Cahiers Techniques 2018

Commission
Systèmes d'Information

Le règlement général sur la protection des données (RGPD)

La protection des données du citoyen européen par l'entreprise

En partenariat avec

CGI | Business Consulting

AMRAE L'ASSOCIATION

A propos de l'AMRAE

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

L'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) est née de la fusion, en 1993, de deux associations créées vingt ans plus tôt : l'ACADEF et le GACI. La rencontre de ces deux entités donne naissance aux Rencontres du Risk Management AMRAE.

Association professionnelle, organisme de formation continue, organisateur des Rencontres du Risk Management AMRAE : l'AMRAE se décline en 4 couleurs pour 4 activités majeures.

Objectifs

- développer, exposer, et faire évoluer les méthodologies de gestion des risques ;
- faire entendre la voix des entreprises sur le marché de l'assurance et des autres opérateurs du transfert de risques ;
- aider ses membres à acquérir ou à améliorer une expertise métier répondant aux standards nationaux et internationaux les plus exigeants ;
- former les professionnels de la gestion des risques avec AMRAE Formation ;
- diffuser la culture de la prise de risque d'entreprise.

A propos de CGI Business Consulting

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 quelque 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

En rendant, pour tout type d'organisation, quelle que soit sa nationalité, obligatoire au 25 mai 2018, la conformité au « Règlement Général sur la Protection des Données » (RGPD ou en anglais « General Data Protection Regulation », GDPR) de tout traitement de données à caractère personnel appartenant à des citoyens européens, un changement de premier ordre s'opère dans la **protection de la vie privée et surtout dans la protection de nos données personnelles !**

En effet, après la loi « Informatique et Liberté » de 1978 donnant, en France, naissance à la CNIL comme autorité administrative indépendante, et suite à différentes modifications et Directives, l'**Union européenne, via le RGPD, renforce considérablement les obligations de transparence sur la gestion des données personnelles**, tout en **uniformisant la législation** au sein de ses états membres.

Ce règlement répond à une nécessité **politique** – l'Union européenne protège les données de ses citoyens, notamment vis-à-vis des GAFAM -, **économique** - l'économie numérique nécessite la confiance des citoyens -, et **humaine** – l'Union européenne protège l'atteinte à la vie privée des personnes lors du traitement de leurs informations.

Les fuites d'informations personnelles font de nos jours la « une » de l'actualité quasiment chaque semaine. Le RGPD vise à prévenir ce **risque pour les citoyens.** En effet, après avoir bien souvent fourni lui-même ses informations personnelles, le citoyen voit ses données exploitées par des tiers, voire revendues à d'autres tiers, et il en perd alors 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 (droit à l'oubli par exemple), ni l'assurance d'un traitement maîtrisé lorsqu'il s'agit par exemple d'éviter pour une personne :

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

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

- des impacts sur leur image et leur réputation avec des conséquences potentielles graves comme une perte de confiance de 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 (lié 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, que ce soit en le coordonnant, ou plus simplement en en étant partie prenante en guidant alors le projet et la mise en conformité dans une approche par

les risques (afin d'éviter les impacts les plus importants, ne pas surinvestir vers une sur conformité inutile, ou encore, être en veille sur l'interprétation et la déclinaison du Règlement.). Dans certaines organisations il pourra même 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 RM 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 de gestion de crise « cyber ».

A l'approche de cette entrée en vigueur désormais très proche, 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, en apportant notamment un éclairage sur les questions suivantes :

- Comprendre ce qu'est le RGPD, comment est constitué le Règlement ?
- Quels sont les nouveaux droits introduits ?
- Qui 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
Administrateur AMRAE et président de la commission Systèmes d'Information

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 : Mouloud Aït-Kaci, Vincent Mallet, Thomas Nguyen, Marine Verbecke, Alexandra Zelmans, Erwan Bompard.

Ce cahier technique a été relu, corrigé et amélioré par : Sophie Mauvieux (Administrateur AMRAE et membre de son Comité Scientifique Permanent), François Beaume (Administrateur AMRAE et président de la commission Systèmes d'Information), Hélène Dubillot (Bureau Permanent de l'AMRAE, Directrice de la coordination scientifique) et Marie-Christine Vittet (Data risk Manager, membre de la commission Systèmes d'Information).

1. Le Règlement Général sur la Protection des Données

Le traité sur le fonctionnement de l'Union européenne définit, à l'article 288, qu'un règlement est un acte juridique contraignant pour ceux ou celles 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 états membres. Le Règlement Général sur la Protection des Données (RGPD) est entré en vigueur le 24 mai 2016 et sera applicable à partir du 25 mai 2018, à toute société, organisme public ou association effectuant des traitements liés à des **données de citoyens européens**, et ne se limite pas aux organisations européennes mais vise toutes celles qui collectent et manipulent les données de citoyens européens, présentes au sein **ou hors de l'Union européenne**. Son domaine d'application est extrêmement large, car il vise à la fois les données collectées par l'organisation à l'extérieur, auprès de clients ou prospects par exemple, ainsi que les **données internes de collaborateurs** dont elle dispose. 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 dans la lignée de la Loi Informatique et Liberté (LIL - promulguée en France en 1978 et révisée en 2004), des avis et ordonnance 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 » :

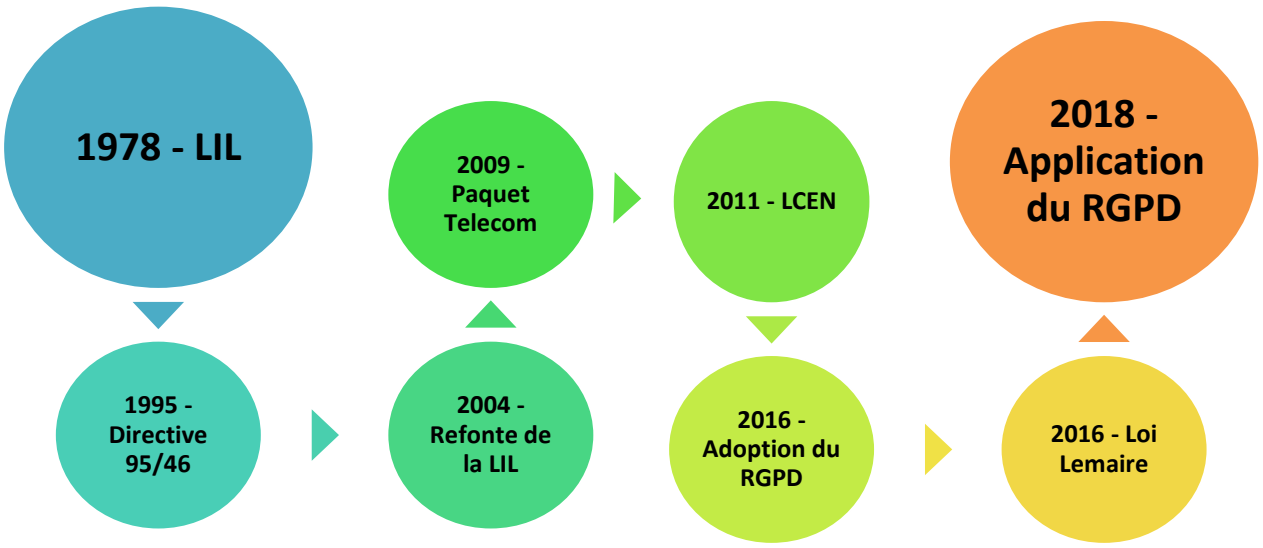


Figure 1 : Chronologie de l'évolution de la réglementation européenne et française

Le règlement laisse aux Etats membres une marge de manœuvre dans une cinquantaine de paramètres, pour lesquels chaque Etat peut légiférer de manière souveraine Au moment de l'élaboration du présent document, parmi les états membre de l'UE, seuls l'Autriche et l'Allemagne ont déjà adopté une législation nationale adaptée au RGPD, et ce dès Juillet 2017. Ces éléments sont attendus en France au travers d'une révision de la loi informatique et liberté, révision non encore pas publiée à cette même date.

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 lesquelles (cf. annexe pour plus de détail):

- Loi pour la Confiance dans l'Economie numérique (LCEN) – Texte Français
- Directive e-Privacy – Texte Européen
- 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 dans le cours 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 §5.10) ou le chiffrement.

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

A cet égard, le responsable de traitement des DCP (cf. Glossaire), c'est à dire celui qui détermine les finalités du traitement des DCP et la manière dont les traitements seront mis en œuvre (ex. personne morale, l'entreprise, ou bien physique telle que le directeur/responsable du service concerné), doit s'assurer que les mesures techniques et organisationnelles mises en œuvre sont appropriées et garantissent un niveau de sécurité adapté. Pour ce faire, il a souvent besoin de s'appuyer sur des compétences spécifiques (ex. direction des risques, direction sécurité, DSI), notamment pour mener l'analyse d'impact sur la vie privée et mettre en place les mesures nécessaires.

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

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. Celles-ci concernent les 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.

