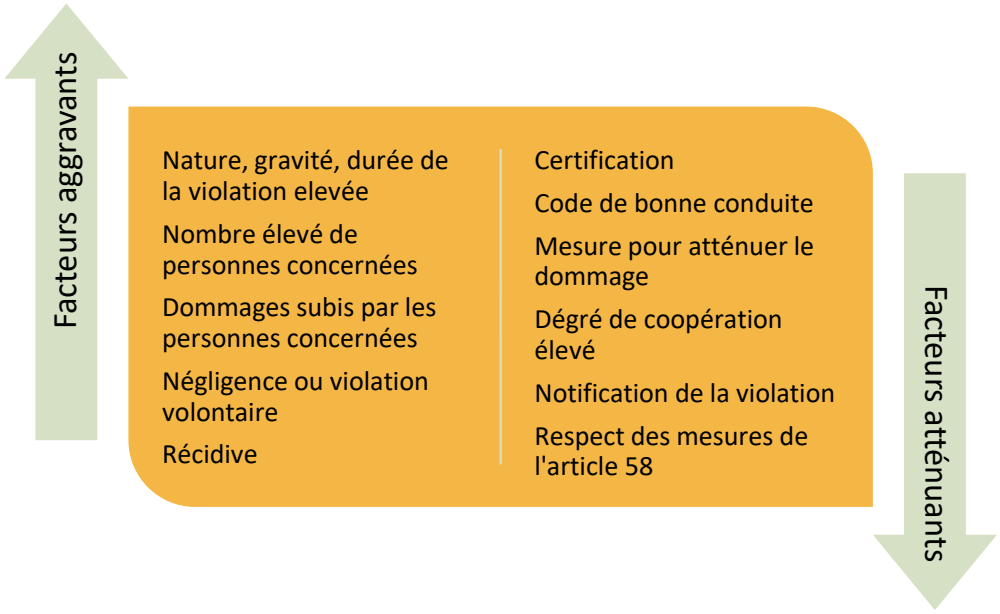


Figure 8 : Amendes : les facteurs atténuants et aggravants

L'assurabilité des amendes administratives reste, quant à elle, un sujet ouvert. En effet, au regard de la législation française, une amende n'est assurable que si elle est de nature civile et n'est pas assurable si elle est pénale.

Le statut de l'amende administrative n'est quant à lui pas arrêté. Sur ces bases, il semble qu'il faille attendre la jurisprudence et davantage d'informations pour savoir si ces amendes sont assurables ou non. L'étude DLA Piper et Aon a, quant à elle, révélé que seules la Finlande et la Norvège, parmi les pays étudiés, permettraient

d'assurer les amendes attribuées dans le cadre du RGPD[5]. 3.3 Risques pour l'organisation

Toutes les organisations sont visées (associations incluses), y compris celles localisées en dehors de l'Union Européenne, dès lors qu'elles traitent des données personnelles de résidents européens.

Afin de comprendre les risques pour l'organisation, il faut comprendre que la motivation du régulateur est de protéger les informations personnelles des résidents européens.

Impacts potentiels sur la vie privée

Les atteintes à ses données personnelles peuvent affecter directement chaque citoyen. En effet, une organisation qui ne maîtrise pas la disponibilité, l'intégrité ou la confidentialité des DCP fait porter un risque pour la personne concernée. De nombreux exemples récents illustrent cette tendance :

Exemples de cas	Exemples d'impacts pour les personnes concernées
Ashley Madison	Chantage ; divorce
Licenciement de 13 membres du personnel de cabinet de Virgin Atlantic – Facebook	Perte de travail
Celebgate	Sensation d'invasion dans la vie privée
Panama Papers, Paradise papers	Révélation de fraude fiscale ou d'optimisation fiscale
Cambridge Analytica – Facebook	Sensation d'invasion dans la vie privée et manipulation de l'opinion publique

Figure 9 : Exemples d'impacts sur les citoyens d'une défaillance de protection de leurs données personnelles

D'autres cas de fuites massives d'informations, contenant des données personnelles, ont été observés récemment au sein d'entreprises françaises (acteurs majeurs des télécoms ou de l'industrie) ou européennes. Pour autant, l'analyse d'impact sur le citoyen est rarement réalisée et encore moins rendue publique.

En retour, les conséquences pour les personnes impactées sont sources de risques pour l'entreprise impliquée, que ce soit en termes d'image, de sanction pécuniaire ou de procès (potentiellement en action de groupe).

L'impact pour l'organisation d'une défaillance de protection des données personnelles

[5] « The price of data security », DLA Piper & Aon, 16 mai 2018

Exemples de risques	Typologie d'impacts pour l'organisation
Perte de confiance des clients suite à une fuite massive de données	Image, réputation
Perte de marché suite au vol de la base de données des clients et prospects	Financier (perte de chiffre d'affaires)
Interruption des activités suite à une perte ou une corruption massive des données	Organisationnel, opérationnel
Traitements illicites constatés par l'autorité de contrôle (non-conformité au RGPD)	Juridique (cf. §3.2 Amendes & sanctions)

Figure 10 : Typologie d'impacts pour les personnes concernées ou pour l'entreprise

4. De nombreuses fonctions impliquées au sein de l'entreprise

Si les propriétaires des données personnelles sont directement identifiables (ex : collaborateur interne ou client externe concernés), les fonctions nécessaires à la mise en place et au maintien de la conformité de l'organisation au RGPD, telles que le responsable de traitement, le sous-traitant, le DPD (cf. Glossaire) et les contributeurs (ex : sponsor, chef de projet, responsable de processus), sont diverses et variées. Elles sont attribuées au sein des différentes Directions de l'organisation dont le rôle doit donc être précisé dans le cadre de la mise en place du projet.

4.1 La Fonction de DPD 

Le Règlement crée la nouvelle fonction de Délégué à la Protection des Données (DPD ou *Data Protection Officer* - DPO) identifiée au fil du document par cette icône : 

Cette fonction s'inscrit dans la continuité de la démarche initiée par les réglementations nationales, notamment la réglementation française avec le « Correspondant Informatique et Libertés » (CIL), instauré par la loi Informatique et Libertés de 1978. Si les deux fonctions peuvent paraître proches de prime abord, le DPD a, dans les faits, un rôle plus important au sein de l'entreprise. Le Risk manager peut, par exemple, être nommé DPD par l'organisation, comme toute autre personne de l'organisation disposant du profil adéquat, et en évitant les conflits d'intérêts (ex. : CIL, responsable juridique ou conformité, etc.). Les compétences requises et les missions qu'exerce le DPD sont explicitées au fil du présent cahier technique.

Trois articles du Règlement (37 à 39) sont dédiés à la présentation du DPD.
L'article 37 définit les modalités de désignation du DPD. Ces modalités peuvent être représentées comme suit :

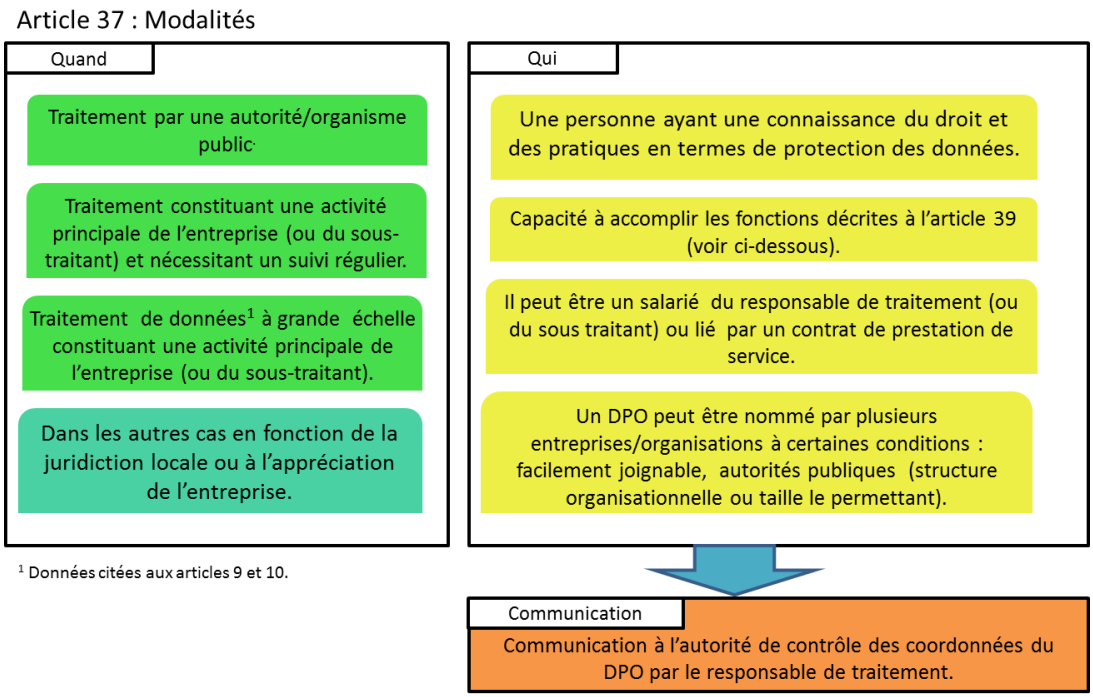


Figure 11 : Modalités de désignation du Data Protection Officer (DPO)

L'article 39 s'inscrit dans la continuité de l'article 37, et définit les fonctions du Délégué à la Protection des Données. Ces fonctions incluent :

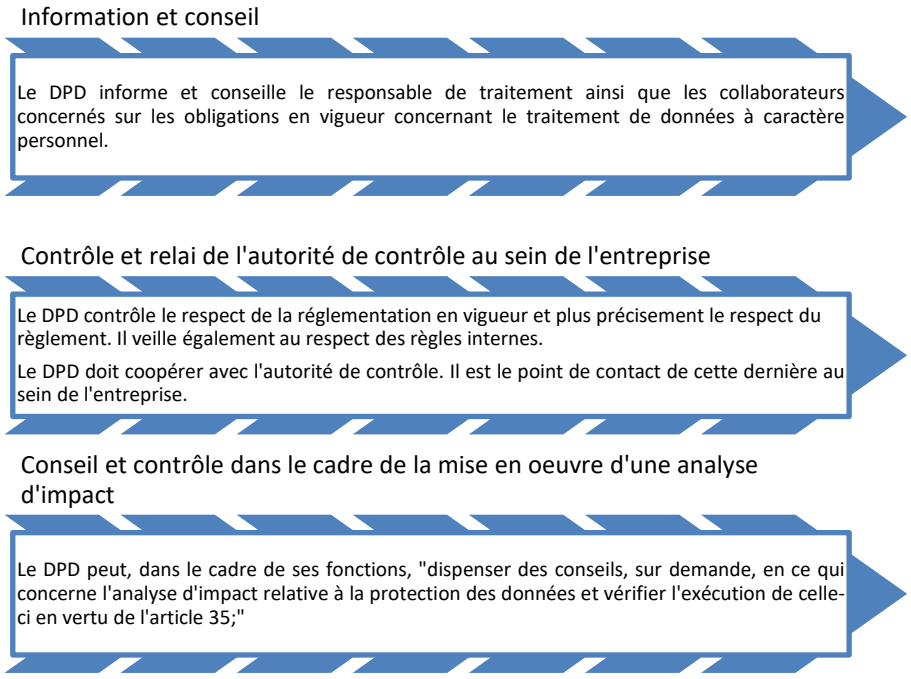


Figure 12 : Missions du Data Protection Officer (DPO)

L'article 38 définit les obligations auxquelles l'organisation doit se conformer. Ainsi, le responsable des données ou le sous-traitant, doit impliquer le DPD pour « toutes les questions relatives à la protection des données personnelles ».

En outre, cet article précise les dispositions que l'organisation doit mettre en œuvre afin de permettre au DPD de réaliser ses missions. Ainsi, le DPD doit se voir offrir les moyens et les ressources nécessaires à l'exercice de sa mission par la Direction de son organisation. Celle-ci doit également lui garantir une **indépendance hiérarchique**. Il doit reporter directement « au niveau le plus élevé de la Direction du responsable du traitement ou du sous-traitant » et ce afin de lui donner une large liberté d'action.

4.2 Directions Juridique et Conformité 

La Direction juridique, et/ou quand elle existe, la Direction de la conformité, sont des entités essentielles dans la mise en conformité au RGPD. Dans l'entreprise, elles sont bien souvent en charge, ou tout du moins sponsor majeur, du programme de mise en conformité au RGPD.

Mise en conformité au RGPD

Dans ce cadre, elles contribuent notamment à l'évaluation du niveau de conformité aux nouveaux droits, au renforcement des droits existants des personnes concernées (accès, mise à jour, portabilité…), à l'identification des traitements devant être mis à jour ainsi qu'aux modifications à apporter pour assurer la conformité au RGPD. En tant qu'entités responsables de la conformité des accords/contrats avec les sous-traitants, elles participent également à l'identification des prestataires traitant des données à caractère personnel pour l'entreprise.

Le texte laisse place à plusieurs interprétations, et bien que des lignes directrices soient éditées par le G29 (Cf. Glossaire) pour guider les organisations dans leur projet de mise en conformité, la Direction juridique a aussi un rôle primordial dans l'analyse des risques juridiques, pris ou à prendre par l'organisation.

Application de la règlementation RGPD dans les contrats

La Direction juridique est en charge, au sein de la société, de l'encadrement des relations contractuelles et contentieuses. A ce titre, elle a, en théorie du moins, une visibilité sur l'ensemble des données contenues dans les contrats. Il est donc primordial qu'elle intègre l'ensemble de la réglementation du RGPD dans ses activités, ainsi que dans celles des responsables opérationnels et sous-traitants.

Dans ce cadre, elle veille à la conformité des contrats, qu'ils concernent les salariés (en relation avec les RH), les partenaires de la société, les clients ou les prestataires (en relation avec les achats, commerciaux et opérationnels).

Contrat avec le sous-traitant

Elle doit également veiller, lors de la négociation du contrat avec un sous-traitant, à s'assurer du partage de la responsabilité avec ce dernier. En effet, l'article 28 du RGPD, relatif au sous-traitant, prévoit dans son premier paragraphe que le

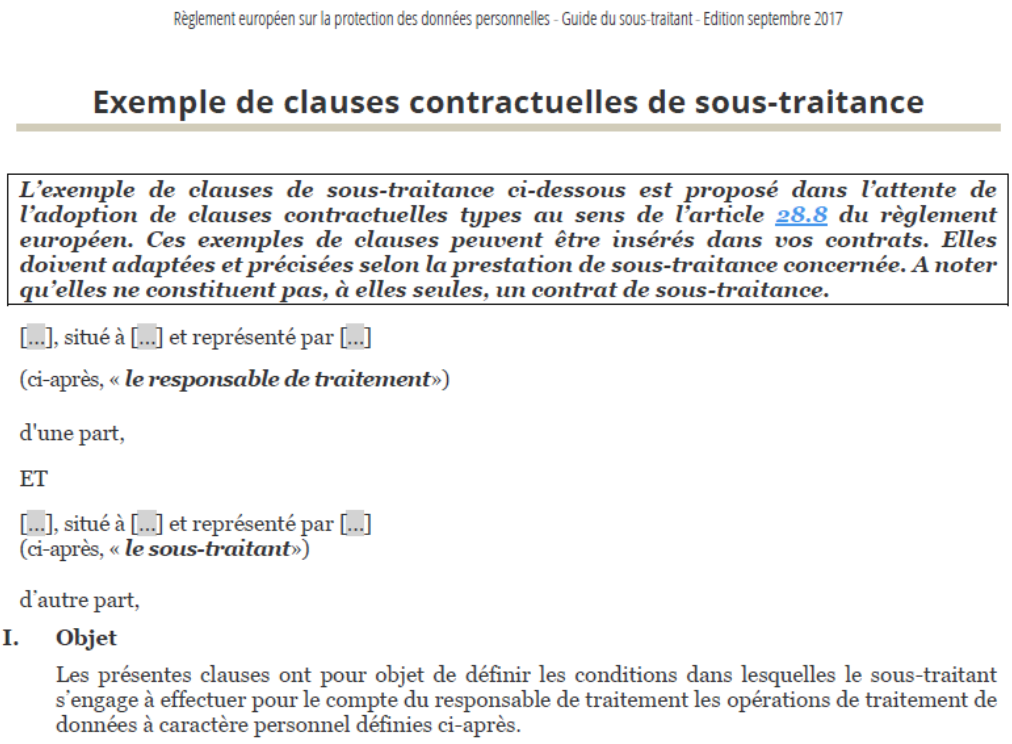
responsable de traitement doit faire « uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent Règlement et garantisse la protection des droits de la personne concernée » (Art. 28, paragraphe 1 RGPD).

Par ailleurs, le sous-traitant sera lié au responsable de traitement par un contrat, ou un autre acte juridique, qui doit définir « l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données et les catégories de personnes concernées, les obligations et les droits du responsable de traitement » (Art. 28.3 du RGPD).

Par conséquent, au regard de l'article 28 dudit Règlement, et en cas de violation du RGPD, un sous-traitant, qui aura déterminé les finalités et les moyens du traitement tels que mentionnés ci-dessus, sera considéré comme le responsable du traitement, pour ce qui concerne le traitement en question.

Notons, par ailleurs, que le sous-traitant doit tenir un registre des traitements qu'il effectue pour le compte du responsable de traitement (Art.30.2 du RGPD).

A titre d'illustration, voici un exemple de clause de sous-traitance élaborée par la CNIL dans son guide datant de septembre 2017 sur le sous-traitant[6] :



Règlement européen sur la protection des données personnelles - Guide du sous-traitant - Edition septembre 2017

Exemple de clauses contractuelles de sous-traitance

L'exemple de clauses de sous-traitance ci-dessous est proposé dans l'attente de l'adoption de clauses contractuelles types au sens de l'article 28.8 du règlement européen. Ces exemples de clauses peuvent être insérés dans vos contrats. Elles doivent adaptées et précisées selon la prestation de sous-traitance concernée. A noter qu'elles ne constituent pas, à elles seules, un contrat de sous-traitance.

[...], situé à [...] et représenté par [...]

(ci-après, « ***le responsable de traitement***»)

d'une part,

ET

[...], situé à [...] et représenté par [...]
(ci-après, « ***le sous-traitant***»)

d'autre part,

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Figure 13 : Clause de sous-traitance entre le responsable de traitement et son sous-traitant

[6] Cette clause est disponible au lien suivant : https://www.cnil.fr/sites/default/files/atoms/files/rgpd-guide_sous-traitant-cnil.pdf

Transferts de données hors de l'Union européenne

Le service juridique doit également anticiper, dans la rédaction des contrats cadres ou autres, les conditions de transferts de données à caractère personnel hors de l'Union européenne, notamment en prévoyant la rédaction de règles d'entreprise contraignantes (Art. 47 *Binding Corporate Rules* – BCR, RGPD). Il s'agit de règles internes permettant d'encadrer les transferts de données personnelles en dehors de l'Union européenne, et de garantir à la personne concernée par le traitement une protection adéquate de ses données.

Etant bien souvent en charge des litiges, dont ceux autour des questions de protection des données à caractère personnel, la Direction juridique doit être vigilante en rédigeant les clauses des différents contrats. Elle doit anticiper les conséquences pour l'entreprise d'une éventuelle violation du RGPD, en prenant en compte la dimension internationale de l'organisation, l'éventuel recours à de la sous-traitance…

En l'absence de DPD au sein de l'organisation, la Direction juridique répondra aux demandes de l'autorité de contrôle concernant la conformité de l'entreprise au RGPD. Ainsi, par exemple, le consentement recueilli au travers du contrat permettra de prouver à l'autorité de contrôle la licéité du traitement de données à caractère personnel.

Notification des droits et recueil du consentement

La Direction juridique doit être vigilante, non seulement lors de la rédaction des contrats, mais aussi lors de la rédaction des conditions générales de vente ou des conditions générales d'utilisation, et doit s'assurer de la prise en compte du RGPD.

Au regard du principe de transparence des informations et des communications énoncé à l'article 12 du RGPD, il devra être exprimé clairement dans ses conditions de vente, l'existence de l'opération de traitement et ses finalités, afin que la personne concernée soit informée de l'utilisation de ses données personnelles :

« Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 ainsi que pour procéder à toute communication au titre des articles 15 à 22 et de l'article 34 en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples… » (Art. 12.1 du RGPD).

Selon l'article 13 paragraphe 1, point c) du RGPD, le fondement juridique du traitement devra être indiqué à la personne concernée. Cette exigence étant une nouveauté par rapport à la loi « Informatique et Libertés », la Direction juridique devra déterminer la base juridique des traitements réalisés avant l'application du RGPD et préciser, à partir de mai 2018, ce fondement dans les conditions générales de ventes/d'utilisation et les formulaires de collecte de DCP. Pour rappel, le traitement doit au moins répondre à une base légale parmi les six fixées par le

RGPD dans son article 6 relatif à la licéité du traitement (cf. conditions de licéité du traitement §1.2 du présent cahier technique).

Rôle de conseil et d'accompagnement de la direction juridique

La Direction juridique, en plus de sa mission contractuelle, a un rôle de conseil, de sensibilisation et d'accompagnement des opérationnels (métiers) pour toutes les questions relatives à la réglementation sur la protection des données.