Le droit des personnes sur leurs données personnelles : es citoyens européens voient leurs droits s'élargir et les conditions d'utilisation de leurs données personnelles explicitées. Ces

nouveaux droits pour les personnes concernées décrits plus en détail dans le chapitre §2 du présent document, sont évoqués dans un grand nombre d'articles du Règlement parmi lesquels les articles 15, 16, 17, 18, 20, 21 et 22.

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

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

Data Protection Officer (DPO) : L'article 37 du RGPD, crée une nouvelle fonction au sein de l'entreprise, le Data Protection Officer (DPO), qui aura pour mission de veiller au respect de sa bonne application. 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 de DCP. Enfin, il a pour rôle de conseiller et de sensibiliser les différents acteurs de l'entreprise impliqués dans le traitement de données personnelles.

Cette nouvelle fonction peut être attribuée à différents acteurs au sein de l'entreprise. Ainsi certains Risk Managers sont parfois nommés DPO, de même que des collaborateurs issus d'autres fonctions (juridique, conformité, contrôle interne, SI…). Enfin le Correspondant Informatique et Libertés (CIL), lorsqu'il a été nommé au sein de l'organisation, voit parfois son rôle évoluer pour devenir DPO (même si cette évolution n'est pas systématique compte tenu de l'évolution de l'enjeu).

Privacy by design & by default : Le règlement, en son 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 :

- la protection de la sphère privée (dès la conception),
- la pseudonymisation des données (dès que possible),
- la limitation au minimum des informations nécessaires (ne pas prendre des informations qui ne serait pas vraiment « utiles » au traitement) lors de la collecte de données,
- 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 : Le responsable de traitement doit effectuer une analyse d'impact sur les traitements de données personnelles potentiellement à risque.

Cette notion de Private Impact Assessment (PIA ou APID en français, Analyse d'Impact relative à la Protection des Données) 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 et savoir démontrer la conformité au Règlement.

Obligations des responsables de traitement de DCP et de leurs sous-traitants :

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. §5) et de protection des droits des personnes (cf. §2).

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

Selon la Loi Informatique et Liberté, la charge de la preuve incombait à la personne concernée ou à l'autorité compétente (ex. CNIL) qui devait démontrer la non-conformité d'une organisation lors d'un traitement de données à caractère personnel. Or, le RGPD renvoie désormais cette responsabilité vers l'organisation qui doit démontrer que ses traitements sont conformes au règlement. Ainsi, l'article 5 modifie profondément les modalités de génération de la preuve.

L'entreprise devra, désormais, être en mesure de **prouver qu'elle a mis en œuvre toutes les mesures nécessaires** à la protection des données personnelles qu'elle avait en sa possession (cf. principe de responsabilité/accountability §3.1).

Licéité et consentement : L'exigence de licéité est introduite à l'article 5 du Règlement. D'après le premier paragraphe du présent 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. Le respect d'une seule 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. 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.

Et, à défaut du recueil formel du consentement :

- **L'exécution d'un contrat** (Art. 6, paragraphe 1, point B) : 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.

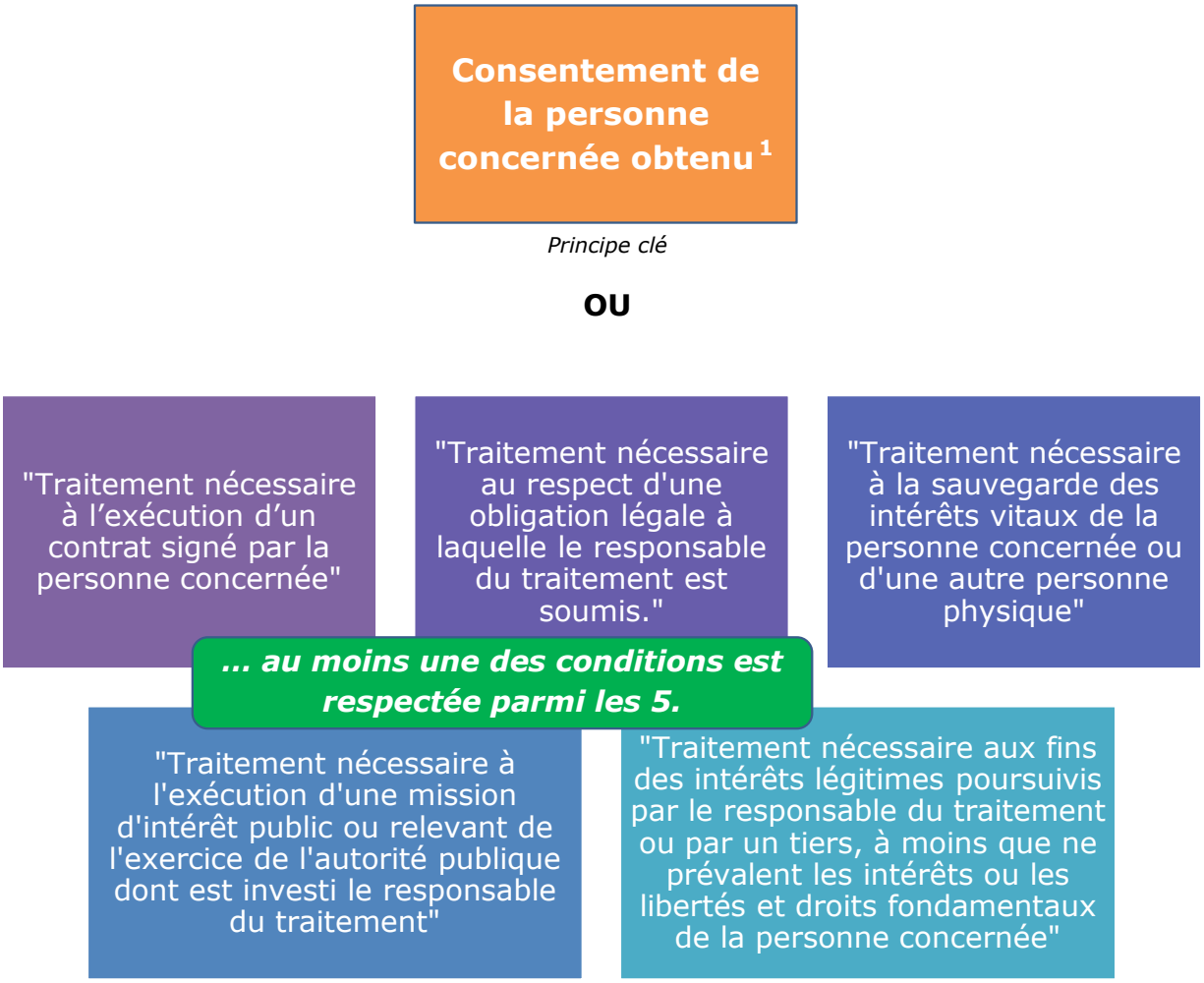
- **L'obligation légale** (Art. 6, paragraphe 1, point C) : Le traitement est considéré comme licite s'il est effectué conformément à une obligation légale à laquelle le responsable de traitement est soumis.
  Ex : traitement des données relatives aux rémunérations de leurs salariés par les employeurs pour pouvoir les communiquer à la sécurité sociale ou à l'administration fiscale.

- **La sauvegarde des intérêts vitaux** (Art. 6, paragraphe 1, point D) : 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 à des fins humanitaires.

- **L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique** (Art. 6, paragraphe 1, point E) : 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, paragraphe 1, point F)) : 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.
  Ex : traitement de données à des fins de prévention contre la fraude.

Le traitement est considéré comme licite si le consentement est obtenu ou, à défaut, si au moins une des cinq autres conditions est respectée :



[1]La notion de consentement est définie à l'Article 4 paragraphe 11 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 ».

L'autorité de contrôle d'un état membre veille au respect du règlement européen par les organisations présentes sur son territoire mais aussi celles qui traitent des données personnelles de ses citoyens 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, etc.

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

Le Règlement ne prévoit pas la création d'une autorité de contrôle supranationale. Néanmoins, certains traitements sont transfrontaliers. Un traitement transfrontalier se caractérise par un traitement de données dans plusieurs pays membres de l'UE ou par un traitement de données de citoyens de 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.

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 Liberté* (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. §2.3 à §2.8 du présent cahier technique), **quatre sont nouveaux ou sensiblement modifiés** :

1. Le droit à l'effacement (« droit à l'oubli ») - Art. 17,
2. Le droit à la limitation du traitement - Art. 18,
3. Le droit à la portabilité des données - Art. 20,
4. Le droit d'opposition (y compris le droit de refuser de faire l'objet d'une décision entièrement automatisée) - Art. 21 et 22.

Les droits d'accès et de rectification sont, par ailleurs, réaffirmés dans le Règlement (Art. 15 & 16).

2.2 Quelles sont les personnes concernées par ces droits ?

Pour ce qui est de l'exercice des droits, le RGPD ne fait pas de distinction entre les personnes, il s'applique donc à tous les citoyens européens.

Cependant, les restrictions dans les possibilités d'user du droit peuvent exclure, *de facto,* certaines catégories de personnes (ex : les employés).