Elle est en charge de la rédaction de guides de bonnes pratiques en la matière, et notamment de la transposition du code de conduite, s'il en existe un.

Le code de conduite, défini à l'article 40 du RGPD, est destiné à contribuer à la bonne application du RGPD. Chaque code de conduite est élaboré par des groupements d'entreprises, en fonction des spécificités sectorielles des traitements des données, et des besoins des entreprises. Ce code est soumis à l'autorité de contrôle du pays concerné (en France, la CNIL), qui émet un avis sur la question de savoir si le projet de code respecte le RGPD. Il sera alors approuvé « si elle estime qu'il offre des garanties appropriées suffisantes » (Art. 40, paragraphe 5 RGPD).

L'objectif de ce document est de préciser les modalités d'application dudit Règlement, telles que « le traitement loyal et transparent, les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques, la collecte de données, les informations communiquées au public et aux personnes concernées… » (Art. 40.2 du RGPD).

Par ailleurs, la rédaction et l'application du code de conduite approuvé revêtent un intérêt particulier pour l'organisation, puisque l'existence de ce code lui permet de démontrer la volonté de respecter les obligations incombant au responsable de traitement (Art. 24.3 du RGPD). Ce principe s'applique également pour le sous-traitant. En effet, l'application par un sous-traitant, d'un code de conduite approuvé par l'autorité peut servir d'élément pour démontrer l'existence de garanties suffisantes (Art. 28.5 du RGPD).

D'autre part, en ce qui concerne le transfert de données à caractère personnel en dehors de l'Union Européenne, le code de conduite approuvé, accompagné de l'engagement contraignant et exécutoire pris par le responsable du traitement, ou le sous-traitant dans le pays tiers, constitue une garantie appropriée et permet alors le transfert des données vers un pays tiers (Art. 46.2.e du RGPD).

Rôle de la Direction juridique pour assurer la protection des données dès la conception (« Privacy by design »)

La protection des DCP doit être intégrée en amont de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le traitement des données à caractère personnel.

La Direction juridique devra proposer des solutions aux problèmes rencontrés et inciter les opérationnels, prestataires de services et producteurs d'applications à

prendre en compte le droit à la protection des données dès l'élaboration de nouveaux produits et/ou services.

4.3 Direction des Systèmes d'Information 

La Direction des Systèmes d'Information (DSI) joue un rôle important dans la mise en œuvre de la conformité qui est le plus souvent un rôle d'accompagnement des métiers et de maîtrise d'œuvre des mesures à appliquer. En effet, de nombreuses actions techniques sont à mener par l'organisation pour être en conformité avec les articles traitant : de l'exercice des droits (Art. 15 à 22 du RGPD), des outils de gestion des registres (Art. 30 du RGPD), de la gestion des notifications/communications en cas de violation des données (Art. 33 et 34 du RGPD), de l'assistance à fournir aux responsables de traitement dans les analyses de risques au sein des PIA ou AIPD (Art. 35 du RGPD), et bien sûr la sécurisation de systèmes d'information (Art. 32 du RGPD).

Implémentation technique des droits

Certaines organisations choisiront de simplifier l'exercice des droits en l'automatisant, par exemple, en donnant directement un accès à leurs données, via un site Web, aux personnes concernées.

La DSI doit accompagner les métiers et la Direction juridique pour formaliser les spécifications de ces outils, s'assurer que les demandes d'exercice des droits sont bien honorées et s'assurer que les demandes d'opposition, limitation ou suppression sont bien répercutées dans le système d'information, et auprès des sous-traitants concernés.

Implémentation des outils de registre

L'inversion de la charge de la preuve rend désormais nécessaire l'utilisation, par les responsables de traitement, d'outils dédiés pour conserver les traces qui démontreront la conformité des traitements.

La DSI a alors, *a minima,* un rôle d'accompagnement auprès des Directions dans le choix d'un outil adapté à l'organisation, sa taille et sa complexité (Voir chapitre Registre pour davantage de détails).

Gestion des notifications/communications

Le nouveau délai de notification à l'autorité de contrôle en cas de violation (72 heures maximum), et les modalités de communication imposées à l'organisation (sous conditions) auprès des personnes concernées, obligent les Directions à préparer une procédure de gestion de ces violations, qui peut être directement intégrée à la procédure de gestion de crise, si elle existe. Elle nécessite des moyens techniques, humains et financiers pour pouvoir répondre dans les délais impartis

aux demandes de l'autorité et fournir toutes les informations demandées. L'ENISA (Cf. Glossaire) a mis à disposition un outil de notification (à destination des autorités de contrôle), et des éditeurs de logiciel proposent également déjà des solutions.

Mener les Analyses d'Impact relative à la Protection des Données (AIPD)

Selon les organisations, les Analyses d'Impact relatives à la Protection des Données peuvent être confiées à d'autres Directions (DPD, Risques, etc.) que la DSI. Dans tous les cas, il sera nécessaire que la DSI intervienne pour indiquer les mesures techniques déjà en place et implémenter les mesures supplémentaires qui seraient nécessaires.

Sécuriser le système d'information

Pour mettre en place une solution de pseudonymisation, de chiffrement, et implémenter les autres chantiers identifiés lors des AIPD, la DSI aura besoin de moyens techniques, humains et financiers, pour préparer la mise en conformité du SI puis, pour maintenir cette conformité dans le temps.

4.4 Direction des Risques

La Direction des Risques, et en particulier le Risk manager, est également concernée par le RGPD. Cette Direction peut, par exemple, être en charge de mener une cartographie des risques d'entreprise et faire ainsi apparaître, s'ils n'ont pas été identifiés préalablement, de nouveaux risques liés à la protection des données personnelles des clients ou collaborateurs (le risque de non-conformité n'existant pas par essence), ou *a minima* d'en réévaluer la criticité (Cf. 3.3 Risques pour l'organisation).

Les risques, ayant un impact sur la vie privée des clients ou des collaborateurs, doivent également en toute logique trouver leur place dans cette cartographie globale et impliquer un pilotage spécifique par la Direction des Risques. DPD, coordinateur ou simplement contributeur, le Risk manager verra son rôle évoluer pour prendre en compte et gérer ces nouveaux risques qui pèsent sur le citoyen et de plus en plus fortement sur l'entreprise. Ceci peut également conduire à revoir ou compléter le dispositif assurantiel de l'organisation, le cas échéant par la mise en place d'une police d'assurance « Cyber » offrant entre autres garanties des services d'assistance à la gestion de crise en cas de fuite de données personnelles, ainsi que la prise en charge des frais liés aux notifications à effectuer, etc.

4.5 Les Directions du Contrôle interne, RH et autres Directions

Ces Directions jouent un rôle essentiel comme contributeurs, même si elles sont plus rarement les sponsors directs du programme de mise en conformité en question.

La Direction du contrôle interne

La Direction du Contrôle Interne a un rôle de suivi de la conformité.

C'est grâce à ses travaux que l'on récupérera notamment les éléments de preuve, qui pourront être présentés en cas de contrôle de l'autorité. Ainsi, chaque mesure, qu'elle soit, juridique, organisationnelle ou technique, doit faire l'objet d'un contrôle associé afin d'en garantir l'efficacité. Le nombre de contrôles a donc vocation à augmenter significativement à compter de ce jour. Les outils de GRC (Gouvernance, Risque, Conformité) ou de RPA (*Robotic Process Automation* - Automatisation de processus robotique) permettent dès aujourd'hui de faciliter le contrôle en automatisant les tâches à faible valeur ajoutée.

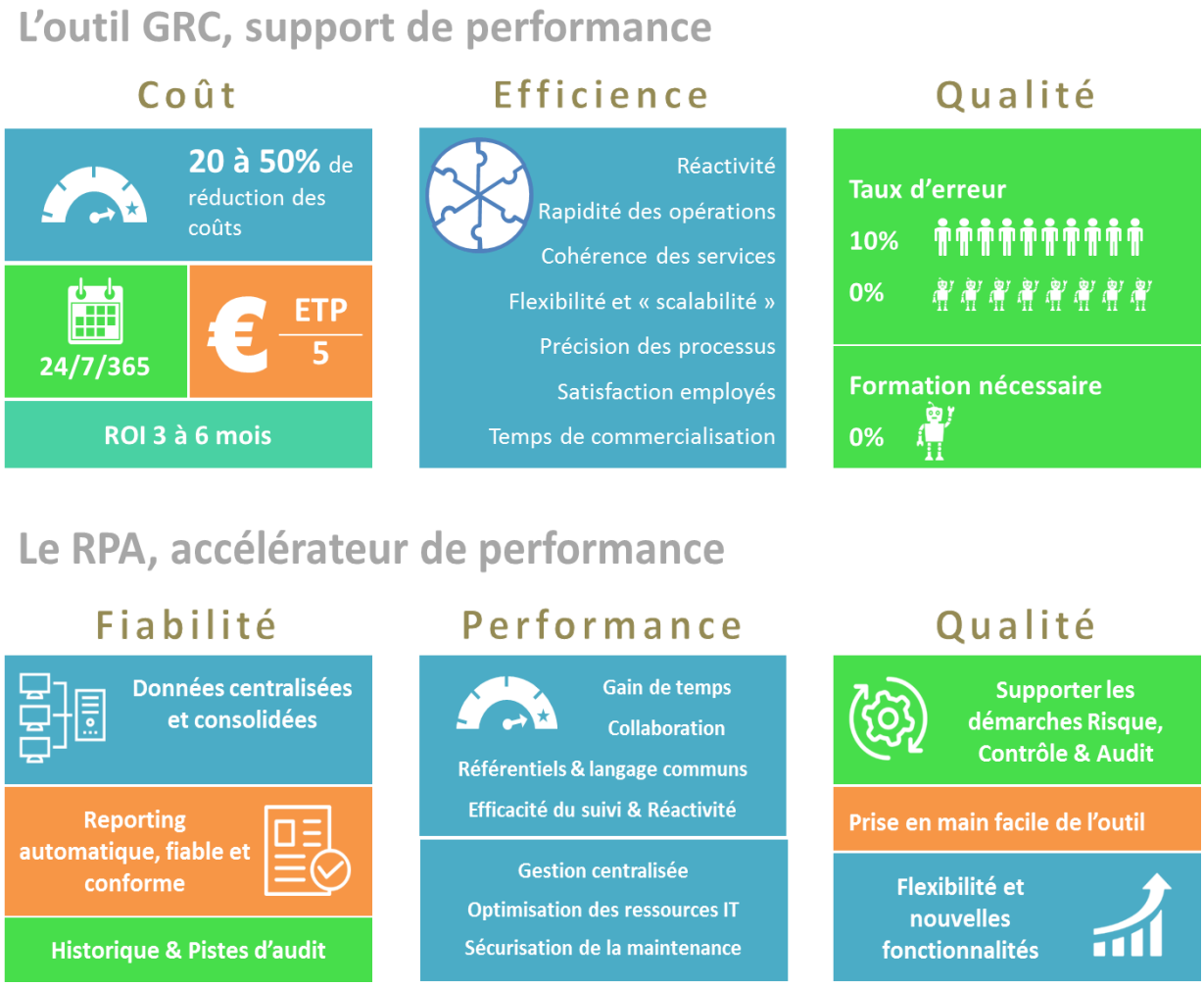


Figure 14 : GRC et RPA, des outils utiles dans le cadre du RGPD

En pratique…

Les acteurs de l'outillage de Gouvernance Risk Compliance (GRC) proposent depuis quelques mois ou années des modules permettant de gérer sa conformité à la loi I&L ou au RGPD.

Pour rappel, l'AMRAE publie chaque année un panorama des Systèmes d'Information de Gestion des Risques (SIGR http://www.amrae.fr/parution-du-panorama-sigr-2018)

La Direction des Ressources Humaines

Un sondage européen de SD Worx[7] du 28 novembre 2017 montre que 44% des collaborateurs des équipes de Ressources Humaines ne savaient pas, à cette date, ce qu'était le RGPD.

Cependant, c'est paradoxalement cette même fonction qui est en première ligne pour recruter les futurs DPD, ou autres acteurs de la conformité au RGPD.

De plus, la Direction des Ressources Humaines traitant les informations des employés, et bien souvent de leur famille proche, doit être intégrée aux processus de tenue des registres, et s'assurer de la protection de ces données : minimisation, disponibilité, confidentialité, intégrité.

Il est par ailleurs fort probable que dans nombre d'organisations, les Ressources Humaines soient le point de contact des employés pour ce qui est de l'exercice de leurs droits.

Les autres Directions (Marketing, Ventes, Achats, etc.)

Les autres Directions, utilisatrices des systèmes d'information, doivent également être mises à contribution dans la mise en conformité au RGPD.

Selon un récent sondage, les dirigeants français seraient nombreux (33 %) à ne pas savoir que des données marketing (ex : base de données clients) peuvent être considérées comme des données personnelles[8].

Pourtant, ces mêmes Directions génèrent régulièrement de **nouveaux traitements**, et à ce titre **peuvent être désignées comme responsables de traitement** : offres promotionnelles, profilage, registre des fournisseurs, contrôle

[7] https://www.sdworx.be/fr-be/sd-worx-r-d/publications/communiques-presse/2017-11-28-44-des-professionnels-en-ressources-humaines-en-europe-ne-connaissent-pas-le-rgpd

[8] http://www.zdnet.fr/actualites/le-rgpd-et-ses-impacts-sur-la-fonction-marketing-39861228.htm

anti-fraude, etc., autant de traitements qui nécessitent d'être connus et compris du DPO.

Ces Directions doivent *a minima* être mises à contribution à deux niveaux : lors de la conception du nouveau projet (« *Privacy by Design »),* ainsi que dans le combat contre le « *Shadow IT ».*

Il découle de l'obligation de « *Privacy by Design* » que les Directions Juridique et de Systèmes d'Information doivent être impliquées très tôt dans les projets, notamment pour évaluer les données qui seront traitées, et mettre en place les mesures juridiques et techniques appropriées. Seuls les métiers, initiateurs des projets peuvent garantir que ces Directions seront intégrées au juste moment.

Il est également indispensable de leur faire comprendre les nouveaux risques pesant sur les systèmes non maîtrisés : impossibilité de garantir la sécurité des données, impossibilité d'apporter les preuves nécessaires en cas de contrôle, voire de violation de données, avec des risques accrus si l'on regarde les sanctions prévues à l'Article 84 du Règlement.

5. Conduire le projet de mise en conformité de l'organisation

Le projet de mise en conformité RGPD implique une transformation majeure du rapport de l'organisation à la donnée, et nécessite l'implication de l'ensemble des parties prenantes et contributeurs cités précédemment :


Dir. Juridique
Directions


DSI


DPO


Dir. des Risques


Autres

En pratique, le rôle du Risk manager…

Evoqué dès la préface de ce Cahier Technique, le Risk manager peut parfois se voir confier le rôle de Délégué à la Protection des Données (DPD) ; son rôle est alors global puisqu'il doit assurer la conformité au RGPD et assurer le pilotage du projet de mise en conformité. Il interviendra dès lors sur tous les sujets de mise en conformité au RGPD.

De manière plus classique, le Risk manager s'attachera avant tout à traiter les sujets en rapport avec sa fonction. Son spectre d'intervention pouvant varier selon les organisations (voir la publication de l'AMRAE « Le Baromètre du Risk manager » - http://amrae.fr/barometre-du-risk-manager) son action peut donc, selon les cas, être particulièrement attendue sur les sujets suivants :

- **Gestion de crise** : il s'agit d'organiser la gestion de crise, y compris celle liée à une éventuelle fuite de DCP, lors de laquelle il faudra notamment : suivre les opérations de *forensics* (recherche de preuves sur un SI), informer les personnes concernées, notifier l'autorité du pays d'origine des personnes concernées, …
- **Relation avec les autorités** : en France, on pense avant tout à la relation avec la CNIL, mais on intégrera également les organismes tels que l'ANSSI qui publient des bonnes pratiques de sécurité ;
- **Cartographie globale des risques** : intégrer les risques d'atteintes aux données personnelles ;
- **Gestion des assurances**, y compris « cyber », pour mieux couvrir certains risques et fournir également via la police d'assurance Cyber des services additionnels à mobiliser (par exemple dans les premières heures), en support à la gestion d'une crise de cybersécurité ou lors d'analyse post-mortem en cas d'incidents, … ;
- **Conformité** : mise sous contrôle de la conformité au RGPD : contrôle

L'organisation doit tout d'abord définir ses ambitions quant à la mise en œuvre du RGPD, et donner les orientations ou piliers de ce projet de mise en conformité :

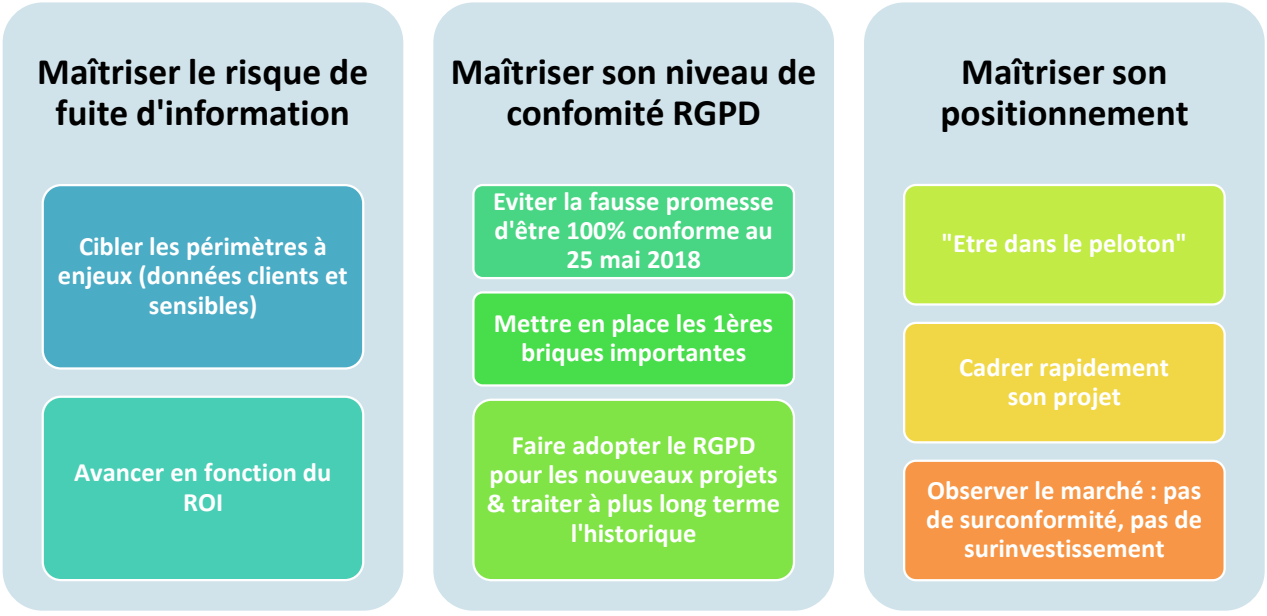


Figure 15 : Un projet de mise en conformité basé sur trois piliers

5.1 Le diagnostic initial

Il est nécessaire de réaliser **en premier lieu un diagnostic, ou état des lieux, du niveau de conformité de l'organisation au RGPD** pour mesurer l'effort à réaliser, et en prenant en compte les exigences ayant déjà été implémentées, notamment en vertu de la Loi Informatique et Libertés.

Ce diagnostic s'effectue généralement au travers d'une **analyse d'écarts** entre les exigences du RGPD et les mesures existantes dans l'organisation : modèle organisationnel, processus, corpus documentaire associé, outils, … La mise en conformité se traduit ensuite par un **plan de mise en conformité** intégrant un certain nombre de chantiers, définis en fonction des écarts observés précédemment, et priorisés dans le temps :

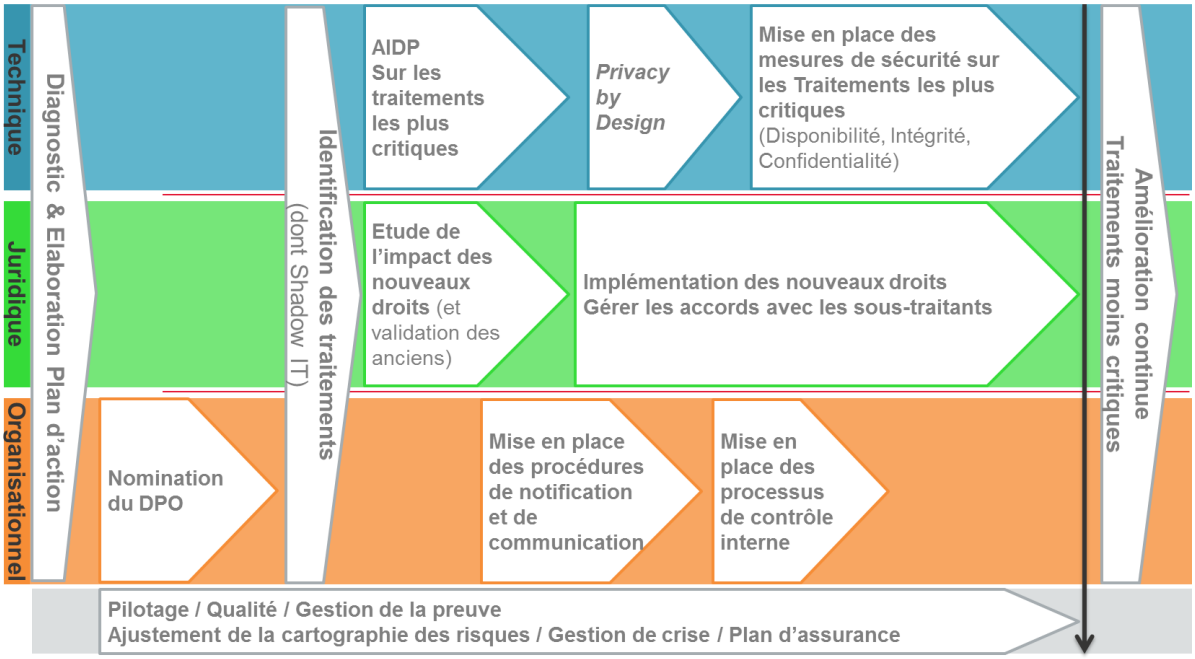


Figure 16 : Exemple de planning de mise en conformité d'une organisation

5.2 La nomination du Déléguà la Protection des Données (DPD)

La nécessité de nommer un DPD doit être étudiée dans les premières étapes d'un projet de mise en conformité RGPD. La fonction DPD est décrite plus en détail au chapitre 4.4 du présent Cahier.