2.3 Droit d'accès (Art. 15)

Présentation

L'article 15 du RGPD réaffirme, pour une personne, le droit d'accès à ses DCP, déjà présent dans la *Loi Informatique et Liberté* 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 (Article 15) à tout moment : quelles sont les **finalités** des traitements dont leurs données font l'objet, les **catégories** de données utilisées, les **destinataires** (i. e. à qui sont communiquées les DCP), la **durée** de conservation prévue pour ces données, l'existence éventuelle de **profilage**.

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

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 (Article 40), mais apporte peu de nouveauté par rapport à celle-ci. Cependant, la directive 2016/680 précise certains aspects : ce droit peut 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 Liberté, 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, et étant :

- inexactes,
- incomplètes,

- équivoques,
- 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 est légitime et nécessaire à des fins d'archivage dans l'intérêt général. Par exemple, à des fins scientifiques, statistiques et historiques, 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.

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…

En pratique, il est difficile de garantir l'effacement total des données dans la mesure où celles-ci sont bien souvent rapidement copiées, transférées, stockées sous plusieurs formes (Cloud, sauvegardes, bases de données non structurées, etc.).

Néanmoins, le régulateur a prévu une obligation pour le responsable du traitement de mettre en œuvre des « moyens raisonnables » (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 Liberté et prévoit la limitation temporaire des traitements dans quatre cas très spécifiques :

1. lorsque la personne concernée **conteste l'exactitude** d'une donnée, le temps que le responsable du traitement puisse contrôler cette exactitude.
2. si le traitement est **illicite** et que la personne concernée s'oppose à l'effacement (ex. constituant un élément de preuve dans le cadre d'une action en justice).

3. lorsqu'il **n'est plus nécessaire** 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.
4. 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. ou 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 demandes).

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

Présentation

Ce droit prévoit qu'une personne peut demander à un responsable de traitement de lui fournir toutes les données la concernant dans le but de les fournir à un autre responsable de traitement.
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* ».
Ce droit ne s'applique qu'aux données que la personne a elle-même fourni au responsable de traitement, dans le cadre d'un consentement ou d'un contrat, et dont le traitement se fait par des procédés automatisés.

La CNIL précise que les données considérées comme « fournies par la personne concernée » sont :

1. « 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), » ;
2. « 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.). »

La CNIL exclut « les données personnelles dérivées, calculées ou inférées », considérant que ces données sont créées par l'organisme.

Quelles sont les personnes concernées ?

La CNIL précise que les établissements financiers n'ont pas à répondre à une demande de portabilité concernant les données personnelles traitées dans le cadre de leurs obligations de lutte contre le blanchiment.

De même, les données des employés traitées par les employeurs, sur la base d'un intérêt légitime ou d'obligations légales, ne sont pas concernées par le droit à la portabilité.

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 générées par la suite par l'organisme, des données issues de profilages par exemple ou des données potentiellement sensibles.

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, etc.).

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

Présentation

Ce droit est présenté dans deux articles distincts : Article 21 relatif au droit d'opposition et 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 (article 38). Sur ce point, le droit français est plus contraignant que le nouveau Règlement. Ainsi

il est possible d'exercer son droit d'opposition pour des traitements effectués, par exemple, à des fins de prospection.
Dans le cas où le traitement est licite et nécessaire pour une mission d'intérêt public 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. Le traitement devrait alors exclure les personnes ayant fait cette demande.

Le régulateur précise également que la personne peut également retirer le consentement donné initialement à tout moment, obligeant le responsable à arrêter son traitement.

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 à toute autre communication.

Généralement, ce droit se traduit par une case à cocher par la personne physique qui déclare ainsi refuser le traitement de ses données à des fins commerciales ou de profilage.

Un consentement doit pouvoir être retiré à tout moment. 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 d'opposition.

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 : *« 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 responsable de la conformité aux six points du paragraphe 1 de l'Article 5 du RGPD qui sont :

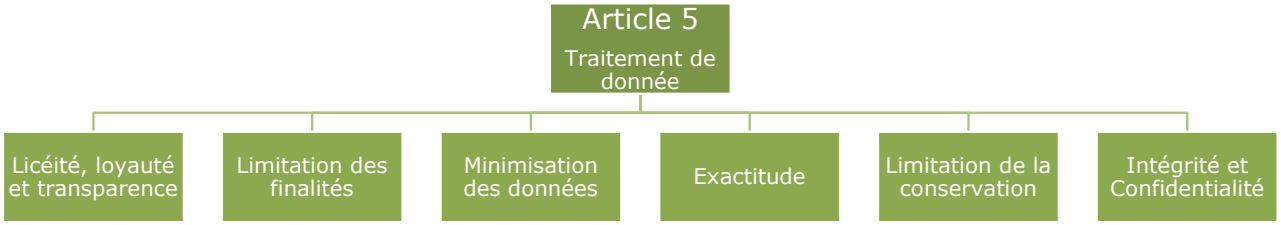


Figure 6 : Six points clés à respecter pour le responsable de traitement (Accountability)

Le responsable de traitement doit pouvoir assurer et être en capacité de démontrer la conformité à l'ensemble du RGPD.

En effet, en inversant la charge de la preuve, c'est-à-dire en demandant aux entreprises ou organismes de **se porter garantes,** et d'**être en capacité de démontrer le respect de la vie privée** plutôt que d'effectuer **une déclaration** à l'autorité de contrôle (CNIL), 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 et 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, évaluation d'impact sur la vie privée, transferts de données hors UE ;
- L'information relative aux personnes :
  Mentions d'information, recueil des consentements, exercice des droits,
- Les contrats avec les sous-traitants :
  Obligations, matrice des responsabilités ;
- Les procédures internes et les preuves associées.

Avec ce processus d'auditabilité, le RGPD (Articles 40, 41, 42 et 43) encourage l'élaboration de codes de conduite et de certification 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 ont droit à un recours contre un responsable du traitement ou un de ses sous-traitants. Le RGPD définit que le

responsable du traitement, ou son sous-traitant, peut être une personne morale ou physique. Des règles spécifiques de désignation pour le responsable du traitement peuvent être prévues par le droit de l'Union ou des états membres.

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. Ces 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 examine en début d'année 2018 un projet de loi adaptant le droit français au RGPD, autorisant au travers d'un amendement les actions de groupes (« class action »).

Le responsable du traitement est responsable du dommage causé par le traitement. Son sous-traitant quant à lui, ne peut être responsable que pour les obligations prévues dans le Règlement et spécifiques aux sous-traitants.

Le Règlement prévoit, à l'Article 58, paragraphe 2 points a) à h), un premier volet de mesures « correctrices » à la disposition de chaque autorité de contrôle nationale. 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 en fonction des violations des obligations. Cet article laisse aussi aux états 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.

En effet, le Projet de loi relatif à la protection des données personnelles (JUSC1732261L) français 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. Le retrait 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. »

Ce projet de loi va être amené à changer jusqu'à son adoption définitive, mais le texte actuel renforce l'arsenal dissuasif. Les organisations doivent s'assurer qu'elles sont en mesure de répondre aux demandes dans des délais raisonnables.

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

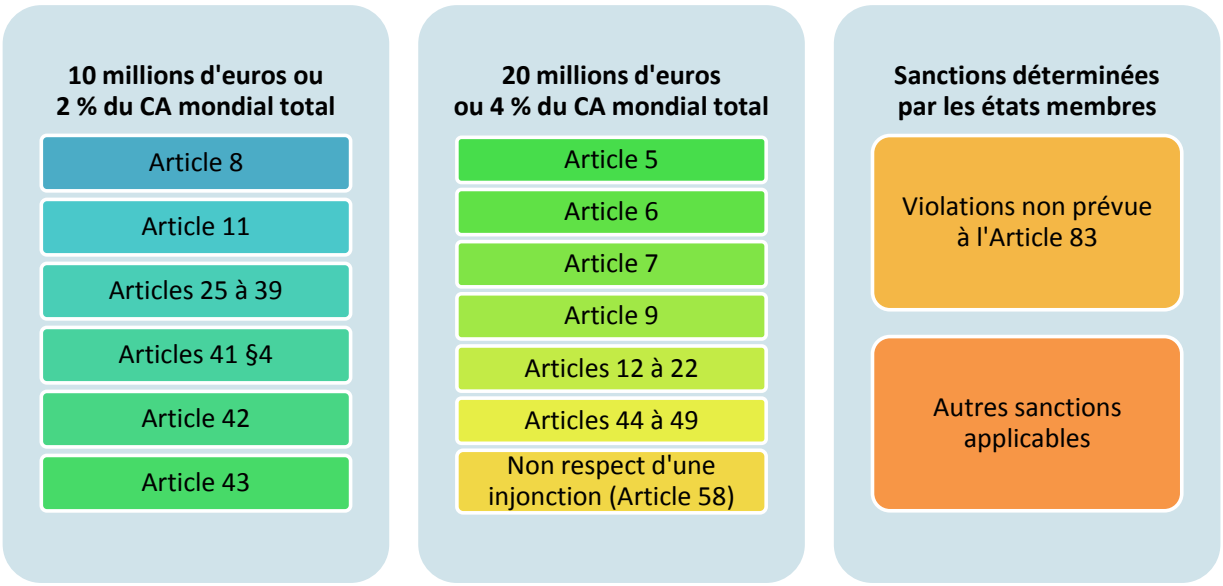


Figure 7 : Tableau de synthèse concernant les amendes administratives en cas de non-respect du RGPD

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

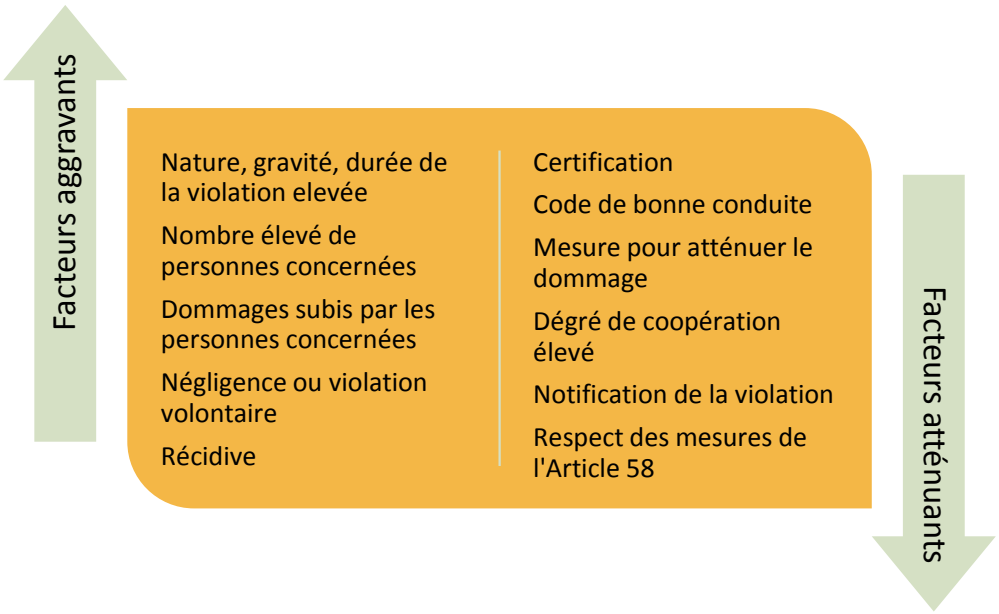


Figure 8 : Amendes : les facteurs atténuants et aggravants

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, selon leurs interprétations, certains assureurs proposant un produit d'assurance « Cyber » pourront garantir ce type d'amende, d'autres non.

3.3 Risques pour l'organisation

Tous les types d'organisations sont visés (associations inclues), y compris celles localisées en dehors de l'Union européenne dès lors qu'elles traitent des données personnelles de citoyens européens.

Afin de comprendre les risques pour l'organisation, il faut comprendre que la motivation du régulateur est de protéger les informations personnelles des citoyens 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 ses DCP en termes de disponibilité, intégrité ou confidentialité est source de risques pour la personne physique elle-même. De nombreux exemples récents illustrent cette tendance :

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

Figure 5 Exemples d'impacts sur les citoyens d'une défaillance de protection de leurs données personnelles

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

Et 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

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 6 : 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 concerné), les fonctions nécessaires à la mise en place du RGPD au sein de l'organisation, telles que le responsable de traitement, le sous-traitant, le DPO (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 DPO

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

Cette fonction s'inscrit dans la continuité de la démarche initiée par les juridictions nationales, notamment la juridiction française avec le « correspondant informatique et libertés » (CIL) instauré par la loi Informatique et Liberté de 1978. Si les deux fonctions peuvent paraître proches de prime abord, le DPO à, dans les faits, un rôle plus important au sein de l'entreprise. Le Risk Manager peut, par exemple, être nommé DPO par l'organisation, comme toute autre personne de l'organisation disposant du profil adéquat (CIL, responsable juridique ou conformité, DSI, RSSI, etc.). Les compétences requises et les missions qu'exerce le DPO sont explicitées au fil du présent cahier technique.

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

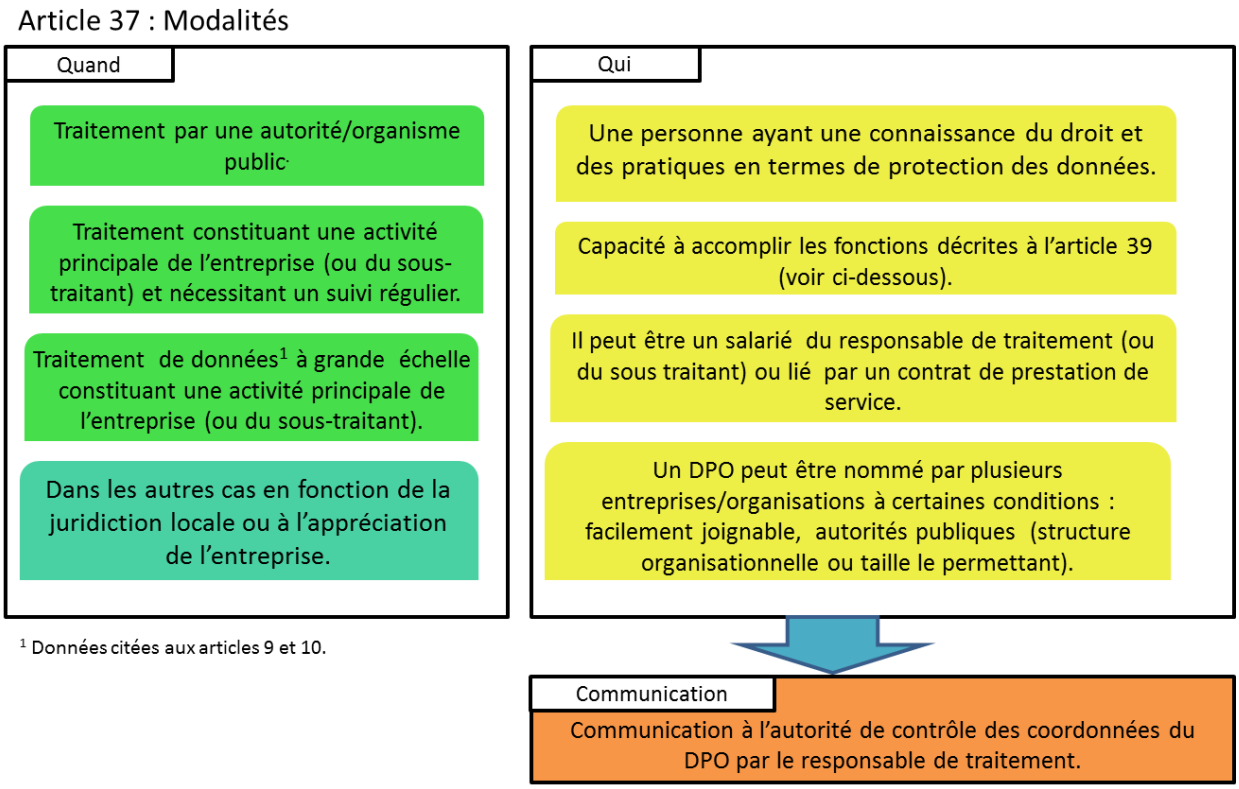


Figure 7 : Modalités de désignation du Data Privacy Officer (DPO)

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 :

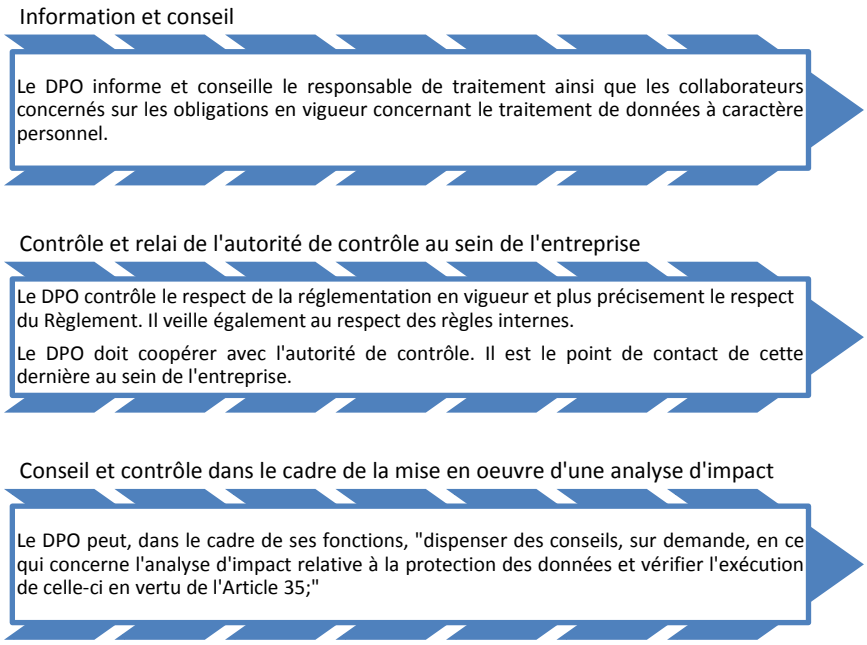


Figure 8 : Missions du Data Privacy Officer

L’Article 38 définit les obligations auxquelles l’organisation doit se conformer. Ainsi celle-ci, c’est-à-dire le responsable des données ou le sous-traitant, doit impliquer le DPO 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 DPO de réaliser ses missions. Ainsi, le DPO 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 liberté d’action.