Si l'organisation fait le choix de ne pas nommer de DPD, elle devra tout de même nommer une équipe ou une personne pour coordonner sa mise en conformité.

5.3 Le registre et l'identification des traitements

Le Règlement Européen sur la Protection des Données impose la tenue de deux registres et d'une information documentée :

- Le registre des traitements en tant que responsable de traitement ;
- Le registre des traitements en tant que sous-traitant ;
- L'information documentée des violations de données à caractère personnel.

Ces registres ne sont pas de simples documents, même si l'article 30 du Règlement, indique en son paragraphe 3 que cette documentation doit se présenter « sous une forme écrite y compris la forme électronique », laissant supposer qu'un registre papier pourrait être suffisant. Cette documentation contribue alors à fournir des éléments de preuve permettant de prouver et documenter la conformité des traitements mis en place par l'organisation (données collectées, destinataires,

durée de conservation des données, droits des personnes, sécurisations des données, etc.).Des éléments de preuve permettant de prouver …

A titre d'illustration un fac-similé du registre des traitements proposés par la CNIL est reproduit ci-après :

Fiche de registre ref-000

Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

Finalité(s) du traitement effectué	
Finalité principale	
Sous-finalité 1	
Sous-finalité 2	
Sous-finalité 3	
Sous-finalité 4	
Sous-finalité 5	

Mesures de sécurité	
Mesures de sécurité techniques	
Mesures de sécurité	

Catégories de données personnelles concernées	Description	Délai d'effacement
Etat civil, identité, données d'identification, images…		
Vie personnelle (habitudes de vie, situation familiale, etc.)		
Informations d'ordre économique et financier (revenus, situation		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM,		

Données sensibles	Description	Délai d'effacement
Données révèlant l'origine raciale ou ethnique		

Figure 17 : Registre proposé par la CNIL [9]

Les organisations de moins de 250 salariés sont dispensées de tenir les registres évoqués plus avant, « sauf si le traitement qu'elles effectuent est susceptible de comporter un risque pour les droits et les libertés des personnes concernées, s'il

[9] https://www.cnil.fr/fr/cartographier-vos-traitements-de-donnees-personnelles

n'est pas occasionnel ou s'il porte notamment sur les catégories particulières de données visées à l'article 9, paragraphe 1, ou sur des données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10. ». Cela ne dispense pas pour autant l'organisation de tenir l'information documentée concernant les violations des données à caractère personnel.

Le registre des traitements

C'est le pendant du registre tenu par le CIL jusqu'alors.

De nouveaux éléments font cependant leur apparition, tandis que d'autres disparaissent (le service chargé de la mise en œuvre par exemple). Un comparatif des deux registres (CIL et RGPD) est présenté ci-après :

Registre CIL	Registre des traitements (RGPD)
Un Registre tenu par le **CIL**	Un Registre tenu par le **Responsable** des traitements et/ou le représentant du Responsable s'il y en a un
Nom et adresse du Responsable	Nom et coordonnées du Responsable des traitements, du Responsable conjoint s'il y en a un et du délégué à la protection des données (cf. fonctions §4 ou Glossaire du présent Cahier Technique)
Finalité du traitement	Finalité du traitement
Service chargé de la mise en œuvre	N/A (possibilité de préciser un représentant du responsable de traitement, ou un responsable conjoint).
Fonction et coordonnées de la personne/service en charge de répondre aux demandes de droits d'accès et de rectification	Délégué à la protection des données (DPO)
Description des catégories de personnes concernées et des catégories de données	Description des catégories de personnes concernées et des catégories de DCP
Destinataires habilités	Catégories de destinataires (y compris pays tiers ou organisations internationales)
	Existence de garanties de sécurité pour les données transférées dans des pays tiers ou à des organisations internationales
Durée de conservation des données	Délais d'effacement des différentes catégories de données (si possible)
	Description des mesures de sécurité adaptées au risque (si possible)

Figure 18 : Comparaison registre CIL et registre des traitements.

Ce registre doit maintenant être exhaustif, puisqu'il pourra servir, en cas de contrôle à distance ou sur place, d'élément de preuve de la conformité au Règlement.

Il devient donc difficile pour une organisation de gérer ses traitements grâce à un tableur, type Excel, dans la mesure où avec ces outils l'on ne maîtrise pas forcément l'ensemble des composants du système d'information et le transfert des données entre systèmes (en interne comme en externe).

Trois solutions s'offrent alors aux organisations :

- Acquérir un outil du marché, dédié ou non à ce type de tâches ;
- Développer leur propre outil de tenue du registre ;
- Utiliser un outil de *Data Governance*.

Démarche	Explications	Avantages	Inconvénients
Acquisition d'un outil du marché	De nombreux outils de gestion des registres ont vu le jour sur le marché. Ils répondent à la grande majorité des besoins et proposent des outils souvent intuitifs	+ Des outils généralement intuitifs + Mise à jour selon les modifications de la loi	− Statique : difficile de faire passer ses propres besoins en développement − Intégration
Développement d'un outil propre à l'entreprise	Développer un outil permet à la solution de correspondre parfaitement aux besoins de l'organisation, dès lors que les spécifications sont biens définies en amont	+ Adaptation à l'organisation + Intégration dans le SI facilitée	− Il faut prendre des mesures adaptées : avoir des spécifications détaillées très proches des besoins des utilisateurs afin de limiter les coûts de mise à jour − Fort coût de maintenance
Tableur type « Excel »	Outil très peu couteux, et permettant de gérer une multitude d'options	+ Coût + De nombreuses possibilités de « développement »	− Long, très long à « développer », difficile à maintenir − Réversibilité quasiment impossible si le tableur comporte des données croisées − Problématique sur l'*accountability* / preuve −Défaut d'agilité
Outil de gouvernance de la donnée / MDM	Outil pouvant s'intégrer dans un projet de plus grande ampleur, et permettant de gérer dynamiquement ses données	+ Outil s'intégrant dans un projet de plus grande ampleur + Permet de faire tout ce que l'organisation souhaite : dynamisme du remplissage du registre	− Projet de grande ampleur, devant s'inscrire dans une véritable stratégie − Coût élevé

Figure 19 : Comparatif des différents types d'outils de registre

Le registre des sous-traitants

Le registre des sous-traitants n'est pas à tenir directement par le responsable du traitement, mais bien par ses sous-traitants qui agissent pour les besoins du responsable de traitement. Détaillé dans l'article 30, paragraphe 2, ce registre est légèrement plus léger que le registre des traitements.

Ce dernier regroupe 4 informations principales :

- Le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit […] ;
- Les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers […] ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques […].

5.4 Cybercrise & RGPD

Les récentes cyber attaques mondiales (Wannacry, NotPethya…) et plus particulièrement celles liées à la violation de données à caractère personnel (Uber, Twitter, Ashley Madison...) encouragent les entreprises et les organisations à structurer, harmoniser et améliorer leur dispositif de crise pour répondre à ce nouveau type de menace/attaque.

Les attaques cyber ont des caractéristiques différentes des autres types de crise : incertitude, difficulté à analyser la gravité de l'impact immédiatement, la nature humaine de l'attaque, la durée de la crise et l'impact médiatique éventuel nécessitant une stratégie de communication adéquate.

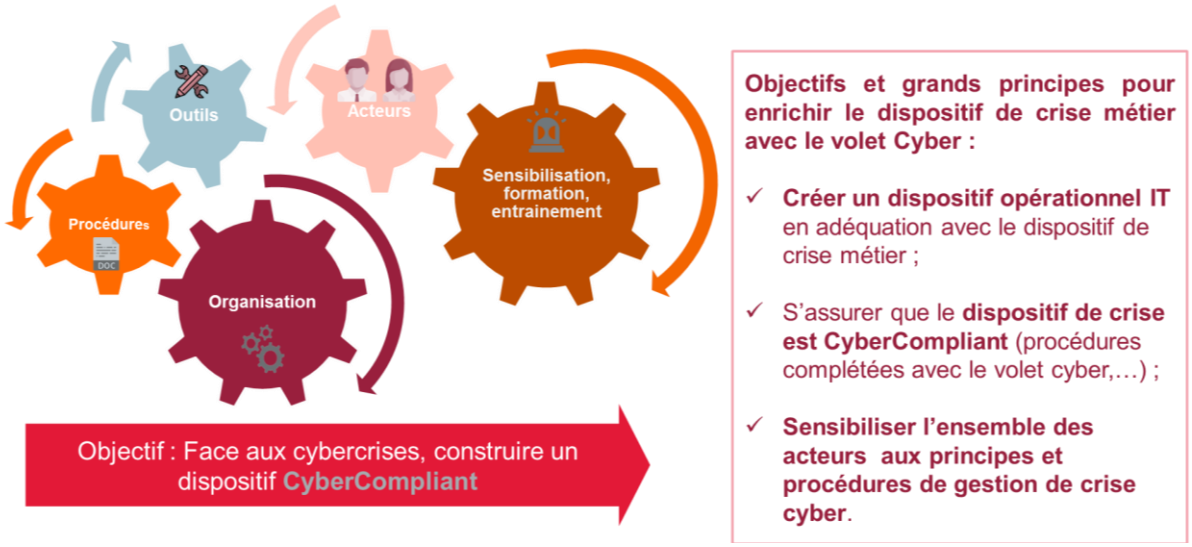


Figure 20 : Composants d'un dispositif de crise opérationnel

Elles nécessitent donc la mise en place d'un dispositif de crise spécifique et adapté dans lequel, chaque composant doit être *cyber compliant* (acteurs, procédures, organisation…).

Dès lors, des dispositifs de crise « cyber opérationnels » s'intègrent peu à peu dans les dispositifs de crise « métiers » existants (modèle miroir ou cellule centralisée au niveau des Directions des Systèmes d'Information) selon des principes structurants (permanence, transversalité, interaction, veille et auto activation…). (Cf. Dispositif de crise en cas de violation de données page suivante).

Le Règlement Général sur la Protection des Données (RGPD) entraîne de nouvelles obligations en cas de crise cyber et de violation de données à caractère personnel. Il s'agit de la notification à l'autorité de contrôle (CNIL), de la communication à la personne concernée et de la mise en œuvre de mesures d'urgence notamment.

Il apparaît donc nécessaire de faire évoluer chacun des composants du dispositif de crise cyber existant pour répondre aux exigences réglementaires.

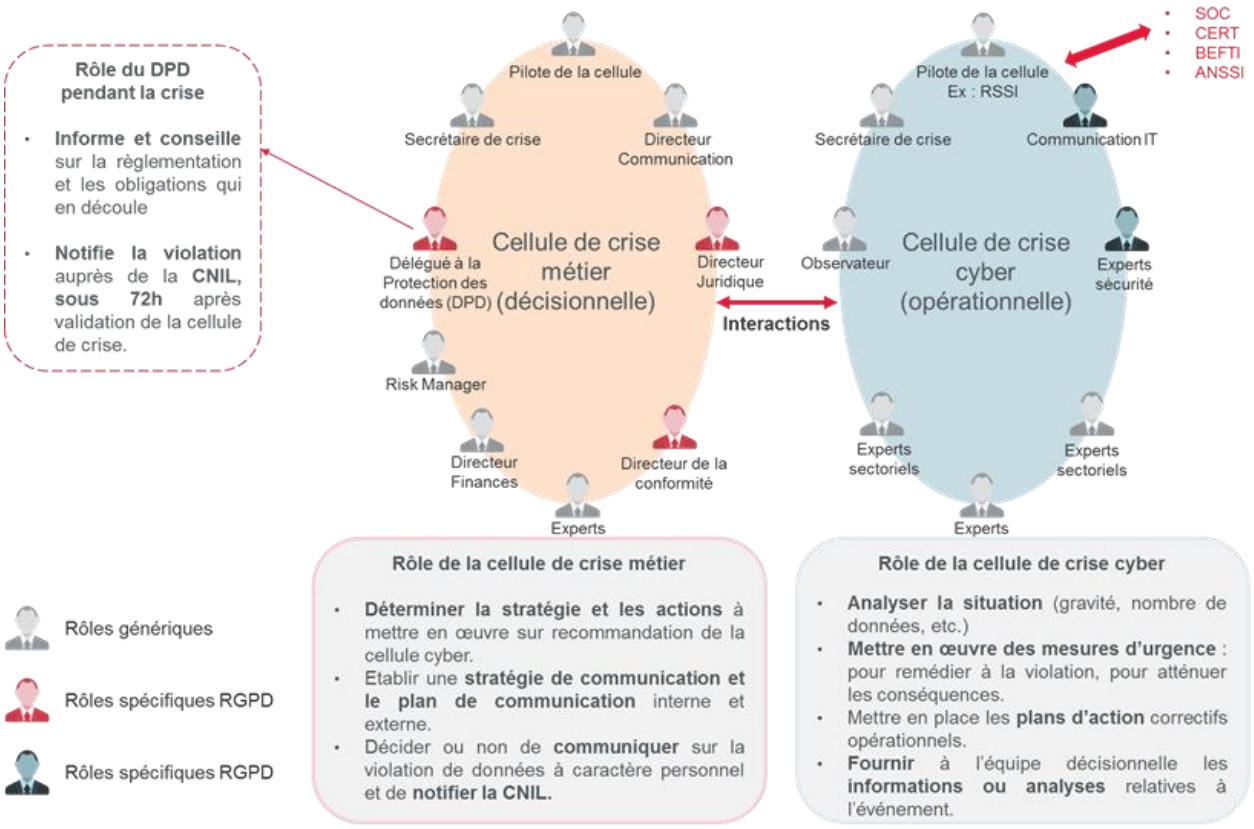


Figure 21 : Dispositif de crise en cas de violation de données à caractère personnel

De nouveaux acteurs sont mobilisés dans le cadre du RGPD : le Délégué à la Protection des Données (DPD), la Direction juridique, la Direction de la Conformité, la Direction des finances, la Direction de la communication IT, des experts cybersécurité…

De nouvelles procédures opérationnelles peuvent également être mises en œuvre afin de faciliter le respect des exigences de notification et de communication du RGPD :

- **Une grille d'auto-évaluation relative à la violation des données personnelles** permettant de qualifier la gravité et l'impact de l'évènement, et la nécessité ou non de notifier l'autorité de contrôle (CNIL) ;
- **Une procédure de notification auprès de l'autorité de contrôle** (CNIL) type fiche reflexe ;
- **Un plan de communication à destination des personnes concernées par la violation de données**, permettant d'identifier la nécessité de communiquer aux personnes concernées (contexte et délais, les éléments à porter à la connaissance des individus et la nature de la violation) ;
- **Un processus de communication et des modèles de réponse adaptés au niveau de gravité de la violation de données**, décrivant les rôles et responsabilités des parties prenantes, le type de communication à réaliser selon le niveau de gravité, les modèles à utiliser, etc.

Au même titre que les dispositifs de crise « métiers », les dispositifs de crise opérationnels « cyber » doivent être implémentés et testés dans le cadre d'une démarche d'amélioration continue, au minimum une fois par an.

Les violations de données à caractère personnel

L'article 33, paragraphe 5, du Règlement impose que chaque responsable de traitement doit documenter toutes les violations de données à caractère personnel qu'il détecte.

L'information documentée doit également contenir les effets de la violation et les mesures prises pour y remédier. Ce document doit être remis à l'autorité de contrôle pour valider le respect de l'article 33.

Attention cependant, l'autorité de contrôle pourrait ne pas se montrer très clémente si l'organisation « oublie » de mettre en place des moyens de détection des violations de données.

5.5 La notification 

Les conditions de notification dans le cadre d'une violation des données personnelles sont spécifiées à l'article 33 en ce qui concerne la notification à

l'autorité de contrôle, et à l'article 34 en ce qui concerne la communication aux personnes concernées.

Contenu de la notification

D'après l'article 33, une notification de violation de données personnelles aux tiers (autorité de contrôle et personne concernée) doit *a minima* :

- **Décrire la nature de la violation de données à caractère personnel** y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation, ainsi que les catégories, le nombre approximatif d'enregistrements de données à caractère personnel concernées *;*
- **Communiquer le nom et les coordonnées du délégué à la protection des données** ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- **Décrire les conséquences probables** de la violation de données à caractère personnel ;
- **Décrire les mesures prises,** ou que le Responsable du traitement propose de prendre, pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Condition de notification à l'autorité de contrôle [10]


CNIL.

NOTIFICATION DE VIOLATION DE DONNÉES À CARACTÈRE PERSONNEL

1 Identification du responsable de traitement

1.1 Identité du responsable de traitement

Raison sociale*

Service

N° SIRET*

Adresse*

Code postal* Ville*

Téléphone* Fax

La notification à l'autorité de contrôle compétente, donc la CNIL en France (se référer au chapitre 1.3 du présent document), est obligatoire en cas de violation des données personnelles. Elle doit être réalisée dans les meilleurs délais, et de préférence dans les 72 heures qui suivent la découverte de la fuite de DCP.

Cependant, il faut noter qu'il existe une exception à l'obligation de notification. Elle concerne le cas où « *la violation n'engendre pas un risque pour les droits et libertés des personnes physiques* » (Art. 33 du RGPD). Encore faut-il pour cela que le responsable de traitement puisse démontrer qu'il a, par exemple, pris des mesures ultérieures qui garantissent que le risque est désormais maîtrisé, ou bien que les données ne sont pas lisibles (ex. chiffrées).

Condition de communication aux personnes concernées

L'article 34 pose les conditions de notification aux personnes victimes de la violation des données.

10

https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

Si une violation est « susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique », le responsable de traitement est tenu de le notifier à la personne concernée dans les meilleurs délais.

L'interprétation de la notion de risque élevé relève de la responsabilité de l'organisation, donnant ainsi une marge de liberté à cette dernière. Elle devra toutefois démontrer à l'autorité de contrôle, si elle en fait la demande, le bien-fondé de son analyse et la cohérence des critères utilisés pour apprécier le risque. Il s'agit d'éviter qu'un risque soit volontairement sous-estimé par une organisation en vue d'échapper à l'obligation de notification par exemple.

La communication à la personne concernée n'est pas nécessaire, si l'une des trois conditions ci-dessous est remplie :

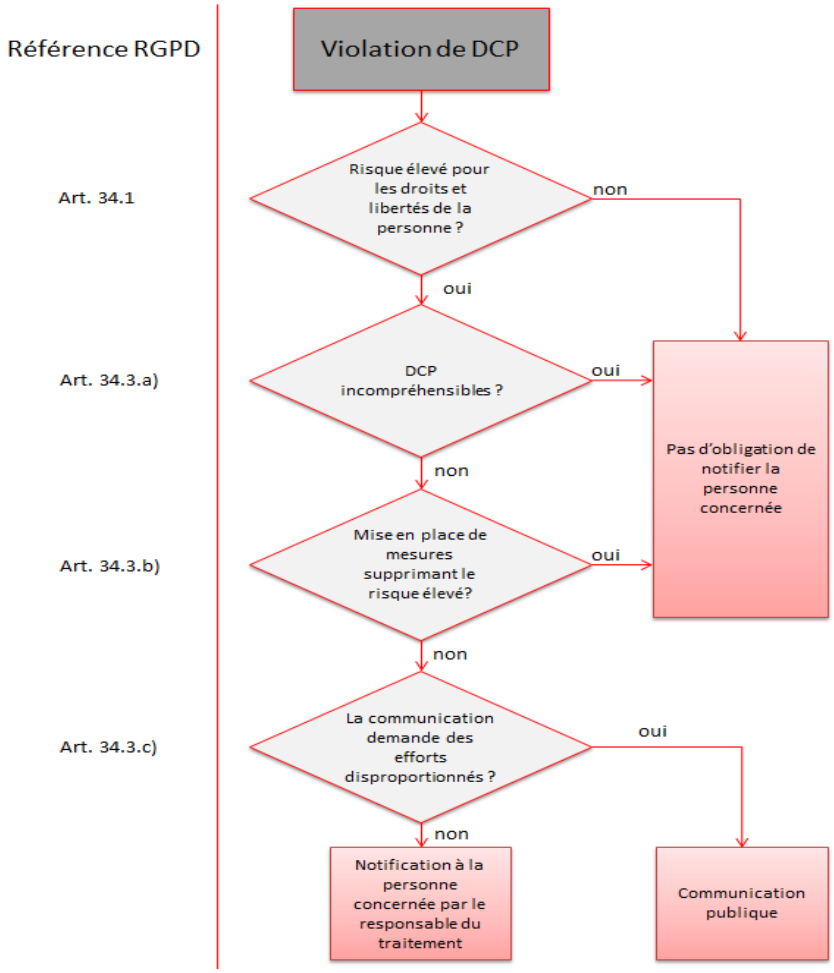


Figure 22 : Dérogation à la notification des violations de données personnelles aux personnes concernées

5.6 La communication

L'organisation doit s'interroger en amont sur les traitements qu'elle réalise et sur le risque engendré par une éventuelle violation des données personnelles associées.