4.2 Direction 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, du programme de mise en conformité au RGPD.

Mise en conformité au RGPD

Dans ce cadre, elle contribue notamment à l'évaluation du niveau de conformité aux nouveaux droits et au renforcement des droits existants des personnes concernées (accès, mise à jour, portabilité…) ainsi qu'à l'identification des traitements devant être mis à jour et des modifications à apporter pour assurer la conformité au RGPD. En tant qu'entité responsable de la conformité des accords/contrats avec les sous-traitants, elle participe 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 que cette dernière prenne en compte l'ensemble de la réglementation du RGPD dans ses activités ainsi que dans celle des responsables opérationnels et sous-traitants.

Dans ce cadre, elle veille à la conformité de ces 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

Une attention est également à porter lors de la **négociation du contrat avec le sous-traitant**, étape durant laquelle, la direction juridique ou les correspondants juridiques locaux doivent 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* » (Article 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* » (Article 28, paragraphe 3 RGPD).

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

traitement en question. En d'autres termes, pour le traitement concerné, le sous-traitant et le responsable de traitement seront co-responsables.

Notons par ailleurs que le sous-traitant doit tenir un registre des traitements qu'il effectue pour le compte du responsable de traitement (Article30, paragraphe 2).

Transfert de données hors de l'Union Européenne

Le service juridique doit également anticiper, dans la rédaction des contrats cadres ou autres, les conditions de transfert 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 hors de l'union européenne et de garantir au citoyen une protection adéquate de ces 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 et 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, etc.

En l'absence de Data Protection Officer (DPO) 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, 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, lors de la rédaction des contrats, et plus particulièrement des conditions générales de vente ou des conditions générales d'utilisation afin de s'assurer de la prise en compte du RGPD. Au regard du principe de transparence des informations et des communications de 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, paragraphe 1 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 de ventes. Six conditions, servant de bases légales, ont été 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 (métier) pour toutes les questions relatives à la réglementation relative à la protection des données.

Pour cela, elle est en charge de la rédaction de guides de bonnes pratiques en matière de protection des données et notamment du code de conduite, si il en existe un.

Le code de conduite, défini à l'Article 40 du RGPD, est destiné à contribuer, au sein de l'organisation, à la bonne application du RGPD, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des organisations (Art 40, paragraphe 1 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, paragraphe 2 RGPD).

Une fois élaboré par l'entreprise, le code de conduite est soumis à l'autorité de contrôle du pays concerné qui émet un avis sur la question de savoir si le projet de code respecte le RGPD. Cette dernière approuve alors le projet de code *« si elle estime qu'il offre des garanties appropriées suffisantes* » (Art. 40, paragraphe 5 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, paragraphe 3 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, paragraphe 5 RGPD).

D'autre part, en ce qui concerne le transfert de données à caractère personnel hors 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, paragraphe 2, point e) RGPD).

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

Enfin, le rôle de la direction juridique ne doit pas apparaître comme une contrainte pour les opérationnels. Celle-ci 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.

Elle 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 lors de l'élaboration de ces produits et/ou services.

4.3 Direction des Systèmes d'Information

La Direction des Systèmes d'Information joue un rôle important dans la mise en conformité. Ce rôle est souvent un rôle d'accompagnement des métiers et de maîtrise d'œuvre des mesures à appliquer, décidées par les directions métiers en accord avec le pilote du projet.

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), des outils de gestion des registres (Art. 30), de la gestion des notifications/communication en cas de violation des données (Art. 33 & 34), de l'assistance à fournir aux responsables de traitement dans les analyses de risques au sein des PIA ou AIDP (Art. 35), et bien sûr la sécurisation de systèmes d'information (Art. 32).

Implémentation technique des droits

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

La DSI doit accompagner les métiers et la direction juridique pour formaliser les spécifications de ces outils, s'assurer que les demandes d'accès, rectifications, etc. sont bien honorées et s'assurer que les demandes d'opposition, limitation ou suppression sont bien répercutées dans tout le SI, et auprès de tous les sous-traitants.

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 d'information).

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 gestion de crise, mais qui nécessite des moyens techniques, humains et financiers pour pouvoir répondre aux demandes de l'autorité et leur fournir toutes les informations demandées. L'ENISA (cf. Glossaire) a mis à disposition un outil de notification mais des éditeurs de logiciel proposent également déjà des solutions.

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

Selon les organisations, les Analyses d'Impact relatives à la Protection des Données peuvent être confiées à d'autres directions (DPO, 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 le SI à l'approche de la date butoir du 25 mai 2018. Puis, pour maintenir cette conformité dans le temps.

4.4 Directions des Risques

La Direction des Risques, et en particulier le Risk Manager, est également très concerné 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. risques pour l'organisation §3.3 du présent cahier technique).

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. DPO, 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.

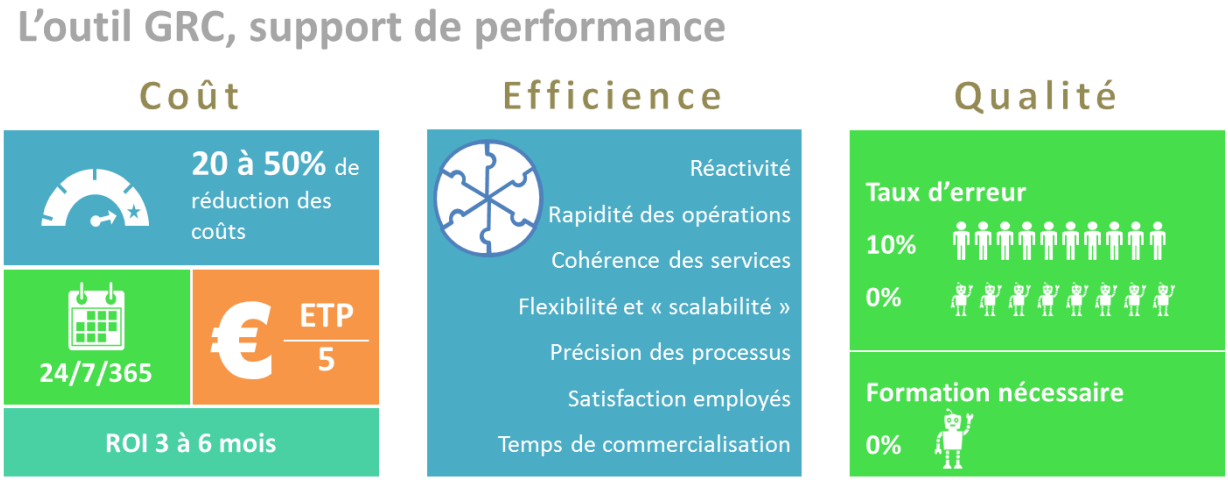
4.5 Les directions du Contrôle interne, RH et autres directions

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 preuves, 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 à 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.



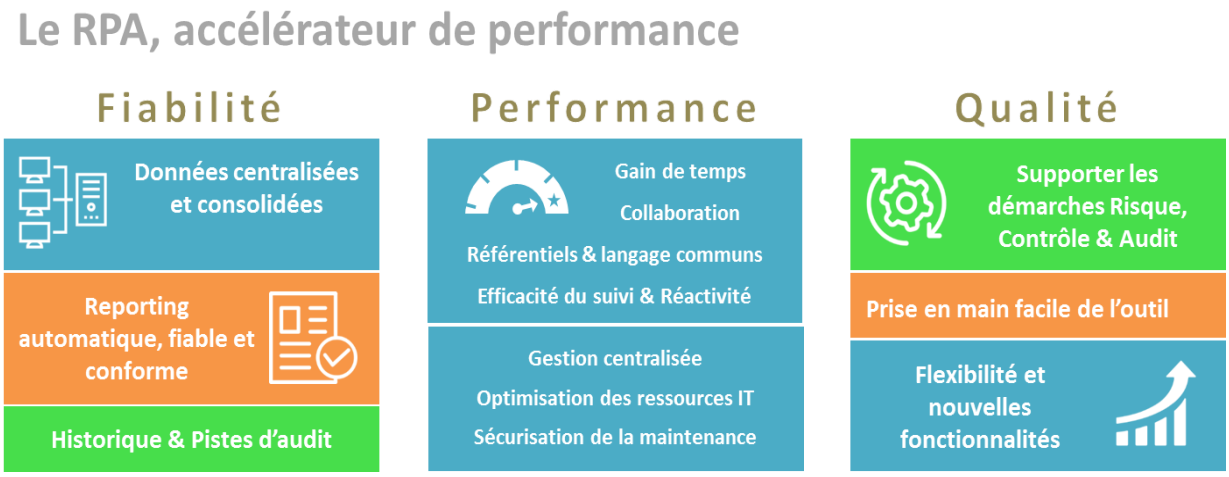


Figure 10 : GRC et RPA, des outils utiles dans le cadre du RGPD

La Direction des Ressources Humaines

Un sondage européen de SD Worx[1] du 28 novembre 2017 montre que 44% des collaborateurs des équipes de Ressources Humaines ne savent pas ce qu'est le RGPD.

Cependant, c'est paradoxalement cette même fonction qui est en première ligne pour recruter les futurs DPO, 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, elle doit être intégrée aux processus de tenu 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 de 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 [2].

Pourtant, ces mêmes directions génèrent régulièrement de **nouveaux traitements**, et à ce titre elles **peuvent être désignées comme responsables de traitement** : offre promotionnelle, registre des fournisseurs, contrôle anti-fraude, etc., autant de traitements qui nécessitent d'être connus et compris du DPO.

Ces directions doivent à minima être mises à contribution à deux niveaux : lors de la conception (« *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 Système 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.

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.

[1] 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

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

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


DSI


DPO


Dir. des Risques


Autres directions

*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 DPO ; 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 « Baromètre du RM », AMRAE), 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, informer les personnes concernées, notifier l'autorité du pays d'origine des personnes concernées, etc. ;
- Relation avec les autorités : en France, on pense avant tout à la relation avec la CNIL ;
- Intégrer dans la cartographie globale des risques, 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 en plus 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, etc. ;
- Mise sous contrôle de la conformité au RGPD : contrôle interne, gestion de la preuve.

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 :

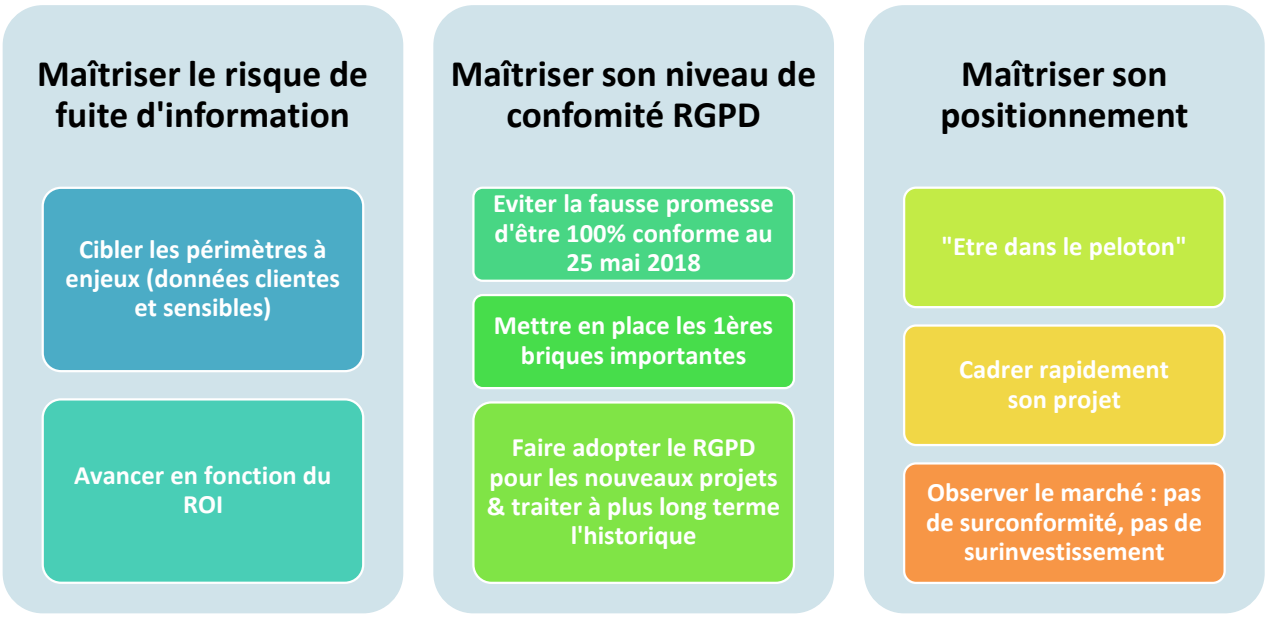


Figure 9 : Un projet de mise en conformité basé sur trois piliers

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, 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, etc.

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 :

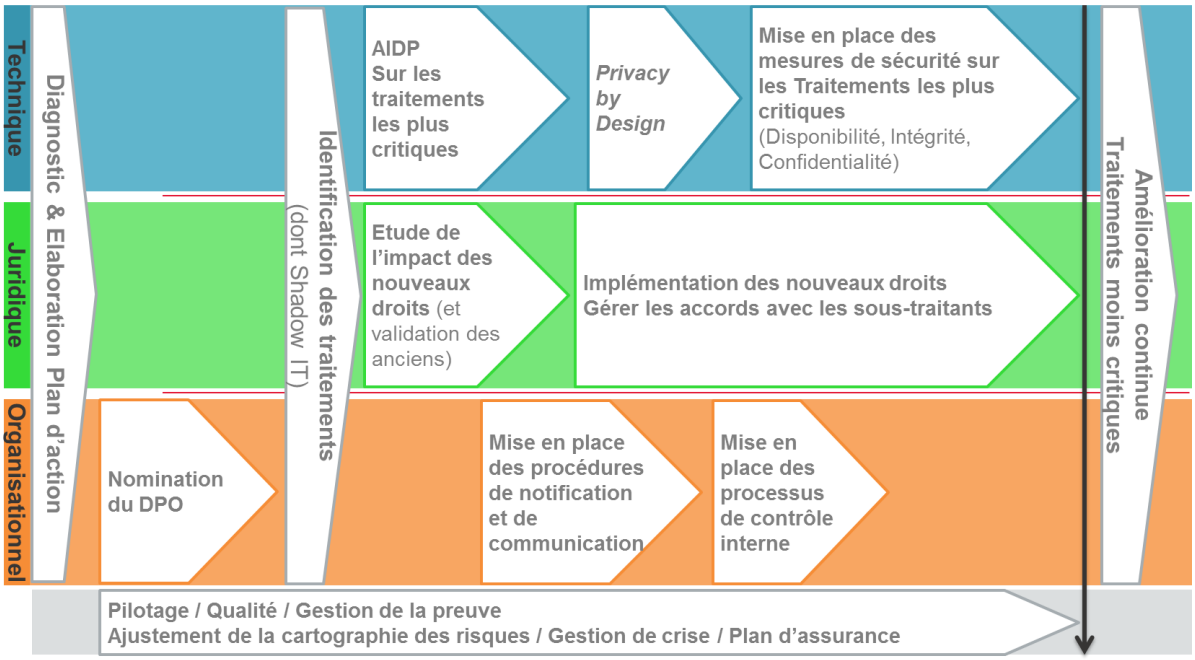


Figure 10 : Exemple de planning de mise en conformité d'une organisation

5.2 La nomination du DPO

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

5.3 Le registre et l'identification des traitements

Le Règlement Européen pour la Protection des données propose la tenue de deux registres et d'une information documentée :

- Le registre des traitements ;
- Le registre des sous-traitants ;
- 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, stipule 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 des moyens mis en œuvre par les organisations pour : favoriser l'exercice des droits, sécuriser les données, etc.

A titre d'illustration un fac-similé du registre des traitements proposé 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 11 : Registre proposé par la CNIL [3]

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 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.

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

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 ayant des droit 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 12 : 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 maitrise 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 intuitifsMise 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 aval	+ 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 13 : 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 :

1. le nom et les coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit […] ;
2. les catégories de traitements effectués pour le compte de chaque responsable du traitement ;
3. 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 […] ;
4. dans la mesure du possible, une description générale des mesures de sécurité techniques […].

Les violations de données à caractère personnel

L'Article 33, paragraphe 5, du Règlement postule que chaque responsable de traitement doit documenter toutes les violations de données à caractère personnel dont il fait l'objet.

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.

5.4 La notification 

Les conditions de notification dans le cadre d'une violation des données personnelles sont spécifiées au sein de l'Article 33 en ce qui concerne la notification à l'autorité de contrôle et à l'Article 34 en ce qui concerne la notification aux personnes concernées.

Contenu de la notification :

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

a) ***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 ;*

b) ***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 ;*

c) ***Décrire les conséquences probables*** *de la violation de données à caractère personnel ;*

d) ***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 :

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* » (Article 33, 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 notification aux personnes concernées :

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

La notification de la violation de données personnelles est obligatoire lorsqu'elle « *est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique ».* La déclaration doit alors être réalisée 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.