Une stratégie de communication de crise adaptée doit être développée par l'organisation au sein de son dispositif de gestion de crise. L'objectif d'une telle démarche est de réduire l'impact de la crise sur la réputation et l'image de l'entreprise.

Le schéma suivant synthétise les actions à réaliser par l'entreprise :

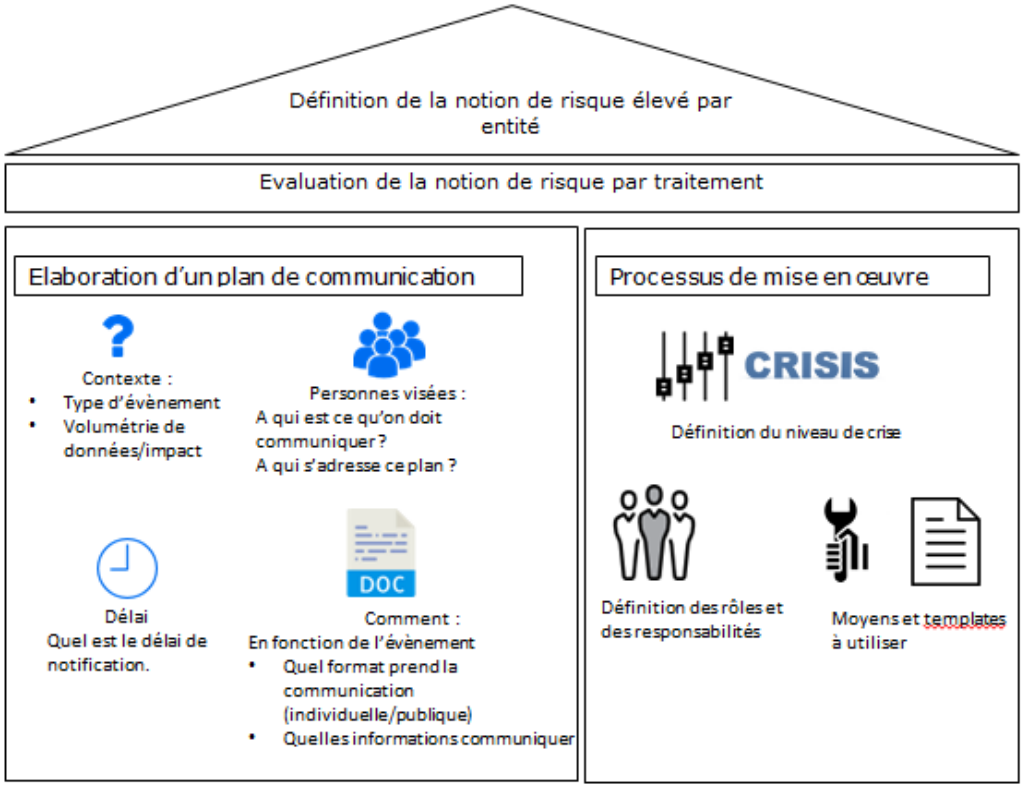


Figure 23 : Actions à mener afin de mettre en place une communication efficiente dans une entité (exemple donné), un service, une organisation.

5.7 Implémentation du droit des personnes sur leurs données

Les droits des personnes à mettre en œuvre pour être en conformité avec le RGPD sont détaillés au chapitre « 2. Un renforcement du droit des personnes sur leurs données personnelles » du présent Cahier Technique.

5.8 Gestion des sous-traitants

Une gestion spécifique des sous-traitants est nécessaire dès lors que ces derniers traitent des données personnelles pour le compte de l'organisation responsable du traitement, car ils détiennent également une responsabilité dans le traitement des DCP. Ainsi, les exigences décrites tout au long de ce document peuvent s'appliquer entièrement ou partiellement au sous-traitant. Le contrat mis en place avec le sous-traitant est le principal levier pour définir et suivre les engagements du sous-traitant relatifs au RGPD (cf. paragraphe 4.2 du présent document pour plus de détails sur le contrat sous-traitant).

Dans un premier temps, l'organisation devrait valider que ses sous-traitants aient bien pris le sujet en main en leur demandant un point sur l'avancée de leur projet par courrier. Pour les sous-traitants n'apportant pas de réponse satisfaisante, un contrôle plus approfondi pourra être mené (*crescendo*, non exhaustif : revue du contrat, audit des procédures, audit sur site).

5.9 Privacy by design

L'article 25 du RGPD définit les principes clés du « Privacy by design and by default » ou de la protection dès la conception du projet et par défaut :

- Limitation de la collecte uniquement aux données nécessaires ;
- Durée de conservation adaptée à la durée de traitement ;
- Stockage des données centralisé et accessible uniquement aux personnes qui en ont besoin ;
- Prise en compte de la protection de la vie privée dans la durée de vie complète des données.

Ces principes ont pour objectif de rendre la protection des droits et libertés des personnes concernées plus effective et viennent s'ajouter aux principes déjà présents dans la LIL avec les principes de finalité, de nécessité, de proportionnalité, et de transparence.

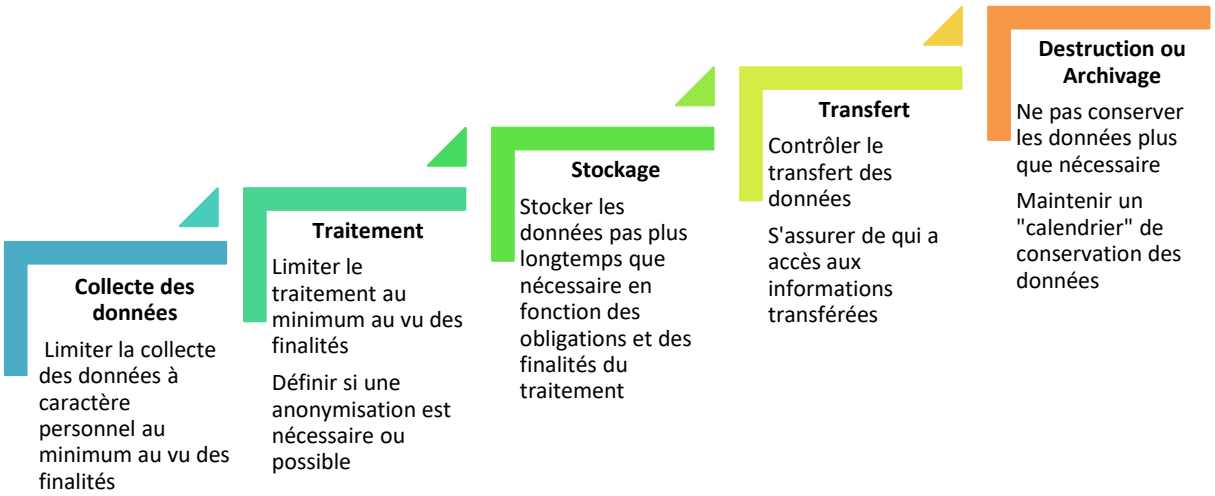


Figure 24 : Mise en œuvre d'une démarche de Privacy by design

Exemples de contrôles à étudier :

- La typologie des personnes concernées par le traitement est-elle établie ? La liste des parties prenantes est-elle établie ?
- La finalité du traitement est-elle clairement définie ? Les données collectées sont-elles uniquement celles nécessaires à cette finalité ?
- Comment les données nécessaires au traitement ont-elles été identifiées ?
- Les cas d'utilisation et les flux de données utilisés dans le cadre du traitement sont-ils définis ?
- Les sources et destinations de données sont-elles identifiées dans une cartographie ?
- La Protection de la vie privée est-elle identifiée comme un besoin critique dans les spécifications du projet ?
- Le cycle de vie des données, de leur collecte à leur suppression, est-il clairement défini ? Des mécanismes de purge, d'anonymisation ou d'archivage sont-ils définis pour encadrer la fin de vie des données ?
- Les données à caractère personnel générées par le traitement (ne provenant pas de la collecte initiale) sont-elles identifiées et encadrées ?

Planifier un projet en prenant en compte la protection dès la conception

La protection dès la phase de conception du projet s'appuie sur trois piliers : des **ressources humaines**, c'est-à-dire des personnes maîtrisant le sujet, en nombre suffisant et ayant des rôles et des responsabilités claires ; des **processus** prenant en compte les exigences du RGPD comme la responsabilité, l'analyse d'impact de la protection des données ; et enfin des **moyens technologiques** comme des registres de traitement, des bases de cartographies des risques.

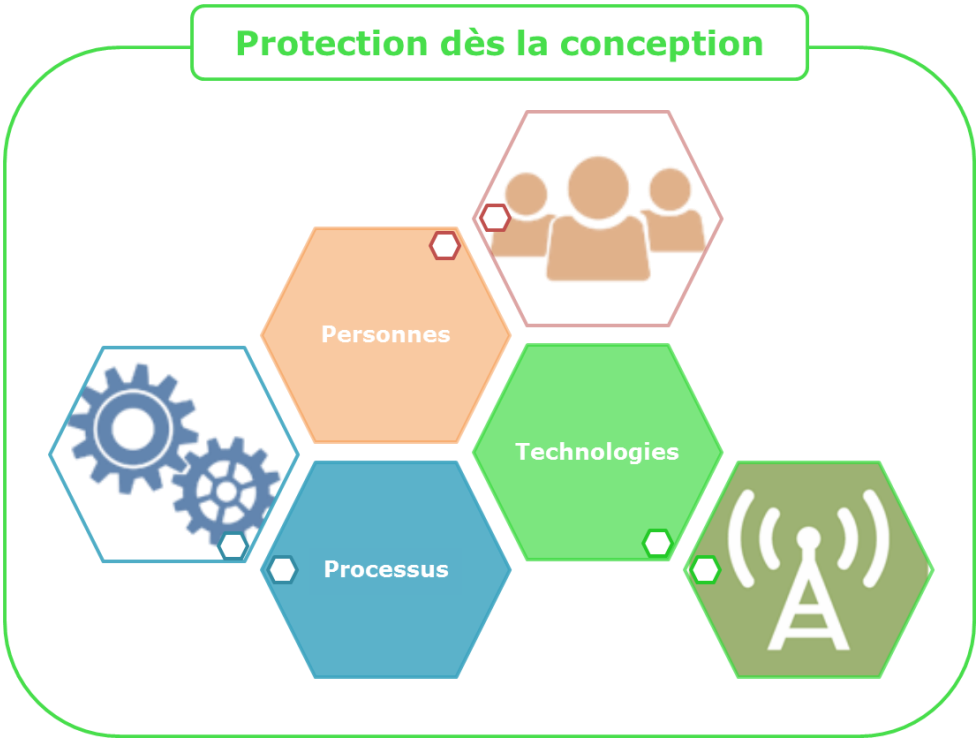


Figure 25 : Mise en œuvre d'une démarche de protection dès la conception

Cette première phase de planification se base sur une **évaluation de l'existant** sur ces trois axes : personnes, processus et technologies, afin d'évaluer les écarts aux exigences. Cette évaluation doit faire ressortir ce qui doit être complété, modifié ou créé.

Acteurs à impliquer :

- Représentant du responsable du traitement ;
- Délégué à la protection des données (DPD) ;
- Directions métiers ;
- Direction juridique / conformité ;
- Direction des systèmes d'information ;
- Direction des risques.

Livrables :

- Analyse d'écarts ;
- Liste de chantiers ;
- Priorisation des chantiers via une approche pragmatique basée sur les risques.

Avec un cadre de protection de la vie privée défini et organisé dès la conception du projet, l'organisation s'assure que toute nouvelle solution **respecte les principes du RGPD** dès sa mise en œuvre.

Déployer une solution pilote prenant en compte la protection dès la conception

Déployer une solution pilote permet de tester la robustesse des choix faits mais également de fournir des preuves pour démontrer sa conformité.

La méthodologie de test doit définir des scenarii de test en portant attention aux indicateurs de suivi et aux critères de réussite. Fixer et obtenir un consensus a priori sur ces deux paramètres est primordial pour permettre de mesurer l'atteinte des deux objectifs (test de la robustesse des choix et constitution de preuves) et de piloter l'implémentation d'un cadre respectant le principe de protection dès la conception.

Trois scenarii peuvent être envisagés pour tester la robustesse du système :

- Un scénario avec impact faible ou nécessitant peu de ressources pour vérifier la bonne prise en compte des exigences par toutes les parties, il peut aussi s'agir d'un premier scenario pour entrainer les acteurs ;
- Un scénario avec impact moyen ou mobilisation moyenne de ressources qui « mimera » un projet classique ;
- Un scénario avec impact fort ou la mobilisation de beaucoup d'acteurs, pour éprouver l'organisation mise en place.

La revue des résultats au travers de retours d'expérience permettra à l'organisation de s'améliorer et de conforter sa conformité.

Après avoir éprouvé le système mis en place, l'organisation doit pérenniser dans chaque solution, la notion de protection dès la conception.

5.10 L'Analyse d'Impact relative à la Protection des Données (AIPD)

L'Analyse d'Impact relative à la Protection des Données (AIPD) s'inscrit dans la démarche de responsabilisation des responsables de traitement ou des sous-traitants manipulant des données à caractère personnel. L'objectif du législateur dans l'article 35 du RGPD est de limiter l'obligation de formalités préalables (à l'autorité de contrôle) aux seuls traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Les autres traitements sont inscrits au registre des traitements sans déclaration préalable. Ils peuvent néanmoins être analysés lors des contrôles effectués par l'autorité compétente.

Faut-il réaliser une AIPD pour tous les traitements de données à caractère personnel ?

L'article 35 en son paragraphe 1 précise les cas pour lesquels il est nécessaire de réaliser une analyse d'impact : « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires ».

De plus, la réalisation d'une AIPD est obligatoire dans trois cas prévus par le Règlement en son article 35, paragraphe 3 :

- L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
- Le traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1, ou de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ; ou
- La surveillance systématique à grande échelle d'une zone accessible au public.

Une étude préalable formalisée est donc nécessaire pour déterminer si une AIPD doit être réalisée.

Afin d'apporter une cohérence dans l'application de ces paragraphes, le G29 (cf. Glossaire) a publié des lignes directrices apportant un éclairage sur les modalités à prendre en compte pour déterminer si une AIDP est nécessaire. La révision de la Loi Informatique et Libertés devrait également proposer ses propres modalités.

Enfin, la CNIL a annoncé que pour les traitements déjà en conformité avant le 25 mai 2018, l'AIPD pouvait être menée dans les trois ans suivants l'entrée en application du RPGD, soit d'ici au 25 mai 2021.

Annexe 2 — Critères d'acceptabilité d'une AIPD [11]

Les critères suivants proposés par le G29 peuvent être utilisés par les responsables du traitement pour déterminer si une AIPD, ou une méthodologie d'AIPD, considérée est suffisamment complète aux fins du respect des exigences du RGPD :

☐ une description systématique du traitement est fournie [Article 35, paragraphe 7, point a)] :
- ☐ la nature, la portée, le contexte et les finalités du traitement sont pris en compte (considérant 90) ;
- ☐ les données à caractère personnel concernées, les destinataires et la durée pendant laquelle les données à caractère personnel seront conservées sont précisés ;
- ☐ une description fonctionnelle de l'opération de traitement est fournie ;
- ☐ les actifs sur lesquels reposent les données à caractère personnel (matériels, logiciels, réseaux, personnes, documents papier ou canaux de transmission papier) sont identifiés ;
- ☐ le respect de codes de conduite approuvés est pris en compte (Article 35, paragraphe 8). ;

☐ la nécessité et la proportionnalité sont évaluées [Article 35, paragraphe 7, point b)] :
- ☐ les mesures envisagées pour assurer la conformité au règlement sont déterminées [Article 35, paragraphe 7, point d), et considérant 90], avec prise en compte :
  - ☐ de mesures contribuant au respect des principes de proportionnalité et de nécessité du traitement, fondées sur les exigences suivantes :
  - ☐ finalités déterminées, explicites et légitimes (Article 5, paragraphe 1, point b)] ;
  - ☐ licéité du traitement (Article 6) ;
  - ☐ données adéquates, pertinentes et limitées à ce qui est nécessaire [Article 5, paragraphe 1, point c)] ;
  - ☐ durée de conservation limitée [Article 5, paragraphe 1, point e)] ;
- ☐ de mesures contribuant aux droits des personnes concernées :
  - ☐ informations fournies à la personne concernée (Articles 12, 13 et 14) ;
  - ☐ droit d'accès et droit à la portabilité des données (Articles 15 et 20) ;
  - ☐ droit de rectification et droit à l'effacement (Articles 16, 17 et 19) ;
  - ☐ droit d'opposition et droit à la limitation du traitement (Articles 18, 19 et 21) ;
  - ☐ relations avec les sous-traitants (Article 28) ;
  - ☐ garanties entourant le ou les transferts internationaux (chapitre V) ;
  - ☐ consultation préalable (Article 36);

☐ les risques pour les droits et libertés des personnes concernées sont gérés [Article 35, paragraphe 7, point c)] :
- ☐ l'origine, la nature, la particularité et la gravité des risques sont évalués (considérant 84) ou, plus spécifiquement, pour chaque risque (accès illégitime aux données, modification non désirée des données, disparition des données) du point de vue des personnes concernées:
  - ☐ les sources de risques sont prises en compte (considérant 90) ;
  - ☐ les impacts potentiels sur les droits et libertés des personnes concernées sont identifiés en cas d'événements tels qu'un accès illégitime aux données, une modification non désirée de celles-ci ou leur disparition ;
  - ☐ les menaces qui pourraient conduire à un accès illégitime aux données, à une modification non désirée de celles-ci ou à leur disparition sont identifiées ;
  - ☐ la probabilité et la gravité sont évaluées (considérant 90) ;
- ☐ les mesures envisagées pour faire face à ces risques sont déterminées [Article 35, paragraphe 7, point d), et considérant 90] ;

☐ les parties intéressées sont impliquées :
- ☐ l'avis du DPD est recueilli (Article 35, paragraphe 2) ;
- ☐ le point de vue des personnes concernées ou de leurs représentants est recueilli, le cas

[11] Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est «susceptible d'engendrer un risque élevé» aux fins du règlement (UE) 2016/679, adoptées le 4 octobre 2017
https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

échéant (Article 35, paragraphe 9).

Comment réaliser une AIPD ?

La réalisation d'une AIPD peut s'appuyer sur des méthodologies existantes, comme par exemple :

- 4 guides de la CNIL sur la méthode, l'outillage et les bonnes pratiques :
  - AIPD : application aux objets connectés [12]
  - AIPD : la méthode[13]
  - AIPD : les modèles[14]
  - AIPD : les bases de connaissances[15]
- Les lignes directrices sur l'analyse d'impact relative à la protection des données (AIPD) et la détermination du caractère « susceptible d'entraîner un risque élevé » [16] - WP248 – 4 avril 2017 ;
- EBIOS[17], Expression des besoins et identification des objectifs de sécurité ;
- Méthodologies issues des critères établis dans l'ISO 31000, Management du risque – Principes et lignes directrices ;
- Méthodologies issues des critères établis dans l'ISO/IEC 27005, gestion des risques liés à la sécurité de l'information ;
- Méthodologies issues de l'ISO/IEC 29134, Lignes directrices pour mener des études d'impact sur la vie privée.

L'article 35 du RGPD mentionne en son paragraphe 7 que l'analyse doit au moins comporter :

- « Une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ;
- Une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- Une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ; et
- Les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent

[12] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-fr.pdf
[13] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf
[14] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf
[15] https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf
[16] https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf
[17] https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées. »

Afin de répondre à cette exigence, il est possible d'adopter pour l'AIPD une structure en quatre parties :

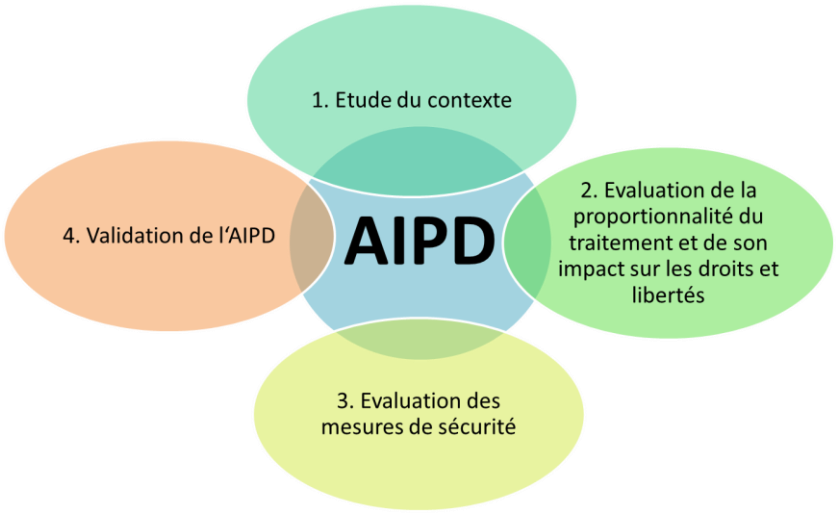


Figure 26 : Exemple de plan d'Analyse d'Impact relative à la Protection des Données

La partie 1 de cet exemple de plan d'AIPD répond à la demande du point a), la partie 2 répond au point b) et en partie au point c), et la partie 3 répond en partie au point c) et au point d). La partie 4 quant à elle concerne la validation, par le responsable du traitement, des impacts évalués et des mesures retenues.

La partie 2 de l'AIPD n'est plus qu'une analyse de risques traditionnelle dédiée aux DCP, dès lors que la licéité du traitement et le respect des droits des personnes concernées ont été validés d'un point de vue juridique (partie 1).

L'étude du contexte d'une AIPD (partie 1 de l'AIPD)

L'étude du contexte doit répondre à l'exigence suivante : « une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement ».

L'étude doit faire ressortir la finalité du traitement, ses enjeux et le cycle de vie de la donnée. Il s'agit de délimiter le périmètre du traitement et de décrire les opérations de traitements, en expliquant quelles sont les données concernées. L'étude de contexte doit *a minima* répondre aux questions suivantes :

- Pourquoi des données sont-elles collectées ?
- Quelles données à caractère personnel sont collectées ?

- Comment sont-elles collectées, traitées, stockées ?
- Sous quel format sont-elles collectées ?
- Qui reçoit les données ?
- Qui peut y accéder ?
- Quelle est leur durée de conservation ?

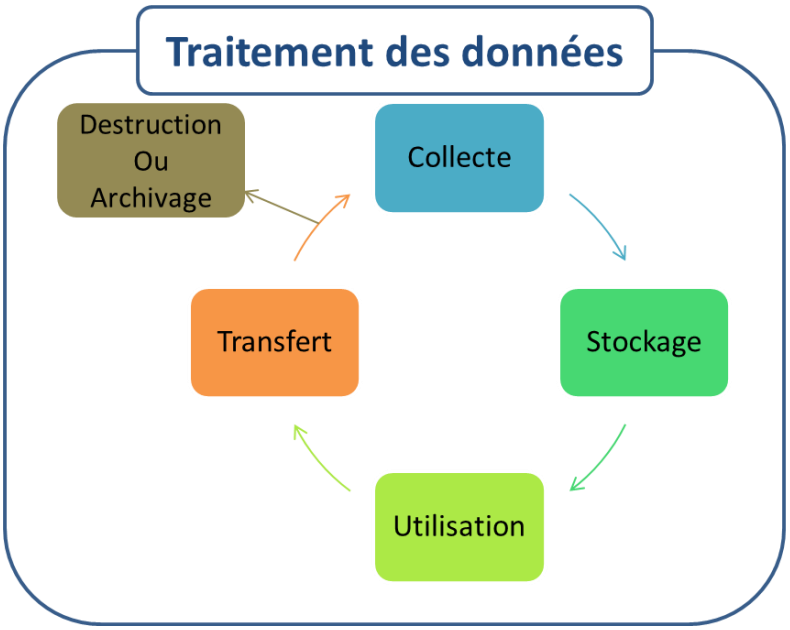


Figure 27 : Processus de traitement des données

L'évaluation de la proportionnalité du traitement et de son impact sur les droits et libertés (Partie 1 de l'AIPD)

Cette thématique est, dans le texte du Règlement, découpée en deux parties découlant des exigences suivantes : « une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités; une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ».

La nécessité et la proportionnalité du traitement sont donc des exigences du RGPD. Il faut, pour l'organisation, être en mesure de démontrer que les principes fondamentaux non négociables sont respectés, éventuellement justifier pourquoi ils ne le sont pas et le cas échéant décrire les mesures correctives mises en œuvre.

Analyse des risques des DCP (Partie 2 de l'AIPD)

La deuxième partie est une analyse de risques sur la vie privée. La présentation du risque selon une matrice, traditionnelle, à deux axes Gravité / Probabilité est encouragée par le RGPD. L'article 32 relatif à la sécurité des traitements exige de traiter plusieurs axes et pas seulement la fuite d'information d'origine malveillante : « Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques […] de la **destruction**, de la **perte**, de **l'altération**, de la

divulgation non autorisée […] ou de **l'accès** non autorisé à de telles données, de manière **accidentelle** ou **illicite** ». L'analyse peut donc être faite en terme de confidentialité, intégrité et disponibilité (au sens de l'ISO/IEC 27000) de la donnée.

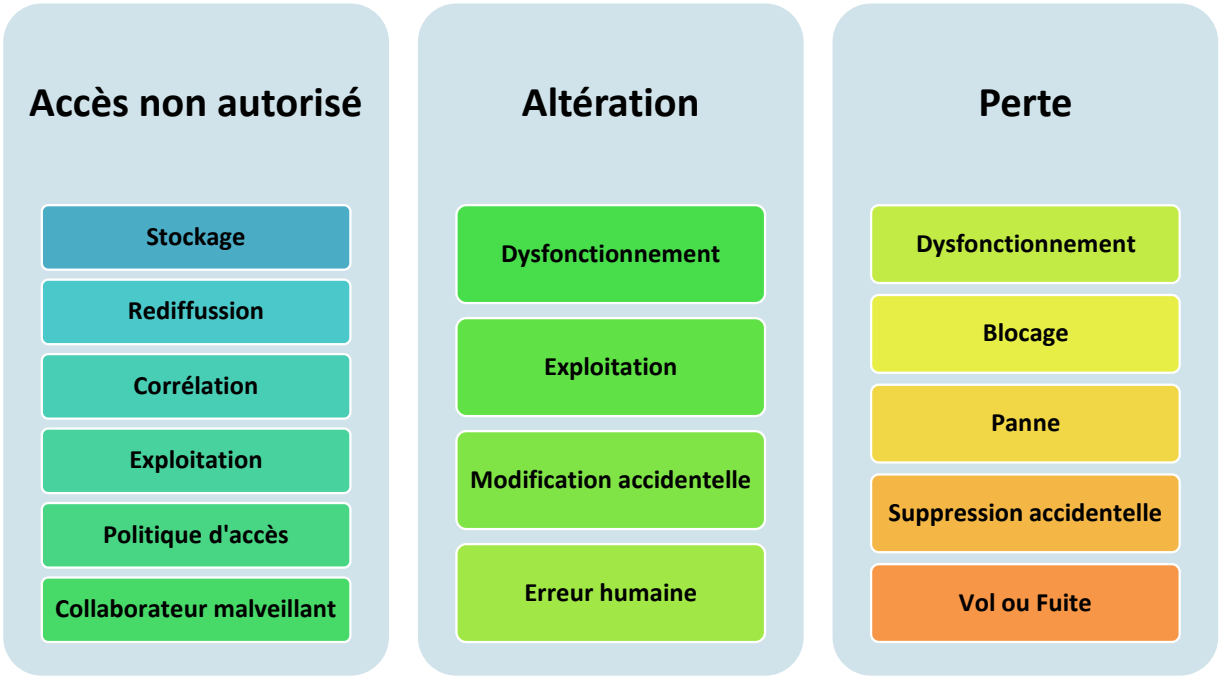


Figure 28 : Exemples de risques de sécurité des systèmes d'information/des données

L'évaluation des mesures de sécurité (Partie 3 de l'AIPD)

A chaque mesure de sécurité prise, le responsable de la sécurité SI (RSSI) doit statuer sur le caractère acceptable de la mesure face aux risques présentés par le traitement.

Puis il doit évaluer le niveau de risque résiduel suite à l'application des mesures.

Extrait issu d'une analyse de risques DCP (le contenu des champs est expliqué ci-après) :

Sources de risques	Evènements redoutés	Menaces	Gravité initiale	Probabilité initiale	Risque initial	Mesures	Gravité résiduelle	Vraisemblance résiduelle	Niveau de risque
1.	2.	3.	Note	Note	4.	5.	Note	Note	6.

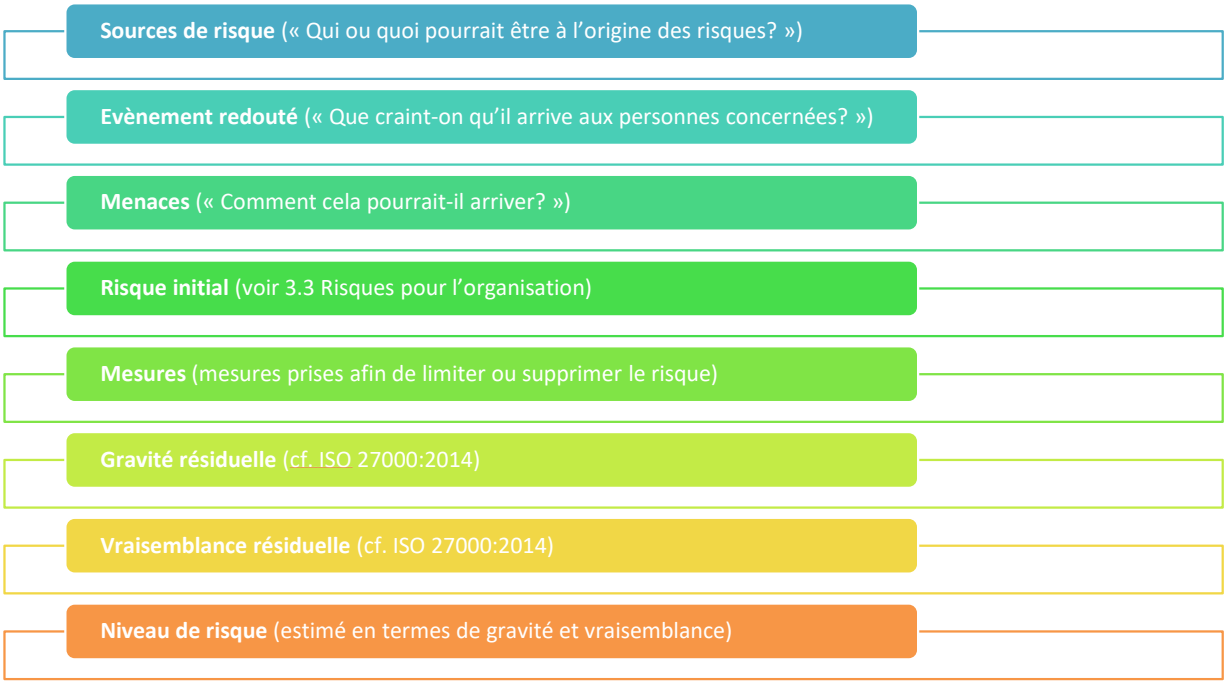


Figure 29 : Processus d'analyse de risques et d'évaluation des mesures de sécurité

La validation de l'AIPD

La validation de l'AIPD est la décision argumentée vers trois issues possibles :

- Acceptation des mesures et des risques ;
- La non-acceptation, c'est-à-dire soit l'abandon du projet, soit une itération sur le plan de mesures des risques pour abaisser le niveau de gravité à un niveau acceptable ;
- La consultation de l'autorité de contrôle.

Cette validation de l'AIPD est un élément central de la mise en œuvre de la démonstration du principe de responsabilité. Elle porte sur la validation du plan de traitement des risques et l'acceptation des risques résiduels.

L'AIPD doit-elle être communiquée à l'autorité de contrôle ?

L'article 36 du RGPD impose que « le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact […] indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque. […] Lorsque l'autorité de contrôle est d'avis que le traitement envisagé […] constituerait une violation du présent règlement, en particulier lorsque le responsable du traitement n'a pas **suffisamment identifié ou atténué le risque**, l'autorité de contrôle fournit par écrit, dans un délai maximum de **huit semaines** […] un avis écrit au responsable du traitement. Ce délai peut être prolongé de **six semaines**, en fonction de la

complexité du traitement envisagé. […] Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation. »

Le G29 ajoute dans ses bonnes pratiques que l'autorité de contrôle devra être consultée de façon systématique […] pour les traitements en rapport avec la protection sociale et la santé publique.[18]

5.11 Sécurité des traitements et sensibilisation des acteurs 

La sécurité des traitements est décrite dans les considérants 39 et 83, ainsi qu'à l'article 32.

Dans l'article 32, il est mentionné que le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées. Au paragraphe 1 de cet Article, quatre points sont mis en avant :

- La pseudonymisation et le chiffrement des données à caractère personnel ;
- Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- Des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Ces **mesures techniques et organisationnelles** visent à assurer la disponibilité, l'intégrité la confidentialité et la traçabilité des données manipulées dans le traitement. Il s'agit d'identifier les mesures mises en œuvre ou à mettre en œuvre :

- Quelles sont les mesures de chiffrement mises en place pour assurer la sécurité du stockage et des transmissions de données ?
- Quelles sont les mesures mises en place pour limiter l'accès aux données aux seules personnes autorisées ? Les procédures de distribution, revue et révocation des accès sont-elles définies ?
- Le développement de l'application se fait-il dans des environnements séparés ?
- Les communications entre les différentes briques du système d'information sont-elles sécurisées ?
- Des systèmes de détection sont-ils mis en place pour remonter tout incident dans l'application ?
- Les aspects relatifs à la continuité d'activité et aux sauvegardes sont-ils pris en compte pour assurer la disponibilité des données ?

[18] https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

- Les prestataires amenés à travailler sur le projet sont-ils encadrés ?
- Les rôles et responsabilités d'administration de l'application sont-ils définis et une séparation des tâches est-elle mise en place ?

Il est possible de s'appuyer sur les référentiels ISO/IEC 2700x, OWASP Top 10 ou NIST 800-53.

La stratégie de sécurisation doit découler d'une approche « de bout en bout »

Les mesures de sécurité doivent se concentrer sur les données et les risques associés à leur cycle de vie.

Budget de la sécurisation et aversion au risque

Les organisations doivent avoir conscience de l'impact financier d'une violation de données. Cette évaluation permet également de motiver le financement et l'exécution de chantiers de sécurité et de mise en conformité au RGPD, et ce pour au moins deux raisons :

- Une violation de données personnelles a, avant tout, un impact direct sur l'organisation ;
    - En 2017, le coût moyen d'une fuite de données était estimé à 3.62 millions de dollars[19],
    - Le coût moyen d'une perte ou divulgation de données sensibles est estimé à 141 dollars par entrée.

- Le RGPD prévoit une gamme complète de sanctions financières, voire pénales, en cas de non-conformité et de violation de données à caractère personnel. Les sanctions financières peuvent notamment atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial consolidé pour l'organisation concernée par le manquement (le montant le plus élevé étant retenu).

[19] Source : Rapport IBM (2017 Ponemon Cost of Data Breach Study)

Exemple d'une stratégie de sécurisation réussie en 10 points

1. La sécurité du système d'information, et notamment des données à caractère personnel, ainsi que les acteurs impliqués dans ces processus doivent être budgétés et une volonté en ce sens doit être affichée au plus haut niveau de l'organisation ;
2. La sécurité du système d'information doit faire l'objet d'un ensemble de processus (dont la conformité au RGPD) clairement décrits et faisant l'objet d'un contrôle interne et d'une amélioration continue ;
3. Les mesures de sécurité doivent viser à traiter les risques impactant potentiellement les personnes et non les risques impactant potentiellement l'organisation ;
4. Le principe de « *Privacy By Design* » doit être décliné en pratique :
    - Au niveau du SI, par des mesures telles que :
        - La surveillance par un Security Operations Center (SOC).
    - Au niveau des projets, par des mesures telles que :
        - La sensibilisation des acteurs des projets (métiers, chefs de projet, développeurs, opérationnels) ;
        - L'intégration efficace et efficiente de la sécurité dans les projets ;
        - L'audit récurrent de code source durant les développements.

Au niveau de l'organisation dans son ensemble :

- L'implémentation d'un Système de management de la Sécurité des SI (ISO27001) ;
- L'intégration de clauses de sécurité dans les contrats fournisseurs/éditeurs.

5. Appliquer concrètement le principe de « Security By default » :
    - Au niveau du SI, par des mesures telles que :
        - Le cloisonnement des accès (réseaux, logiques, tiers prestataires de TMA, etc.) ;
        - La restriction des flux réseaux ;
        - Le scan de vulnérabilités sur les composants du SI, notamment ceux exposés sur Internet.
    - Au niveau des projets, par des mesures telles que :
        - L'application du principe du « stricte nécessaire » en matière de services ouverts ;
        - L'application du principe de « moindres privilèges » ;
        - L'application du principe de « défense en profondeur ».
    - Au niveau de l'organisation dans son ensemble :
        - La définition et l'attribution claire des rôles dans l'organisation (RSSI, DPO, etc.) ;
        - L'intégration de clauses par défaut de sécurité dans les contrats fournisseurs/éditeurs ;
    - Au niveau physique, par des mesures telles que :

- La sécurisation des data centers ;
- La résilience aux pannes et catastrophes naturelles ;
- La sécurisation des accès physiques des personnes aux locaux de l'organisation.

6. Mettre en œuvre des mesures techniques de sécurité « au plus près des données ». De telles mesures impliquent notamment :
   - de chiffrer les données à caractère personnel dans les composants de stockage lorsque c'est nécessaire (en particulier pertinent en cas de stockage sur des supports amovibles, dans un nuage, etc.). Attention, la mise en place d'un chiffrement implique de sécuriser ce mécanisme (cryptographie robuste, gestion des secrets, etc.) et n'est pas toujours applicable (données en cours de traitement dans un processeur quelconque, notamment dans le cloud) ;
   - d'anonymiser les données afin d'en retirer l'aspect sensible du point de vue du RGPD. Attention, une anonymisation parfaite est en soi parfois extrêmement difficile à mettre en œuvre. En cas de possibilité de ré-identification, même indirecte, des données, on parle plutôt de « pseudonymisation ».
7. Les politiques, procédures et pratiques de sécurité doivent être formalisées, documentées, et cette documentation doit être mise à jour régulièrement ;
8. Un processus de sensibilisation des collaborateurs doit être en place. Ce processus doit, en adaptant l'approche, présenter a minima les menaces et cyber attaques, l'hygiène informatique en entreprise et dans la vie privée (notamment en déplacement), les menaces d'ingénierie sociale et une information sur les politiques et pratiques internes de sécurité dans l'organisation ;
9. Un processus d'audit récurrent efficace doit être en place. Ce processus implique la plupart du temps le recourt à des prestataires d'audit spécialisés et de confiance tels que les PASSI qualifiés par l'ANSSI ;
10. Ne surtout pas négliger d'appliquer tous les principes ci-dessus à tous les outils et composants du SI impliqués de près ou de loin dans les opérations du processus de conformité RGPD (sécuriser notamment le registre des traitements, les enregistrements de consentement, etc.). Les traitements liés au RGPD sont le plus souvent des traitements de données à caractère personnel : le RGPD s'applique à l'implémentation de la conformité RGPD.

Anonymisation efficace des données

L'anonymisation efficace des données est un véritable défi du fait de la difficulté d'atteindre un niveau d'assurance[20], voire de preuve formelle, qu'aucune technique[21] de ré-identification ne permet de dégrader cet effet d'anonymisation

[20] Le secret statistique est un sujet difficile : https://www.insee.fr/fr/information/1300624

[21] Inférence statistique, big data, intelligence artificielle, etc.

(on parle alors de pseudonymisation seulement, ce qui est insuffisant pour s'affranchir des exigences du RGPD).

La CNIL propose une fiche sur l'anonymisation dans son guide « La sécurité des données personnelles » et définit qu' « une véritable anonymisation implique nécessairement une perte (irréversible) d'information. Dans certains cas, le simple fait d'effacer ou de noircir une partie des données peut suffire à atteindre l'objectif souhaité. »

Méthodes classiques d'anonymisation

Appauvrissement :

L' « appauvrissement » est un procédé qui consiste à faire perdre du sens à une donnée (telle qu'une date de naissance ou un solde de compte) en remplaçant la valeur par une fourchette. Ce procédé est irréversible.

Exemple : Jean est né le 12 avril 1945 → Jean est né dans les années 40

Masquage :

Le « masquage » est un procédé qui consiste à rendre illisible certaines informations lors de leurs lectures par des utilisateurs de manière à les rendre inutilisables, tout en conservant ces informations intactes. Ce procédé est utilisé par les sites de paiement en ligne qui conservent le numéro de la carte bancaire (PAN) mais n'affichent que les 4 premiers ou 4 derniers numéros à l'utilisateur.