Le Règlement précise un certain nombre d'exceptions concernant la notification dans le cadre d'une violation pouvant impliquer un risque élevé. Ces exceptions visent à protéger l'entreprise. Elles concernent les cas où :

- *« Le responsable a mis en œuvre les mesures de protections techniques et organisationnelles appropriées et que ces dernières ont été appliquées aux données affectées par ladite violation, en particulier celles qui rendent les données incompréhensibles à toute personne non autorisée, telles que le chiffrement ;*
- *Le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé au regard des droits et des libertés des personnes concernées n'est plus susceptible de se matérialiser ;*
- *Une notification risque d'entraîner des efforts disproportionnés. Dans ce cas, il convient plutôt de procéder à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace ».*

5.5 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 :

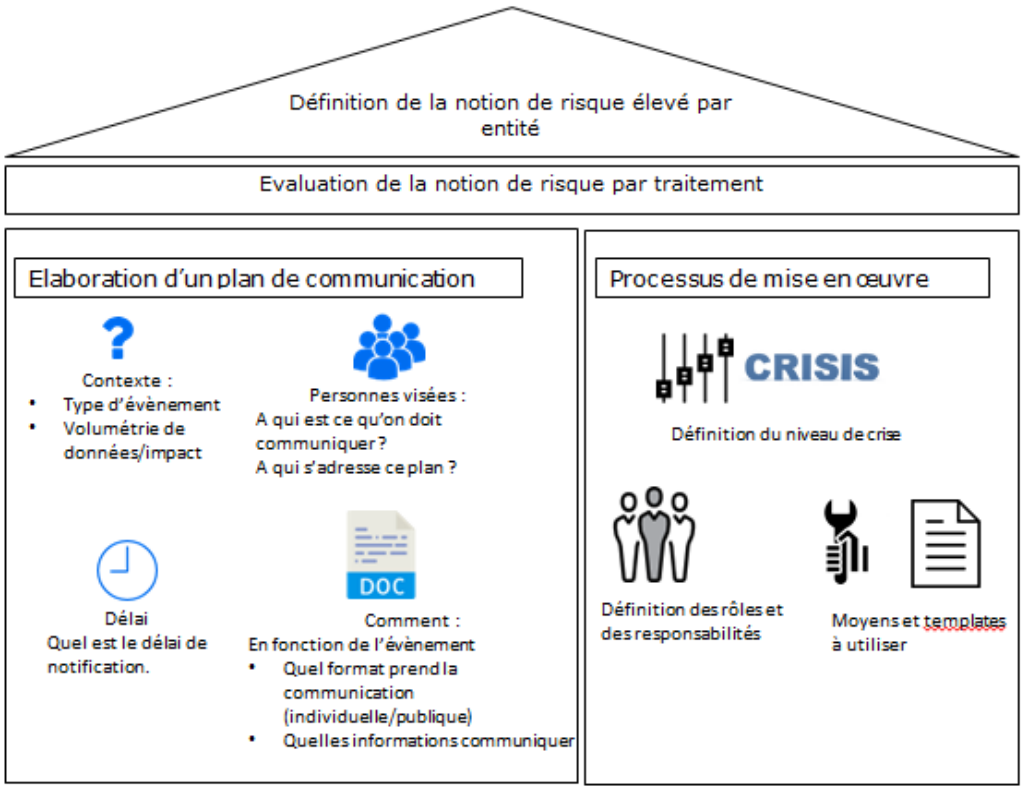


Figure 14 : Actions à mener afin de mettre en place une communication efficiente dans une entité (exemple donné), un service, une organisation.

5.6 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 du présent Cahier Technique.

5.7 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, car ils deviennent alors responsables de traitement. 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. §4.2 du présent document pour plus de détails sur le contrat sous-traitant).

5.8 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 pertinentes ;
- 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, proportionnalité, et de transparence.

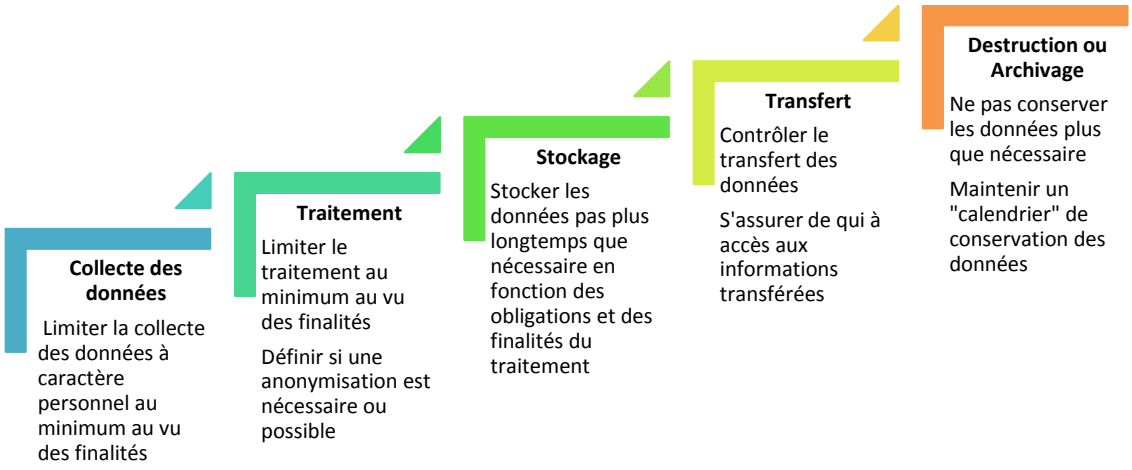


Figure 15 : Mise en œuvre d'une démarche de Privacy by design

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 un mapping ?
- 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 ?

5.8.1 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 maitrisant 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.

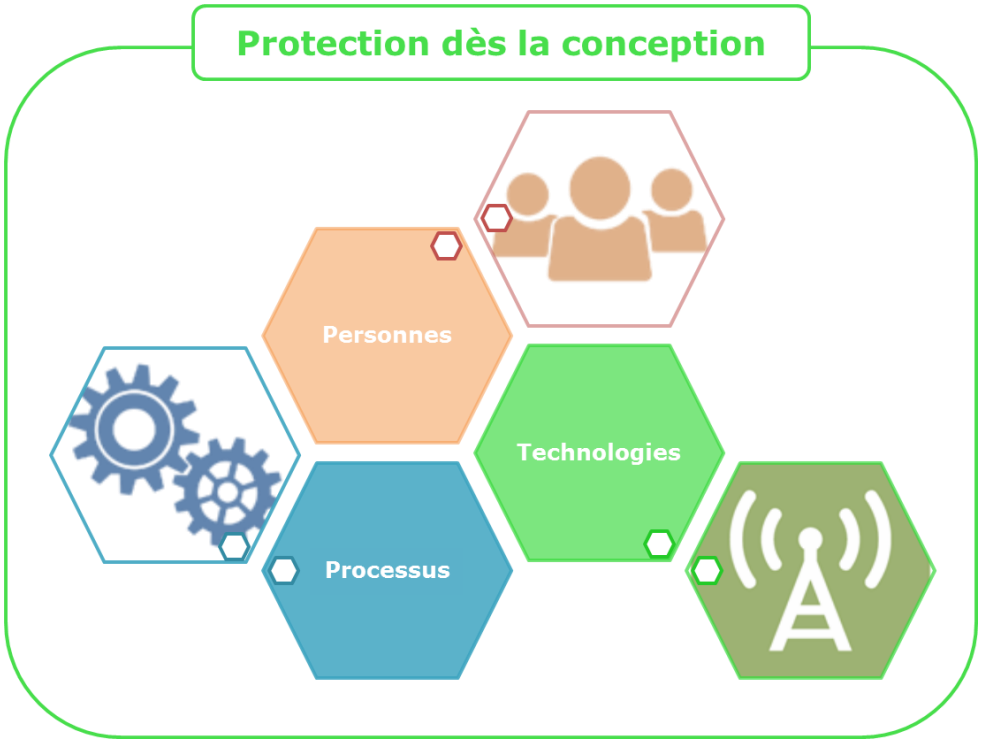


Figure 16 : Mise en œuvre d'une démarche de protection dès la conception

Cette première phase de planification se base sur une **évaluation de l'existant** sur ces trois axes : personnes, technologies et processus, 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 (DPO) ;
- Directions métiers ;
- Direction juridique ;
- 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.

5.8.2 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 scenario 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 scenario avec impact moyen ou mobilisation moyenne de ressources qui « mimera » un projet classique ;
- un scenario 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.

5.9 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 déclaration préalable (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 :

1. 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 ;
2. 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
3. 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.

Annexe 2 — Critères d'acceptabilité d'une AIPD [4]

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 échéant (Article 35, paragraphe 9).

[4] 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

Comment réaliser une AIPD ?

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

- Guides de la CNIL : 3 guides sur la méthode, l'outillage et les bonnes pratiques ;
- 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 » - WP48 – 4 avril 2017 ;
- EBIOS, Expression des besoins et identification des objectifs de sécurité ;
- Méthodologies issues des critères établis dans l'ISO 31000, Management du risque – Principe et ligne 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 en son paragraphe 7 mentionne que l'analyse doit au moins comporter :

a) *« 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 ;*
b) *une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;*
c) *une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1 ; et*
d) *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 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 :

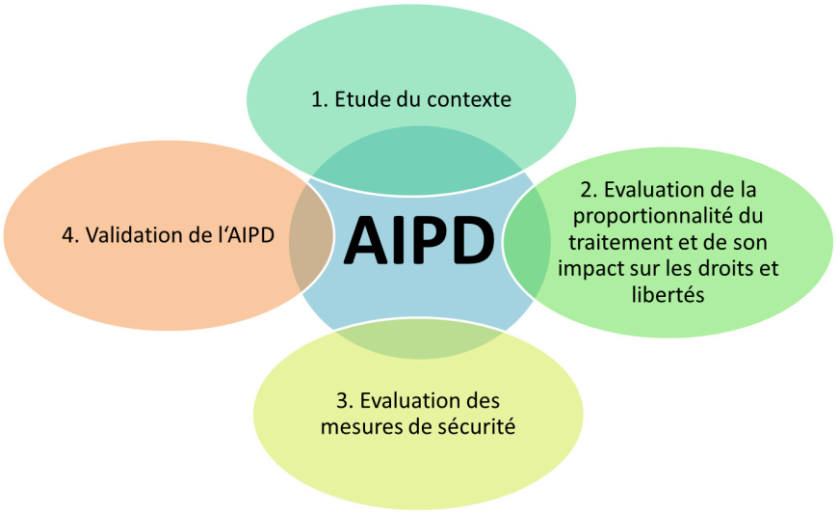


Figure 17 : Exemple de plan d'Analyse d'Impact relative à la Protection des Données

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 risque 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 ?