Exemple : M. Jean DUPONT → M. Jean ######

Suppression :

La « suppression » est un procédé qui consiste à supprimer totalement une information, par exemple une colonne au sein d'une base ou remplacement de la donnée par un jeu de caractères. Ce procédé est irréversible.

Exemple : M. Jean DUPONT → M. Jean <NULL>

M. Jean DUPONT → M. Jean ####

Vieillissement ou décalage :

Le « vieillissement » ou « décalage » est un procédé qui consiste à modifier l'âge d'une personne ou une date. Attention, cette méthode peut parfois donner des résultats illogiques suivant le calcul employé (ex. personne n'atteignant pas la majorité suite au traitement). Ce procédé est irréversible.

Exemple : M. Jean DUPONT né le 04/06/1942 → M. Jean DUPONT né le **07/04/1999**

Mélange de données :

Le « mélange de données » est un procédé qui consiste à mélanger les différentes données entre elles ou, dans le cas d'une base, à mélanger les entrées d'une ou plusieurs colonnes entre elles. Ce procédé permet de conserver la distribution des données mais est irréversible.

Exemple : M. Jean DUPONT 04/07/1945 → M. Jean CARNOT 08/03/1950

M. Pierre MARTIN 08/03/1950 → M. Pierre DUPONT 18/02/1967

M. Paul CARNOT 18/02/1967 → M. Paul MARTIN 04/07/1945

Calcul d'empreinte (Hash) :

Le « hash » est un procédé qui consiste à appliquer un algorithme modifiant la donnée, on dit alors qu'il calcule une empreinte. En effet, la fonction de hachage remplace une donnée par une autre donnée unique (la fonction est déterministe), mais ne conserve pas le format. Ce procédé est irréversible.

Exemple : M. Jean DUPONT → M. Dcffdghew **WZRNFYKIC**

M. Jean MARTIN → M. Dcffdghew **EROFKNTSP**

Variance :

La « variance » est un procédé qui consiste à appliquer une variation dans une fourchette prédéfinie à une donnée de type numérique. Ce procédé est irréversible.

Exemple : variation du solde de -20 à 15%

2300 € → 2330 € (+10%)

4500 € → 4410 € (-20%)

Concaténation :

La « concaténation » est un procédé qui consiste à associer plusieurs données sources pour produire la nouvelle donnée. Il s'agit de concaténer plusieurs données entre elles ou bien faire une moyenne des 3 montants précédents par exemple. Ce procédé est irréversible.

Exemple : M. Jean DUPONT 3400€ → M. **Jeanpierrepaul** DUPONT 3400€

M. Pierre MARTIN 5670€ → M. Pierre **DUPONTMARTIN** 5670€

M. Paul CARNOT 3945€ → M. Paul CARNOT **4338€** (moyenne de 3 soldes)

Offuscation :

L' « offuscation » est un procédé qui consiste à ajouter de nouvelles entrées fictives. Les données réelles existent toujours mais elles sont mélangées à de fausses données. Ce procédé est irréversible.

Exemple : génération de requêtes multiples via le moteur de recherche Google afin que les vraies requêtes soient dissimulées dans la masse (bien que celles-ci soient tout de même enregistrées), et qu'elles ne renseignent en rien sur les centres d'intérêt réels de l'utilisateur.

Autres méthodes d'anonymisation

Chiffrement :

Le « chiffrement » est un procédé qui consiste à rendre illisible une donnée par un procédé cryptographique pour toute personne ne possédant pas la clé de déchiffrement. Ce procédé est réversible (voir fiche BP-04 chiffrement des données stockées pour plus de détail).

Exemple : M. Jean DUPONT → M. XBJF WZRNFY

Pseudonymisation :

La CNIL définit la « pseudonymisation » comme « le remplacement d'un nom par un pseudonyme. C'est le processus par lequel les données perdent leur caractère identifiant (de manière directe). Les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l'identité ne soit révélée. Elle peut être opérée avec ou sans la possibilité de retour vers les noms ou identités (pseudonymisation réversible ou irréversible). »

Exemple : M. Jean DUPONT → M. Matthieu MARTIN

Tokenisation :

La « tokenisation » est un processus qui consiste à substituer une donnée sensible telle qu'une donnée à caractère personnel par une donnée non-sensible désignée comme un token (jeton) unique qui n'a pas de définition exploitable. Le token est un identifiant permettant de retrouver le propriétaire de cette donnée anonymisée. La pseudonymisation réversible est une forme de tokenisation.

Exemple : M. Jean DUPONT 14/05/1949 3400€ → M.**967038** 14/05/1949 3400€

Cas d'usage :

Une application ne doit pas stocker, conserver ou manipuler des données sensibles (ex. données à caractère personnel) dès lors que le traitement qu'elle opère n'en a

pas un besoin légitime. Ainsi, avant toute anonymisation de données il est recommandé de filtrer les informations collectées pour ne conserver que celles qui sont réellement nécessaires.

Dans le cas d'une anonymisation de données à caractère personnel, il est recommandé d'utiliser la Pseudonymisation, qui peut être réalisée de manière irréversible, uniquement s'il n'y a aucun besoin de retrouver l'identité de la personne suite au traitement.

Dans le cas d'une anonymisation de données non nominatives conservées en base, telles que des données bancaires par exemple, pouvant nécessiter une réversibilité pour retrouver l'information source, il est recommandé d'utiliser la Tokenisation.

Dans les autres cas, les méthodes classiques d'anonymisation peuvent être utilisées. Par exemple, les environnements hors production (développement, intégration, pré-production) ne doivent pas contenir de données sensibles de production. Ils nécessitent néanmoins des jeux de données représentatifs afin de réaliser les tests propres à chaque application. Ces jeux de données peuvent être créés en anonymisant de manière irréversible les données de production.

Moyens Cryptographiques	Chiffrement des communications TLS pour le transfert de données (ATTENDU) Chiffrement des données lors du transfert (BONNE PRATIQUE) Anonymisation (irréversible) des données pour les environnements de non production (ATTENDU) Pseudonymisation des données pour la génération de statistique (ATTENDU)
Gestion des accès	Authentication forte des utilisateurs et exploitants internes (ATTENDU) Gestion formalisée des autorisations d'accès aux données (ATTENDU) Authentication forte des exploitants de la base de données (ATTENDU)

Figure 30 : Exemple de mesures préconisées pour un projet

5.12 Sensibilisation et accompagnement au changement

Un changement de paradigme dans le monde du numérique a eu lieu avec l'arrivée du RGPD le 25 mai 2018. En effet, de nombreuses entreprises organisent leur plan d'affaires autour de la consommation massive de données personnelles. Désormais, la législation européenne prône à la fois la sécurisation de ces données, mais aussi **leur minimisation** (ce point était déjà prévu par la LIL, mais les sanctions n'étaient alors pas assez dissuasives au regard des promesses du Big Data). Ce changement radical va apporter avec lui une période de confusion sur les nouvelles pratiques à adopter.

Ainsi, un programme de formation et de sensibilisation, adapté aux différents acteurs de l'organisation, va permettre de faciliter la transition et pourra servir de preuve de conformité auprès de l'autorité de contrôle compétente afin de démontrer l'effort d'adaptation de l'entreprise.

Le programme sera à adapter aux différents profils identifiés au sein de l'organisation et verra ses objectifs changer en fonction des acteurs concernés. Par exemple, la Direction, les membres de la Direction des Systèmes d'Information ou de la Direction Juridique n'ont pas à disposer du même niveau de connaissance en matière de protection des données que le reste des collaborateurs.

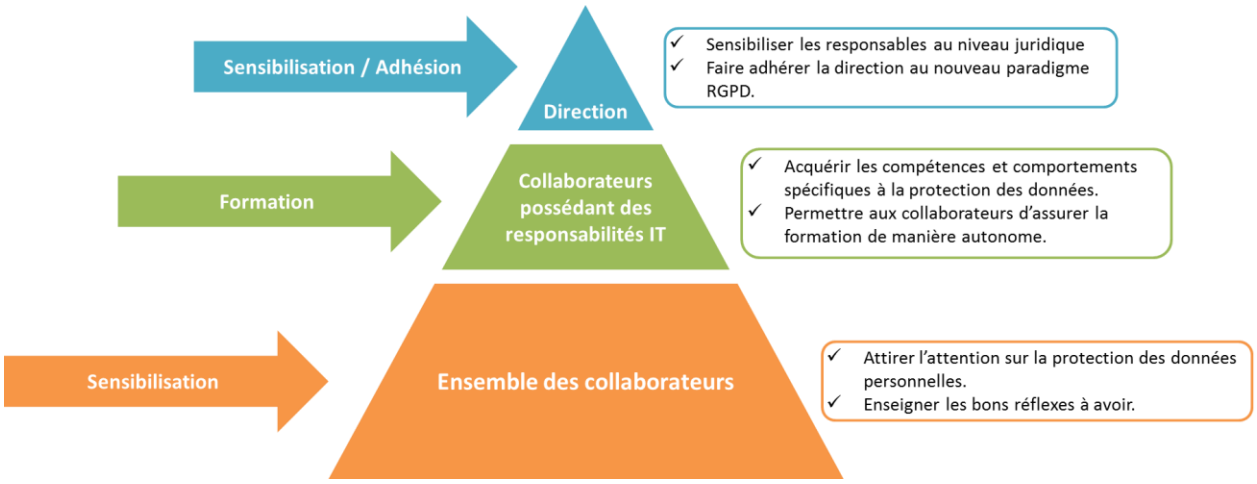


FIGURE 31 : TYPE DE FORMATION PAR PROFIL DE COLLABORATEURS

Concernant la Direction, l'enjeu est de faire intégrer la nécessité de se conformer au RGPD et de sensibiliser sur les conséquences et sanctions administratives et financières en cas de violation de données ainsi que sur les impacts d'un tel événement (juridique, financier, d'image…). Ces nouveautés ne sont pas toujours bien vues des équipes métiers, notamment Marketing, qui pensent risquer de perdre en qualité sur les services apportés, le ciblage des prospects, etc. Il est donc important que la Direction Générale montre un engagement clair afin de définir des procédures, et notamment en communication, afin de minimiser les répercussions.

Les collaborateurs traitant des Données à Caractère Personnel (DCP) tels que les collaborateurs du service Marketing ou des Ressources Humaines, par exemple,

pourraient se voir dispenser une formation en présentiel leur présentant les grands principes et les obligations du RGPD (licéité du traitement, respect du droit des personnes, Analyse d'Impact relative à la Protection des Données, etc.). Cette formation permettra d'adapter leurs pratiques notamment en termes de collecte et de suppression des données afin de se conformer à la nouvelle réglementation. Les procédures mises en place afin de respecter les nouvelles obligations, en ce qui concerne le droit des personnes notamment, pourraient leur être présentées lors de cette formation ainsi que les outils existants et utilisés par l'organisation.

Concernant la sensibilisation de l'ensemble des collaborateurs, différentes méthodes existent pour viser un maximum de personnes telles que des campagnes de mail, l'affichage d'une infographie dans les locaux, la formation en ligne. La sensibilisation vise à informer l'ensemble des collaborateurs de l'existence d'une nouvelle réglementation en matière de protection des données et des points clés de cette dernière.

Le contrôle des objectifs peut être effectué par un questionnaire en ligne obligatoire, à remplir par chacun des collaborateurs. Ainsi, les résultats compilés de ce questionnaire pourront permettre d'avoir une vision globale du niveau de sensibilisation / formation des collaborateurs et de prouver la démarche de sensibilisation de l'organisation.

6. Référentiels et organismes sur lesquels s'appuyer

6.1 Présentation de la CNIL

Législation locale	Loi Informatique et Libertés, CNIL3 	
Modification des lois suite RGPD	• Droits à la récupération des données ; • DPD ; • Action de groupe	
Autorité de contrôle	Commission Nationale Informatique et Libertés	
Depuis	1978	
Site web	https://www.cnil.fr/	
Activité		
Activité	• 8 360 de plaintes en 2017 • 8 297 plaintes traitées • 256 contrôles sur place et 65 en ligne	
Résultats des plaintes : non-lieu/mise en demeure/amende	• 79 mises en demeure • 9 amendes • 5 avertissements • 14 sanctions	
Sanction maximale (prévue loi/appliquée)	3 000 000€ depuis la Loi Lemaire (2016) 150 000€ avant	
Où va l'amende ? (frais de fonctionnement de l'autorité ou Etat)	Trésor Public	
Budget de fonctionnement		
Actuel	17 161 536 €	**+ 600 000 €** 
Prévisionnel avec RGPD	17 761 536 €	
Ressources humaines	198 employés	

6.2 Les Labels de la CNIL

Tous ces labels sont destinés à disparaître au profit de la certification, prévue à l'article 42 du RGPD. Ces certifications seront délivrées par des organismes certificateurs, sur la base de référentiels élaborés par la CNIL[22].

Label CNIL Gouvernance Informatique et Libertés

Ce label « Gouvernance » porte sur l'organisation, les mesures, les règles, les procédures et les bonnes pratiques qui sont conformes aux 25 exigences du référentiel édité par la CNIL. Ces 25 exigences portent sur trois domaines :

- L'organisation interne de la gestion des données personnelles ;
- La procédure de vérification de la conformité des traitements à la loi ;
- La gestion des plaintes et incidents.

Ce référentiel a été modifié en juillet 2017 pour prendre en compte les exigences du RGPD.

Label CNIL Coffre-fort numérique

Ce label « coffre-fort numérique » porte sur la conformité à 22 exigences publiées par la CNIL en janvier 2014. L'objectif est d'attester de la confidentialité, de l'intégrité et de la disponibilité des données stockées.

Audit de traitements

Le label « procédures d'audit informatique et libertés » porte sur la conformité à 73 exigences publiées en octobre 2011. Ce label s'applique à la procédure d'audit du traitement et non au traitement. Cet audit de traitement a pour objectif de vérifier la conformité à la loi Informatique et Libertés.

6.3 Outils et méthodes proposés par la CNIL

La CNIL a mis à disposition des organisations plusieurs outils permettant de faciliter leurs tâches telles qu'un modèle de fiche de registre des traitements[23] et un outil complet d'Analyse d'Impact relative à la Protection des Données (AIPD), entre autre.

Les méthodes, outils, et documents présentés ci-dessous permettent de couvrir les différentes étapes de mise en conformité au Règlement.

[22] https://www.cnil.fr/sites/default/files/atoms/files/cnil-38e_rapport_annuel_2017.pdf
[23] https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

Outil et documentation AIPD

La CNIL a mis en place un outil facilitant la réalisation des AIPD. Ce logiciel permet de couvrir les aspects et informations minimales à renseigner lors d'une AIPD. Le modèle d'AIPD proposé aux organisations comprend les parties suivantes :

- Le contexte du traitement dont notamment une description précise du traitement, de son responsable, des types de données traitées (supports, cycle de vie…) ;
- La mise en ligne de tous les travaux du G29, le groupement des autorités de contrôle européennes ;
- Les principes fondamentaux visant à démontrer le respect des critères énoncés dans l'article 6 du RGPD (proportionnalité, nécessité et mesures protectrices des droits) ;
- L'analyse des risques permettant de réaliser une appréciation des risques sur la vie privée au regard des mesures existantes ou prévues en cas de perte, modification illégitime ou disparition de données à caractère personnel ;
- Une partie validation visant à préparer et formaliser la validation de l'AIPD incluant la cartographie des risques, la description du plan d'action et l'avis du DPO.

Cet outil est également accompagné d'une base de connaissances et de définitions permettant de guider la réalisation d'AIPD. En pratique, cet outil open source permet d'obtenir une AIPD sous un format ouvert, le *JSON*, ce qui permet facilement l'import dans un logiciel interne à chaque entreprise voire de l'intégrer directement au SI interne. Une seconde version incluant une base de connaissance a été mise en ligne.

La CNIL a également publié trois documents en format *PDF* pour aider à la réalisation d'une AIPD. Le premier guide[24] décrit une méthode complète permettant d'obtenir une AIPD valide. Ce document reprend les 4 parties de l'outil : contexte, principes fondamentaux, analyse de risques et validation. Le second[25] fournit des exemples standards pour chaque champ du logiciel. Ensuite, le troisième[26] reprend en totalité la base de connaissances disponible depuis le logiciel. Il renseigne par exemple les typologies de données à caractère personnel, de supports de données, des mesures à mettre en œuvre telles quel le chiffrement, le cloisonnement des données, etc. Enfin, le dernier[27] expose un exemple d'AIPD avec l'un des traitements d'une entreprise fictive « captoo ».

Enfin, la CNIL, dans un article concernant les enjeux pour 2018, a déclaré travailler sur une liste de traitements nécessitant une AIPD et sur une autre recensant ceux, qui au contraire, n'en nécessiteraient pas. Ces listes permettront aux organisations

[24] https://www.cnil.fr/sites/default/files/atoms/files/cnil-PIA-1-fr-methode.pdf
[25] https://www.cnil.fr/sites/default/files/atoms/files/cnil-PIA-2-fr-modeles.pdf
[26] https://www.cnil.fr/sites/default/files/atoms/files/cnil-PIA-3-fr-basesdeconnaissances.pdf
[27] https://www.cnil.fr/sites/default/files/atoms/files/cnil-PIA-captoo-fr.pdf

de mieux appréhender leur obligation de mener une AIPD sur certains types de traitement.

Délégué à la Protection des Données (DPD) ou Data Protection Officer (DPO)

Bien qu'il n'y ait aucune obligation pour les organismes privés ne traitant pas de données sensibles à grande échelle, la désignation d'un DPD est fortement encouragée par le G29, afin de faciliter la mise en conformité au Règlement. C'est pourquoi, la CNIL a mis en place une fonctionnalité[28] pour déclarer en ligne un Délégué à la Protection des Données. Cette nomination prendra effet le 25 mai 2018 au moment de l'application du Règlement.

Registre des traitements

Le registre des traitements étant une étape essentielle dans la mise en conformité au Règlement, la CNIL a récemment publié un exemple[29] de fiche du registre de traitements. Couvrant, *a minima*, toutes les informations exposées dans l'article 30 du RGPD, ce registre permet aux organisations d'identifier toutes les informations à renseigner sur chaque traitement ainsi que de décrire leurs traitements mis en œuvre.

Plan d'accompagnement à destination des TPE/PME

Au cours du mois d'avril 2018, la CNIL et BPIFRANCE ont publié un guide[30] d'accompagnement pragmatique pour les TPE/PME pour une mise en conformité au RGPD adaptée à leurs moyens. Ce guide, sous forme de fiches thématiques, couvre tous les principes fondamentaux du RGPD à respecter *a minima*. Il est également accompagné de fiches pratiques qui reprennent des exemples de traitements communs à la majorité des PME/TPE (gestion RH, vente en ligne, relation client…).

6.4 Les normes ISO autour de la Privacy

A ce jour, 3 familles de normes rédigées par des professionnels peuvent aider les organisations à se mettre en conformité et à répondre aux enjeux réglementaires, c'est-à-dire prouver leur conformité :

- Les normes de terminologie et celles portant sur les principes ;
- Les normes sur les processus/le management ;
- Les normes sur les technologies.

[28] https://www.cnil.fr/fr/designation-dpo …

[29] https://www.cnil.fr/sites/default/files/atoms/files/registre_rgpd_basique.pdf

[30] https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement

Normes ISO/IEC		
ISO/IEC 29100 ISO/IEC 29101	ISO/IEC 29134 ISO/IEC 29190 ISO/IEC 27001	ISO/IEC 27002 ISO/IEC 27018 ISO/IEC 27552 ISO/IEC 29151

FIGURE 32 : NORMES EN LIEN AVEC LA PROTECTION DES DONNEES PERSONNELLES

Les normes de terminologie et sur les principes

La norme ISO/IEC 29100 « Privacy framework », publiée en 2011, a pour objectif d'accompagner les entreprises dans l'identification des besoins de sécurité de la vie privée dans le cadre des Technologies de l'Information et de la Communication en :

- Spécifiant une terminologie commune sur le domaine de la vie privée ;
- Définissant les différents acteurs et leurs rôles au sein du traitement des DCP ;
- Décrivant les besoins de sécurité à mettre en place ;
- Référençant les principes de la vie privée.

Cette norme cadre le développement des autres normes relatives à la protection de la vie privée. Cette base de réflexion, issue de la réglementation européenne et de la loi Informatique et Libertés, définit 11 principes généraux en conformité avec le RGPD tout en précisant certains aspects.

Principe ISO/IEC 29100

- Le consentement éclairé des personnes concernées ;
- La légitimité et la communication de la finalité des traitements ;
- Les données collectées sont adéquates, pertinentes et non excessives au regard de la finalité ;
- Les données utilisées sont minimisées et cloisonnées ;
- Le traitement, la conservation et la diffusio de données sont limités ;
- Les données sont exactes, complètes et tenues à jour ;
- L'information des personnes concernées est complète ;
- Les personnes concernées disposent d'un droit d'accès et de rectification ;
- La capacité à gérer les données et à rendre compte (« accountability ») ;
- La sécurité des données ;
- La gestion des risques et le contrôle continu.

FIGURE 33 : PRINCIPES DE LA NORME ISO 29100

Cette norme complète le RGPD, notamment en dessinant les contours du principe d'auditabilité, et introduit certaines pratiques issues des systèmes de management de la qualité. Citons par exemple :

- La formation adaptée des personnels chargés des traitements ;
- La gestion des plaintes, la notification des failles de sécurité ;
- Les correctifs et compensation en cas de préjudices.

Le contrôle de « la conformité » vise à être réalisé par un système de management avec une approche par amélioration continue, par la gestion de la documentation et par de l'audit interne.

Il existe également une norme, encore peu utilisée en France, l'ISO/IEC 29101 qui définit une architecture de référence et les contrôles associés pour la protection de la vie privée dans les systèmes de communication qui stockent et traitent des données personnelles.

Les normes sur les processus/le management :

ISO/IEC 29134 - « Lignes directrices pour mener des études d'impact sur la vie privée »

Cette norme, publiée en 2017, a pour objectif de donner une méthodologie d'études d'impact sur la vie privée (EIVP – AIPD dans notre document) ainsi que de décrire la structure et le contenu du rapport d'AIPD. Afin de prouver sa conformité au RGPD, cette norme apporte un outil pour répondre de manière homogène au niveau international aux demandes d'AIPD exigées par le Règlement.

ISO/IEC 29190 - « Méthodologie pour la maturité dans le domaine de la protection de la vie privée »

Cette norme a pour objectif de fournir un guide d'évaluation sur l'aptitude d'une organisation à gérer les processus concernant la vie privée. Elle fournit un modèle de maturité qui s'appuie sur des processus d'évaluation déjà normés.

ISO 27001 - Information Security Management Systems (ISMS)

Cette norme a pour objectif de déterminer les besoins afin d'établir, réaliser, maintenir, et améliorer continuellement le système de management de sécurité de l'information dans le périmètre de l'organisation.

ISO 29151 – « Code de bonne pratique pour la protection des données à caractère personnel »

Cette norme a pour objectif d'établir les objectifs de contrôle, leur nature, ainsi que les lignes directrices afin de les mettre en œuvre pour répondre aux exigences identifiées par une évaluation des risques et des impacts relatifs à la protection des données personnelles. Elle ajoute des points de contrôle à la norme 27002 (voir ci-après) pour mettre en œuvre les 11 principes de la norme ISO/IEC 29100.

Les normes sur les technologies :

ISO 27002 – « Code de bonne pratique pour le management de la sécurité de l'information »

Cette norme a pour objectif d'élaborer des lignes directrices de management de la sécurité de l'information spécifiques aux organisations. Ce sont des bonnes pratiques permettant notamment d'être en conformité avec l'annexe A normative de l'ISO 27001.

ISO 27018 – « Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors »

Cette norme a pour objectif de créer un ensemble de catégories de sécurité et de contrôles communs mis en œuvre par un fournisseur de services de *cloud computing* public agissant en tant que traitement de DCP.

ISO/IEC 27552 - Extension d'ISO/IEC 27001 à la gestion de la protection de la vie privée (en cours de rédaction à la date de publication du présent Cahier Technique)

La norme ISO/IEC 27552 « Technologies de l'information – Techniques de sécurité – Extension d'ISO/IEC 27001 à la gestion de la protection de la vie privée – Exigences » est actuellement au stade des commentaires et votes. Cette norme a pour but de donner des exigences et des objectifs complémentaires à l'ISO 27001 sur la protection de la vie privée. En se basant sur l'ISO/IEC 27001, elle prend en compte le cadre et les principes de l'ISO/IEC 29100, l'ISO/IEC 29151, ainsi que le RGPD pour proposer un système de management des informations personnelles.

Cette norme étant en cours de rédaction, le contenu technique et éditorial est susceptible de changer.

6.5 CIGREF, TECH IN France et AFAI

Ces organismes ont édité un livre sur la bonne application du RGPD : « Entreprises, les clés d'une bonne application du RGPD ». Des outils y sont proposés pour une mise en conformité avec le RGPD, ainsi que trois check-lists pour évaluer la conformité. Ils se présentent aussi sous la forme Microsoft Excel avec une liste de recommandations et de mesures techniques.

6.6 Associations d'experts

Association Française des Correspondants aux Données Personnelles (AFCDP) :

Cette association ouverte au CIL, DPD ou à toute personne intéressée par la protection des données à caractère personnel propose à ses adhérents d'échanger de manière concrète autour de la protection des données. De plus, elle a pour but de développer la concertation avec les pouvoirs publics, de participer à la création

de documents ou de recommandations pour les autorités ou les acteurs de la protection des données personnelles. Elle a également pour objectif de promouvoir la fonction de DPD.

Association des Data Protection Officers :

Présidée et fondée par Alain Bensoussan, avocat, cette association a pour but d'accompagner les Délégués à la Protection des Données de tous types d'organismes, et propose un lieu de réflexion et de concertation sur les bonnes pratiques à mettre en œuvre. Elle est organisée en 9 commissions (Ethique, Médiation, Pratiques Professionnelles, RGPD, Conformité et gouvernance, Responsabilité et protection, Santé, Cybersécurité). Hélène Legras, vice-présidente de l'association a récemment présenté sa réflexion et son expertise sur l'application du RGPD (« Data Protection Officer et mise en conformité selon le RGPD », Rev. prat. prospect. innov. n° 2 oct. 2017, Le point sur n° 2, p. 51-52.).

6.7 Certifications

L'article 42 du Règlement Général sur la Protection des Données prévoit la certification de la protection des données personnelles par un organisme agréé. Cette certification vise à faire constater par un organisme de certification que des mesures techniques et organisationnelles appropriées ont été mises en place pour le respect des obligations incombant au responsable du traitement ou à un sous-traitant.

ISO/IEC 27001, beaucoup d'organismes (entre autres : Bureau Veritas, LSTI, PricewaterhouseCoopers, BSI, etc.) sont accrédités pour certifier selon cette norme. Les organisations la suivant sont susceptibles de répondre à différentes exigences de sécurité « techniques et administratives appropriées » du RGPD. Néanmoins, cette norme ne définit pas d'exigences spécifiques à un système de management dédié à la protection de la vie privée.

AFNOR Certification propose une certification « *AFAQ Protection des données personnelles* » qui vise à démontrer à l'autorité de contrôle l'organisation et les moyens techniques mis en œuvre pour atteindre la conformité au RGPD. Elle est construite pour accompagner les organisations dans la garantie du respect de grands principes issus du RGPD.

Bureau Veritas propose également deux certifications : la première sur la gestion de la protection des données et la seconde à destination des DPD. Concernant les DPD, le processus de certification a pour but d'évaluer les compétences de délégué à la protection des données. Il existe actuellement trois catégories de compétences (Experts RGPD, DPD, DPD en matière de santé). Concernant la gestion de la protection des données, Bureau Veritas a élaboré un référentiel technique qui prend

en compte les normes ISO existantes pour aider les entreprises gérant des données à caractère personnel à se conformer au RGPD[31].

[31] http://www.bureauveritas.fr/white-papers/white-papers-standard-protection-des-donnees

7. Ailleurs en Europe

Sont décrits ci-dessous les législations locales et les modes de fonctionnement dans certains des autres pays de l'Union Européééenne (non exhaustif) .

7.1 Allemagne

Législation locale	Bundesdatenschutzgesetz (BDSG) 	
Modification des lois suite RGPD (action de groupe, DPD, etc.)	• DPD • Consentement écrit des employés pour le traitement de leurs données par les employeurs • Actions de groupe	
Autorité de Contrôle	*Federal Data Protection Commissioner and Freedom of Information* + 1 autorité dans chaque Land (17 au total)	
Depuis	1978	
Site web	https://www.bfdi.bund.de/	
Activité		
Activité	• 10386 enregistrements entrants (2016) • ~100 informations/conseils/inspections (rapport 2016) • 7 plaintes au niveau fédéral	
Sanction maximale (prévue loi/appliquée)	20 millions € ou 4% du chiffre d'affaires Pénal : jusqu'à 2 à 3 ans d'emprisonnement	
Destination de l'amende (frais de fonctionnement de l'autorité ou l'Etat)	Compte de l'autorité	
Budget de fonctionnement		
Actuel	13,7 millions € (2016)	**+ 4,5 M€**
Prévisionnel avec RGPD	18,2 million € (2017)	

Législation locale	Bundesdatenschutzgesetz (BDSG)	
Ressources Humaines		
Actuel	149 employés (2017, dont 20 postes vacants à la fin de l'année)	**+18%** 
Après le RGPD	176 employés	

Dès juillet 2017, l'Allemagne a été le premier pays à adapter son droit national à l'arrivée du RGPD. Le nouveau German Federal Data Protection Act[32] (BDSG, « BundesDatenSchutzGesetz » en allemand) a remplacé la législation précédente.

Les législateurs ont grandement usé des « règles spécifiques » (« *opening clauses* ») et ont introduit certaines dispositions applicables pour le secteur privé :

- **Traitement des données dans le cadre des relations de travail** (article 88 du RGPD — section 26 du BDSG) :
  - Enquête sur les salariés : Le BDSG intègre des restrictions relatives aux enquêtes sur des infractions pénales, à moins que la personne concernée n'ait commis l'infraction sur son lieu de travail,
  - Transparence envers le salarié : Le salarié doit être mis au courant des données traitées par l'entreprise par un moyen clair et écrit. Un accord collectif doit déterminer les données sensibles,
  - Précisions sur le consentement : la personne concernée doit donner son consentement de manière claire et explicite par écrit (« à moins qu'une autre forme ne soit plus appropriée » - ce point n'étant pas spécifié davantage). Le traitement des données collectées doit exclusivement avoir une finalité liée à l'emploi.
- **Catégories spécifiques de données** : santé (section 22 du BDSG) :
  - Entre un professionnel de santé (soumis au secret professionnel) et la personne concernée, sous réserve d'un contrat, le traitement des données est autorisé à des fins de médecine préventive, d'élaboration d'un diagnostic médical.
  - Le traitement doit présenter des garanties « adaptées et spécifiques », prenant en compte l'état de l'art, le coût de l'implémentation, tels que des mesures organisationnelles et techniques, des mesures concernant la traçabilité, l'anonymisation, le chiffrement, l'obligation de nommer un Délégué à la Protection des données (DPD), ou encore un ensemble

[32] https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf

de mesures concernant la confidentialité, l'intégrité, la disponibilité, la résilience des systèmes (art. 32 du RGPD).

- **Traitement de données à des fins de recherche et statistiques** (section 27 du BDSG) :
  - la collecte peut être autorisée sans consentement si, et seulement si, les intérêts de la recherche l'emportent sur les intérêts de la personne dont les données ont été collectées et que des garanties de protection (exemple : pseudonymisation) sont apportées.
- **Traitement pour de nouvelles finalités** (section 24 du BDSG) :
  - Le changement des objectifs pour lesquels le traitement a été appliqué n'est autorisé que pour des raisons de défense nationale, sûreté public, poursuites judiciaires, ou faire valoir les droits en justice.
- **Restrictions relatives aux droits de la personne** (section 32 du BDSG — article 13 du RGPD) :
  - Dans certains cas, le BDSG exempte le responsable du traitement de son obligation d'informer la personne concernée si l'information collectée peut compromettre l'intérêt public.
  - Si l'effacement de données (automatisé ou non) est impossible ou si cela implique un effort disproportionné par rapport au stockage, et si les données conservées sont restreintes au minimum, alors la personne concernée ne pourra exercer son droit à l'effacement (section 35 du BDSG — article 17 du RGPD) et le responsable du traitement n'est pas tenu d'informer la personne.
  - Cette section a été beaucoup critiquée par la Commission Européenne en raison des restrictions liées au droit à l'information et à l'effacement. La décision finale devrait être donnée par la Commission Européenne prochainement.
- **Vidéosurveillance** (section 4 du BDSG) :
  - le RGPD ne fournit pas explicitement de clauses dérogatoires, mais le BDSG fait part de règles spécifiques qui s'appliquent aux vidéos de surveillances placées dans les espaces publics (le nom des contrôleurs doit être identifiable).
- **Désignation d'un Délégué à la Protection des Données** (section 38 du BDSG — art. 37 du RGPD) :
  - Les entreprises présentes en Allemagne, employant au moins 10 personnes pour le traitement des données, doivent nommer un DPD ;
  - Si un organisme doit réaliser une AIPD alors un DPD doit être obligatoirement nommé (indépendamment du nombre d'employés dans le traitement des données).
- **Les sanctions** (section 41 à 43 du BDSG) :
  - Le responsable de traitement, le sous-traitant ou la personne désignée pour réaliser le traitement des données, peut être condamné jusqu'à 3 ans de prison pour avoir transféré des données personnelles non publiques à une tierce personne sans autorisation, ou les a rendues accessibles à des fins commerciales ;

- Certaines dispositions de l'Administrative Offenses Act (AOA) ne seront plus applicables en cas de violation de l'article 83, paragraphes 4 à 8 du RGPD. Le montant des amendes sera donc basé sur le plafonnement prévu par le RGPD soit, 20 millions d'euros ou 4% du chiffre d'affaires global.

Conclusion

Certains ministères allemands ont déjà indiqué entrer dans leurs comptabilités des provisions liées notamment à la protection des données de la sécurité sociale.

Par ailleurs, le BDSG est controversé puisque certaines dispositions dépassent le champ d'application du RGPD. Ce qui pose donc un problème quant à l'harmonisation (tout comme la LIL ou d'autres législations nationales) des lois sur la protection des données à l'échelle européenne :

- **La responsabilité** : alors que le RGPD stipule que les amendes seront imposées aux entreprises qui violent le Règlement, le BDSG lui, offre la possibilité de sanctionner des individus, tels que les managers ou les employés ;
- **La nomination d'un Délégué de la Protection des Données :** elle est nécessaire, si 10 employés ou plus d'une entreprise sont impliqués dans le traitement des données, alors que le RGPD ne l'impose que pour les organismes qui traitent des données sensibles ;
- **Protection des données personnelles sur le lieu de travail :** les entreprises doivent se soumettre aux obligations liées à la justification des finalités du traitement des données personnelles de leurs employés. Alors que le RGPD dispose que le consentement écrit n'est pas obligatoire, le BDSG impose une forme écrite et la réalisation d'un « test » pour s'assurer que l'employé a bien donné son consentement.
- **Restrictions des droits des personnes concernées :** l'obligation d'informer la personne concernée du traitement de ses données peut être limitée dans le cas où cette information pourrait avoir un impact sur la défense juridique du responsable de traitement.

7.2 Espagne

Législation locale	Ley Organica de Proteccion de Datos 	
Modification des lois suite RGPD (action de groupe, DPD, etc.)	• DPD • Droits des personnes concernées • Action de groupe	
Autorité de Contrôle	Agencia Española de Protección de Datos (AEPD) deux agences de provinces autonomes : - l'Autorité Catalane de Protection de Données - l'Agence Basque de Protection de Données.	
Depuis	1993	
Site web	http://www.agpd.es	
Activité		
Activité	• 10523 plaintes enregistrées (2016) • 8112 plaintes traitées (2016)	
Sanction maximale (prévue loi/appliquée)	600 000 € 2016 : amendes totales de 14 190 173 €	
Destination de l'amende (frais de fonctionnement de l'autorité ou l'Etat)	Compte de l'autorité	
Budget de fonctionnement		
Actuel	14,10 million € (2017)	?
Prévisionnel avec RGPD	/	
Ressources Humaines		
Actuel	179 employés (2017)	?
Après le RGPD	/	

La Constitution espagnole reconnait le droit à la protection des données personnelles (articles 10 et 18 paragraphe 4). Le traitement de ces données est encadré par la loi organique 15/1999[33] (LOPD) et le décret royal 1720/2007[34]. L'autorité de contrôle Espagnole en charge du respect de ces législations est la « Agencia Española de Protección de Datos » (AEPD).

LOPD et RGPD, ce qui va changer

FIGURE 34 : LOPD ET RGPD

Le rôle et les exigences de l'AEPD

La nouvelle LOPD devra élargir son champ d'application, et protéger les citoyens européens et espagnols. Avec le RGPD, la LOPD devra subir de nombreuses modifications.

L'AEPD devra évoluer notamment sur les points suivants :

- La protection des données génétiques et biométriques ;
- Les principes liés aux traitements des données en plus de l'inscription au registre général de la protection des données ;
- Et définir un délai de notification de violation de données à 72h (alors que la communication de failles de sécurité était jusqu'à présent facultative).

Le droit des utilisateurs

Actuellement, les droits utilisateurs sont couverts selon quatre droits (dits « ARCO »):

- Accessibilité ;
- Rectification ;

[33] https://www.gdt.guardiacivil.es/webgdt/media/Legislacion/LOPD.pdf
[34] https://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

- Annulation (« cancelación ») ;
- Opposition.

Cependant, avec le RGPD, ces droits seront renforcés et des nouveaux droits devront être ajoutés ou complétés, notamment : le droit à l'oubli, à la limitation du traitement et le droit à la portabilité.

Les obligations et les procédures de traitement

Le RGPD demande en plus de la LOPD une minimisation des données collectées et une limitation de la durée du traitement. Par ailleurs, le RGPD ajoute la réalisation d'une Analyse d'Impact relative à la Protection des Données (AIPD) sur les traitements les plus sensibles.

Alors que la LOPD n'impose la mise en place de mesures de sécurité que sur certaines données sensibles (laissant par ailleurs une certaine liberté aux organisations de choisir quelles sont les données jugées sensibles), le RGPD impose qu'il est nécessaire d'établir par défaut et dès la conception des mesures techniques et organisationnelles adéquates à tout traitement de données à caractère personnel. Par ailleurs, le traitement des données doit faire l'objet d'une inscription au registre des traitements.

La nomination du DPD est également une nouveauté.

Le régime des sanctions

Dans la LOPD, en cas d'infraction « mineure » (par exemple une non inscription au registre de l'AEPD, une collecte de données sans information préalable de l'AEPD, ou une absence de réponse aux demandes de rectification ou d'annulation), les sanctions sont plafonnées à 60 000 €. Si l'infraction est jugée comme « grave » (par exemple comme modifier la finalité du traitement sans avertir l'AEPD, ne pas obtenir le consentement de la personne concernée, refuser l'accès aux données collectées, traiter des données sensibles sans autorisation), alors les sanctions peuvent atteindre 300 000 €. Enfin, si les infractions sont considérées comme « très graves », telles que la collecte de données de manière frauduleuse ou le transfert et la vente de données non autorisés, la sanction est plafonnée à 600 000 €.

Ce niveau de sanction doit être ajusté avec le RGPD qui dispose que les amendes pourront aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires global de l'année précédente. Par ailleurs, le projet de révision de la LOPD ajoute que les amendes supérieures à 300 000€ devront être versées dans un délai de trois ans.

Le nouveau projet de loi sur la protection des données personnelles

Depuis le 25 mai 2018, la majeure partie des articles de la LOPD sont en désaccord avec le Règlement. Le Parlement espagnol a entamé une procédure de réforme censée transposer les obligations imposées par le RGPD.

Le projet de loi de modification de la loi organique sur la protection des données[35] a été approuvé par le Conseil des Ministres le 10 novembre 2017. Cependant, à la date d'écriture de ce cahier technique, le projet est toujours en cours d'adoption, depuis le 24 novembre 2017 au sein du Congrès. Par conséquent, depuis le 25 mai 2018, et jusqu'à ce que la nouvelle loi n'entre en vigueur, est né un vide juridique dans lequel certaines spécificités espagnoles ne seront pas régulées.

Quelques exemples de modifications retenues dans le projet de loi :

- Le consentement : une personne est considérée majeure à partir de 13 ans ;
- Le responsable du traitement peut être une personne physique ou morale et n'est pas tenu d'être un employé de l'organisation même. L'AEPD est chargée d'entretenir une relation transparente avec les Délégués de la Protection des Données (leur nomination n'est pas imposée juridiquement) ;
- La loi organique régule le régime de l'AEPD et reflète l'existence des autorités locales de protection des données et la nécessaire coopération entre les autorités de contrôle. L'AEPD est une autorité administrative indépendante en vertu de la loi 40/2015 du régime juridique du secteur public et est sous l'autorité du Ministère de la Justice (art.48.2 « le président de l'AEPD sera nommé par le gouvernement, sous proposition du Ministère de la Justice ») ;
- L'article 83 de la LOPD relatif aux « conditions générales pour imposer des amendes administrative » et son point 7 laissent la liberté aux Etats membres de déterminer « dans quelle mesure des amendes administratives peuvent être imposées à des autorités publiques et à des organismes publics ». Dans son article 77, le projet de loi décide ne sanctionner en aucun cas une autorité ou un organisme administratif en cas d'infraction du droit à la protection des données personnelles d'une personne concernée.

Conclusion

Actuellement, les propositions d'amendements sont revues et le projet de loi n'est pas encore promulgué. Le Congrès des Députés n'a toujours pas fixé la date d'approbation de cette nouvelle loi. A compter du 25 mai 2018 selon les traités de l'Union Européenne, l'Espagne devra appliquer le RGPD, alors que la loi nationale adaptée ne sera pas encore disponible. Cette inadéquation engendre une incertitude juridique.

[35] http://www.congreso.es/backoffice_doc/prensa/notas_prensa/57631_1518684517278.PDF

7.3 Le Brexit et les implications sur le RGPD

Législation locale	Data Protection Act 	
Modification des lois suite RGPD (action de groupe, DPD, etc.)	• DPD • Droits des personnes concernées • Action de groupe	
Autorité de Contrôle	ICO - Information Commission Officer	
Depuis	1984	
Site Web	https://ico.org.uk/	
Activité		
Activité	• 18 354 (2017) • 17 335 (2017)	
Sanction maximale (prévue loi/appliquée)	£500,000 (573 345€) • 23 amendes (£1 923 000); • 16 sanctions civiles (£1 624 500); • 55 DPD infractions; 600 plaintes CCTV - vidéosurveillance)	
Destination de l'amende (frais de fonctionnement de l'autorité ou l'Etat)	Gouvernement	
Budget de fonctionnement		
Actuel	20 345 595 € (2017)	**+ 14 M€**
Prévisionnel avec RGPD	34 587 512 € (2018)	
Ressources Humaines		
Actuel	472 employés (2017)	**+ 37%**
Après le RGPD	650 employés (2018)	

Actuellement, toutes les organisations au sein du Royaume-Uni (RU) qui collectent, traitent et hébergent des données personnelles sont soumises au **Data Protection**

Act 1998 (DPA). En cas de non-respect, elles peuvent être sanctionnées à hauteur de £500,000 (573 345 €).

Le RU héberge le plus grand marché de Datacenters en Europe et le troisième plus grand à l'échelle mondiale. Le RGPD est entré en vigueur depuis le 25 mai 2018, alors même que les négociations sur la sortie du Royaume-Uni de l'UE (Brexit) suivent leur cours. Ainsi, le Royaume-Uni devra se conformer au RGPD avant sa sortie de l'UE, après quoi il pourra faire le choix d'une législation nationale propre répondant aux exigences du RGPD, ou opter pour un accord copié sur le modèle du Privacy Shield entre l'UE et les Etats-Unis.

Data Protection Act (DPA)

L'introduction de la Directive 95/46/CE a été transposée par le **Data Protection Act** (DPA) en 1998 afin de faciliter et de contrôler les flux de données transnationales. Cependant, l'échec de la transposition à l'échelle européenne a conduit le Parlement Européen à la remplacer par le RGPD 2016/679. Ainsi, le nouveau Règlement abrogera la précédente Directive et devra s'appliquer directement au Royaume-Uni**.**

Le RGPD avant le Brexit

Membre de l'UE, le Royaume-Uni a commencé à adapter le RGPD en une loi nationale via le Data Protection Bill[36] (DPB). Les entreprises britanniques et les multinationales présentes au Royaume-Uni devront donc se soumettre aux obligations de cette loi, et de fait, se conformer au RGPD.

L'Information Commission Officer (ICO, autorité de contrôle en charge de la protection des données) s'est vu octroyer de nouveaux pouvoirs d'investigation. En effet, avec le DPA, l'ICO ne pouvait imposer des évaluations que pour des organismes publics. Dorénavant, toute organisation peut faire l'objet d'évaluation sur l'ensemble des procédures de traitement des données. De plus, tel que l'impose le RGPD, l'ICO peut attribuer des amendes allant jusqu'à 4% du chiffre d'affaires global.

Le RGPD après le Brexit

Le 29 janvier 2018, la Commission Européenne a publié un communiqué[37] indiquant qu'à compter du 30 mars 2019, le Royaume-Uni sera considéré comme un « pays tiers ». Les conditions de transfert de données entre les pays membres de l'UE et le Royaume-Uni seront directement impactées, à moins que la Commission ne reconnaisse que le pays assure une protection adéquate des données.

[36] https://publications.parliament.uk/pa/bills/cbill/2017-2019/0190/18190.pdf
[37] http://europa.eu/rapid/press-release_IP-18-463_fr.htm

Ainsi, un transfert vers le Royaume-Uni ne sera accordé que si le responsable de traitement (ou sous-traitant) répond aux « garanties appropriées » (art. 46 du RGPD), telles la signature de clauses contractuelles ou la certification des responsables de traitement.

Cependant, au vu des démarches déjà entamées par le Royaume-Uni pour appliquer le RGPD, on peut prévoir qu'après le Brexit, le Royaume-Uni soit considéré comme un pays assurant une protection adéquate des données.

Le Royaume-Uni souhaite mettre en place « une loi moins contraignante » pour les entreprises et l'innovation, et ainsi rendre le pays plus compétitif et attractif dans les échanges commerciaux. Si le Royaume-Uni fait le choix de se doter d'une réglementation nationale sur la protection des données, en prenant en compte l'extra-territorialité du RGPD, la double conformité au droit anglais et européen pèsera sur le coût des affaires des entreprises britanniques.

Conclusion

Il serait surprenant que les législateurs britanniques reviennent sur le RGPD, d'autant qu'ils auront déjà adopté leur loi nationale au Règlement. L'Union Européenne étant un des plus importants partenaires commerciaux du Royaume-Uni, afin de continuer à commercer avec les membres de l'UE et traiter des données de résidents de l'Union Européenne, ce dernier devra s'assurer que la loi britannique de protection des données est conforme avec le RGPD.

8. Conclusion

Parmi les nouvelles obligations introduites par le RGPD, certaines doivent être traitées prioritairement. Ainsi, comme dans tout projet d'entreprise, il est primordial que la Direction Générale prenne en main le sujet et l'inscrive à l'ordre du jour des Comités de Direction pour **désigner officiellement et au plus tôt un acteur** (sponsor) qui animera la mise en conformité de l'organisation (qu'il soit nommé officiellement DPD ou non).

La Direction Générale doit demander tout d'abord un **état des lieux des traitements de données personnelles réalisés**. Cela signifie une analyse de la conformité de l'organisation et l'identification des écarts de celle-ci par rapport à la règlementation pour s'assurer de leur légitimité, du recueil du consentement, du niveau de protection apporté aux données traitées et du respect de l'exercice des droits. La cartographie des traitements pourra prendre la forme d'un **registre** tel qu'il est décrit dans le chapitre « 5.3 Le registre et l'identification des traitements » de ce cahier.

Par la suite, un **plan d'action de mise en conformité** doit être défini en répartissant la mise en conformité au RGPD en une série de chantiers et d'actions spécifiques qui faciliteront sa mise en œuvre et la répartition des tâches aux différents acteurs impliqués.

Ce plan d'action inclut notamment la **sensibilisation** de l'ensemble des personnels (internes et sous-traitants), la mise en place des **processus organisationnels** requis (notification, traitement d'une demande d'accès, gestion de crise, etc.), l'identification des principales **mesures techniques** (voir « Figure 14: Exemple de planning de mise en conformité d'une organisation »), et le **contrôle** de cette conformité au sein de l'organisation et des sous-traitants.

Le **projet** doit prévoir l'intervention d'une équipe pluridisciplinaire couvrant les aspects juridiques et techniques multiples, le **Risk manager qui peut en être le pilote**, et bien sûr les données personnelles manipulées par les métiers. Sans cette pluridisciplinarité, des aspects importants d'une mise en conformité pourraient être négligés.

Pour l'Union Européenne, le RGPD est une avancée qui vise une harmonisation des règlementations nationales tout en laissant à la **libre appréciation des Etats Membres des marges de manœuvres sur des points importants**, comme par exemple, l'âge minimum du consentement sans nécessité d'un accord parental.

La société s'est emparée de la question primordiale de la consommation et de la protection de la donnée, et un cadre légal existe désormais au niveau européen pour contrôler les usages. Un effort important est demandé aux organisations pour se mettre en conformité dès à présent, diffuser et maintenir dans le temps une

culture de transparence et de respect de la vie privée dans les opérations réalisées à l'avenir.

Remerciements

Nous tenons à remercier l'ensemble des contributeurs de CGI Business Consulting: Mouloud Aït-Kaci, Aurélie André, Hinda Amalou, Erwan Bompard, Antonin Deneux, Thomas Nguyen, Marine Verbeke, Alexandra Zelmans et Vincent Mallet. Nous remercions également les contributeurs de l'AMRAE pour les relectures successives qui contribuent à la qualité de ce cahier technique.

Annexe – Législation associée au RGPD

Loi pour la Confiance dans l'Economie Numérique (LCEN) – Texte Français

La LCEN a prévu que les données collectées et leur durée de conservation devaient être définies dans un décret. Le 1er mars 2011, le ***"décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne"*** **est publié.** Les termes utilisés sont génériques et cherchent à maintenir une neutralité technologique. L'objectif est de contribuer à l'identification de la personne ayant publié un contenu donné. Cette loi vise à lutter contre les contenus illicites, notamment terroristes, diffusés par des hébergeurs sur l'internet.

- Les personnes fournissant un accès à Internet sont tenues de conserver ;
  - L'identifiant de la connexion (en pratique une adresse IP),
  - L'identifiant attribué par ces personnes à l'abonné,
  - L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès,
  - Les dates et heure de début et de fin de la connexion,
  - Les caractéristiques de la ligne de l'abonné,
- La durée de conservation de ces données est de 1 an ;
- Les données peuvent être communiquées aux agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationale spécialement chargés des missions de lutte contre le terrorisme. Ces données communiquées pourront être conservées maximum 3 ans dans des traitements automatisés mis en œuvre par le ministère de l'Intérieur et le ministère de la Défense.

Le RGPD ne va pas à l'encontre de ce décret mais confirme dans son article 5, cette possibilité sous la réserve des buts poursuivis par le traitement :

« e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation); »

e-Privacy – Texte Européen

La directive e-Privacy du 12 juillet 2002 vise à protéger de façon spécifique la vie privée dans le secteur des communications électroniques. Elle traite des aspects

complémentaires à la directive sur la protection des données. Elle vise toute entité et règlemente notamment l'envoi de messages commerciaux (OPt-In) et l'utilisation de cookies (OPt-Out). Elle sera probablement remplacée par un règlement en 2019.

« Lorsque, dans le respect du RGPD, une personne physique ou morale a, dans le cadre de la vente d'un produit ou d'un service, obtenu de son client ses coordonnées électroniques, ladite personne physique ou morale peut exploiter ces coordonnées électroniques à des fins de prospection directe pour des produits ou services analogues qu'elle-même fournit uniquement si le client se voit donner clairement et expressément la faculté de s'opposer, sans frais et de manière simple, à une telle exploitation. Le droit d'opposition est donné au moment où les coordonnées sont recueillies et lors de l'envoi de chaque message. »

L'intégration des métadonnées dans la catégorie « Donnée » apporte une extension du champ d'application de la confidentialité à l'ensemble des prestataires de services en ligne et non plus seulement aux fournisseurs d'accès à Internet. Actuellement, la loi soumet ce type d'entreprise au secret des correspondances sur les métadonnées (relevé téléphonique, durée, localisation, etc.) Autrement dit les entreprises comme Facebook, WhatsApp, SnapChat, Telegram et leurs employés devront respecter la même obligation de secret des correspondances sur les métadonnées que les opérateurs téléphoniques et fournisseurs d'accès à Internet. En cas de violation, ils s'exposent à des sanctions administratives de la part de l'autorité de contrôle locale comme l'ARCEP en France.

En pratique, ces entreprises devront obtenir le consentement de leurs utilisateurs avant d'analyser ou d'observer leurs données. Si ces acteurs s'étaient obligés d'eux-mêmes à respecter la confidentialité des données de contenu, ils pouvaient exploiter les métadonnées des utilisateurs à leur insu. Désormais, la collecte de ces données devra respecter les obligations du RGPD en matière de protection des données personnelles.

A l'instar de ce qui est prévu dans le RGPD, l'e-Privacy exige que ces acteurs s'assurent de la sécurité des données, ce qui leur impose de « mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté ». Le RGPD prévoit, par exemple, le recours à la pseudonymisation et au chiffrement des communications pour limiter le risque d'atteinte de la vie privée.

Capacités de traitement et modalités de stockage

Dans l'article 8 traitant de l'utilisation des **capacités de traitement et/ou de stockage** de l'ensemble des terminaux (ordinateur, smartphone, tablette, montre connectée, etc.), celle-ci **est interdite sans le consentement préalable de l'utilisateur final**. Cette interdiction concerne également la collecte des données transmises ou émises par un terminal.

La notion de consentement dans « e-Privacy » renvoie directement à la définition du RGPD. De plus, un rappel obligatoire tous les 6 mois du droit de retirer ce même consentement (Art.9.3 e-Privacy) est exigé.

Cet article 8 concerne donc principalement les sociétés achetant et/ou commercialisant des fichiers de données de navigation qui permettent de faire du profilage, et les sanctions peuvent s'avérer conséquentes.

La convergence avec le RGPD

Concernant le devoir d'information sur le consentement des utilisateurs, l'e-Privacy renvoie directement à la règlementation européenne. Comme explicité dans le RGPD, le responsable du traitement est en charge du recueil du consentement. Le retrait du consentement doit être facilement réalisable et l'absence de consentement ne pourra empêcher l'accès au service souhaité que dans le cas où le traitement de données concerné est absolument indispensable. Pour finir, la demande de consentement devra être compréhensible, accessible et distinct des autres mentions légales.

Les sanctions prévues au titre du non-respect de l'e-Privacy reprennent le barème des sanctions du RGDP : jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel en cas de violation d'un droit fondamental.

République numérique – Loi Lemaire – Texte Français

Open Data – Ouverture des données publiques

Depuis 1978, un droit d'accès aux documents administratifs pour toute personne est obligatoire. Cela signifie que tous les documents produits ou reçus dans le cadre de leur mission de service public par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une mission de service public doivent être disponibles.

Le champ d'application du droit d'accès aux documents administratifs a été élargi par la loi Lemaire en y ajoutant les codes sources, les règles définissant le traitement algorithmique et les principales caractéristiques de sa mise en œuvre au bénéfice de l'usager. Le règlement européen semble avoir inspiré la loi Lemaire concernant cet élargissement de périmètre.

La Loi Lemaire : une anticipation de la règlementation RGPD

Le RGPD est entré en application le 25 mai 2018, la France a souhaité anticiper en officialisant la loi pour une République Numérique le 8 octobre 2016. La loi Lemaire permet, en partie, de préparer la France de manière progressive au RGPD, le RGPD prévaut par la suite (post 25 mai 2018).

Concernant les points communs entre la loi Lemaire et le RGPD, rappelons :

- L'obligation pour le responsable de traitement d'informer la personne concernée de l'existence d'un droit sur ses données à caractère personnel après sa mort.
- Les responsables de traitement devront préciser la durée de conservation des données.
- Le droit à l'oubli numérique spécifique pour les mineurs.
- Des sanctions allant jusqu'à 3 millions d'euros jusqu'à l'entrée en application du règlement européen.
- L'exercice des droits par voie électronique si les données ont été collectées de cette façon (Article 12 du RGPD).

Pour résumer, la loi pour une République Numérique permet une transition progressive vers le RGPD. Néanmoins, on ne retrouve pas l'ensemble des points essentiels du RGPD comme, par exemple, la désignation des DPO, l'obligation de réaliser des études d'impacts, la notification en cas de violation de données, le respect des principes de privacy by design et d'accountability, etc.

Groupe de travail de l'article 29 (G29) :

Le groupe de travail de l'article 29 (ou G29) doit son nom aux circonstances de sa création. En effet, il a été créé en 1995 par l'article 29 de la directive 95/46/CE.

Actif depuis 1996, il consiste en un organe européen indépendant, chargé d'étudier et de donner un avis sur des questions ayant trait à la gestion des données personnelles. Les avis émis, sont de nature consultative. Cependant, le groupe étant constitué de membres des différentes autorités de contrôle nationales, du contrôleur européen de la protection des données et de la commission européenne, son opinion est réellement prise en compte.

Du fait de ses fonctions, le G29 participe activement au déploiement du RGPD. Il a adopté en décembre 2016, un plan d'action traitant de la mise en œuvre du RGPD. Les principales lignes directrices concernant les litiges transfrontaliers et l'adoption d'une autorité chef de file, le droit à la portabilité et le délégué à la protection des données personnelles ont été définies au sein du groupe.

Une mise à jour du plan d'action initié en 2016 a été publiée en janvier 2017. Les lignes directrices précédemment identifiées ont été précisées. De nouveaux axes de travail tels que la certification, les traitements de données présentant un risque élevé et les analyses d'impact sont venus compléter la liste des sujets en étude. La mise en œuvre de ce plan s'est traduite par l'organisation, par le G29, de plusieurs évènements impliquant différentes parties prenantes parmi lesquelles les entreprises et les autorités de contrôle européennes et hors Union Européenne (USA notamment). Elle s'est également traduite par une prise de position sur

plusieurs sujets dont le projet de règlement sur la ePrivacy et le règlement révisé sur le traitement de données personnelles réalisé par les Institutions Européennes.

Glossaire

Accountability : l'accountability (parfois traduit par les termes « auditabilité » ou « responsabilité »), 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.

AIPD : l'Analyse d'Impact relative à la Protection des Données, parfois appelée EIVP (Etude d'Impacts sur la Vie Privée) ou PIA en anglais (Privacy Impact Assessment), est un processus dont l'objet est de décrire le traitement, d'en évaluer la nécessité ainsi que la proportionnalité, et de gérer les risques associés en les évaluant (ex. impact sur la vie privée) et en déterminant les mesures nécessaires pour y faire face.

DCP : Donnée à Caractère Personnel (ou donnée personnelle), à savoir toute information identifiant directement ou indirectement une personne physique (ex. nom, numéro de téléphone, photographie, adresse, date de naissance, adresse IP, ...).

Donnée personnelle sensible : catégorie particulière de données personnelles regroupant des informations concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle.

DPD/DPO : Data Protection Officer (DPO) ou Délégué à la protection des données (DPD) est chargé de mettre en œuvre et de s'assurer de la conformité de l'organisation au RGPD.

G29 : Groupe de travail rassemblant les représentants de chaque autorité indépendante de protection des données nationales (réunit l'ensemble des CNIL européennes), et contribuant à l'élaboration des normes européennes ayant une incidence sur les droits et libertés des personnes physiques à l'égard des traitements de données personnelles.

Responsable de traitement : personne (physique ou morale), autorité publique, service ou organisme qui détermine les finalités et les moyens nécessaires relatifs à un traitement de données à caractère personnel (ex. directeur de l'entité où le traitement est mis en œuvre, et dont il porte la responsabilité).

Sous-traitant : personne (physique ou morale), l'autorité publique, service ou organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Traitement de données à caractère personnel : toute opération portant sur des données à caractère personnel, telle que la collecte, l'enregistrement, la conservation (stockage), la modification, l'extraction, la consultation, l'utilisation, la diffusion, l'effacement...

Transfert de données : toute communication, copie ou déplacement de données personnelles qui feront l'objet d'un traitement dans le pays destinataire. Des dispositions spécifiques sont prévues si le pays destinataire n'est pas un état de l'Union Européenne

Bibliographie

CIGREF. (2017). *Entreprises, les clés d'une application réussie du GDPR*. Récupéré sur http://www.cigref.fr/wp/wp-content/uploads/2017/11/CIGREF-GT-AFAI-CIGREF-TIF-Donnees-Personnelles-et-Systemes-d-Informations-GDPR-2017.pdf

CNIL. (s.d.). *Communiqué G29, Séance plénière du G29 du 12 et 13 décembre 2016*. Consulté le 12 14, 2017, sur https://www.cnil.fr/fr/communique-g29-seance-pleniere-du-g29-des-12-et-13-decembre-2016

CNIL. (2014). *Pack de conformité assurance.*

CNIL. (septembre 2017). *Guide du sous-traitant.*

G29. (2016). *Guidelines for identifying a controller or processor's lead supervisory authority.*

G29. (2017, janvier 16). Communiqué de presse mise à jour du plan d'action RGPD adopé en 2016. Bruxelles.

G29. (décembre 2016). *Guideline on the right to data portability.*

G29. (décembre 2016). *Guidelines on data protection officers (DPOs).*

G29. (novembre 2017). *Guidelines on consent.*

G29. (octobre 2017). *Guidelines on Personal data breach notification.*

G29. (avril 2017). *Guidelines on Data Protection Impact Assessment (DPIA).*

G29. (novembre 2017). *Guidelines on transparency.*

Traitement des données personnelles au travail, nouvel avis du groupe G29. (s.d.). Consulté le 12 14, 2017, sur https://www.gdprbelgium.be/fr/nouvelles/traitement-des-donn%C3%A9es-personnelles-au-travail-nouvel-avis-du-groupe-de-travail-%C2%ABarticle

Table des illustrations

Retrouvez les autres Publications

Cahiers Techniques
Collection Dialoguer
Collection Maîtrise des Risques

Librairie en ligne
www.amrae.fr/Publications

Prix de vente – exemplaire relié : 20 € TTC FRANCE

www.amrae.fr

Management des Risques et des Assurances de l'Entreprise
80 BOULEVARD HAUSSMANN 75008 PARIS - TEL : +33 (0)1 42 89 33 16 - FAX : +33 (0)1 42 89 33 14 - amrae@amrae.fr - www.amrae.fr