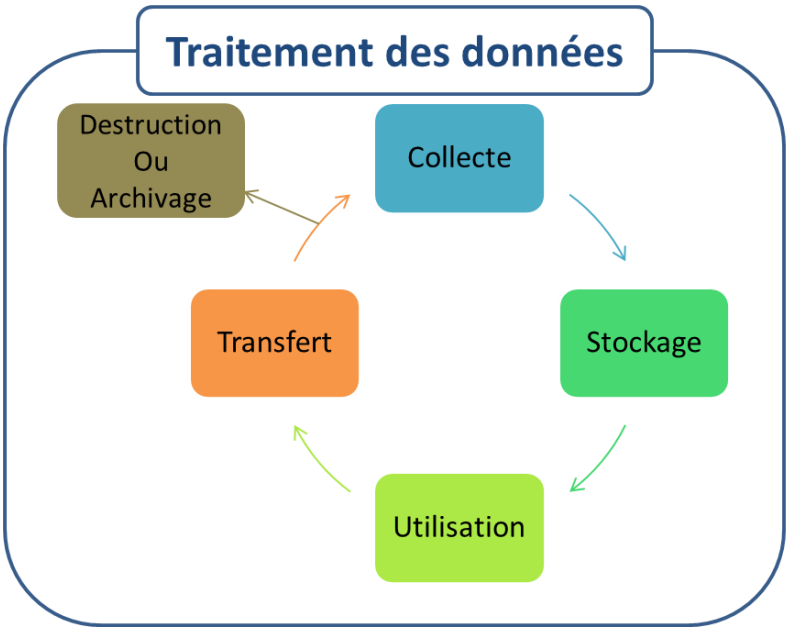


Figure 18 : Processus de traitement des données

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 œuvres.

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.

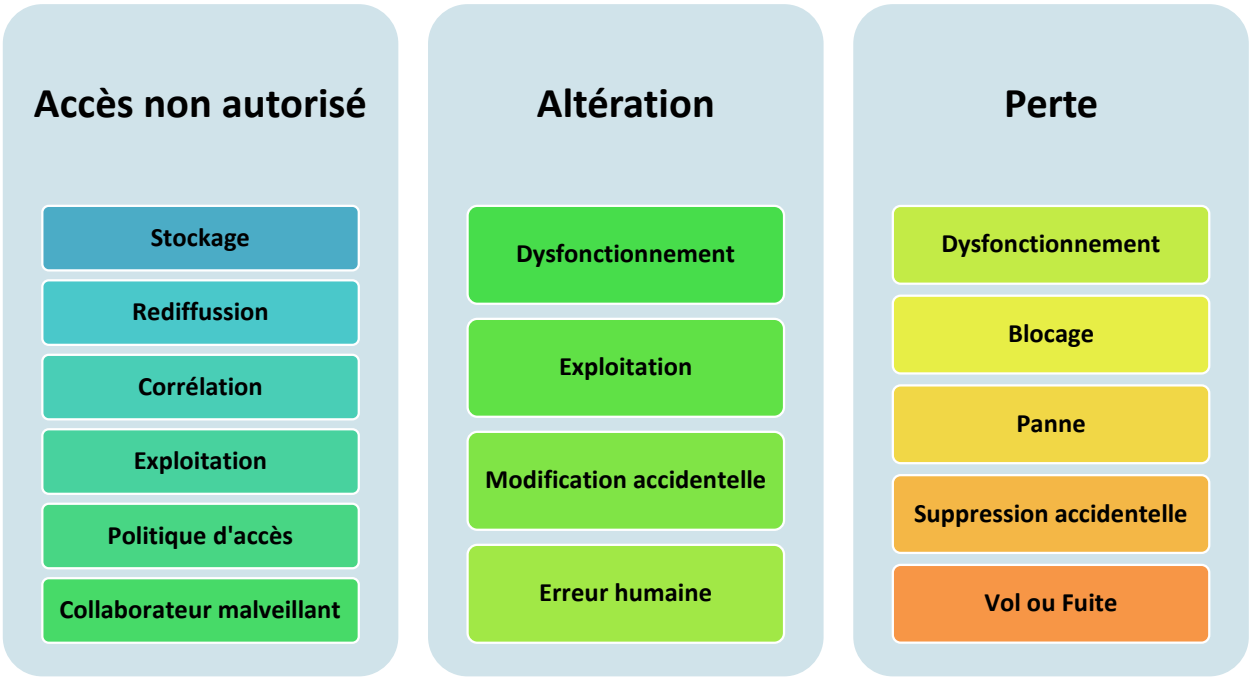


Figure 19 : Exemples de risques de sécurité des systèmes d'information/des données

L'évaluation des mesures de sécurité (Partie 2 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	Mesures	Gravité résiduelle	Vraisemblance résiduelle
1.	2.	3.	Note	Note	5.	Note	Note

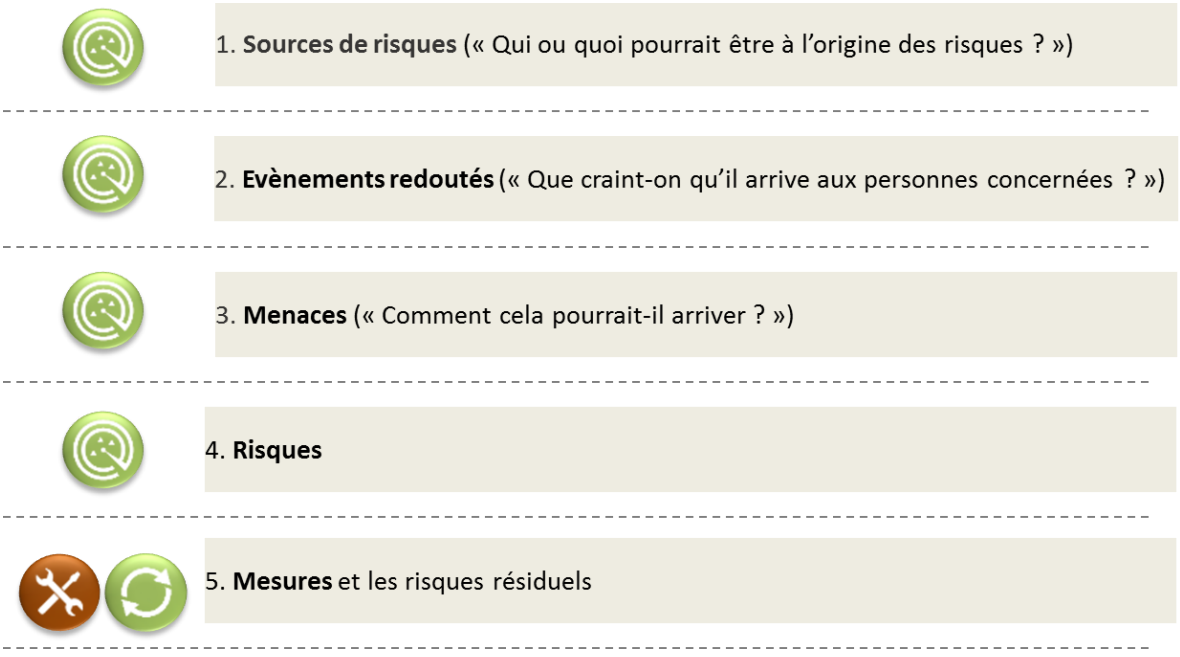


Figure 20 : Processus d'analyse de risques et d'évaluation des mesures de sécurité

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 « l*e 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*** *[…]. 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.

5.10 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.

a) la pseudonymisation et le chiffrement des données à caractère personnel ;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
c) 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 ;
d) 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 ?
- 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 donnée était estimé à 3.62 million de dollars[5],
  - Le coût moyen d'une perte ou divulgation de donnée sensible 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'affaire mondial consolidé pour l'organisation concernée par le manquement (le montant le plus élevé étant retenu).

[5] 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 (métier, 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 à 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 GDPR (sécuriser notamment le registre des traitements, les enregistrements de consentement, etc.). Les traitements liés au GDPR 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[6], voire de preuve formelle, qu'aucune technique[7] de ré-identification ne permet de dégrader cet effet d'anonymisation (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. »*

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

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

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 donnée 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 21 : Exemple de mesures préconisées pour un projet

6. Référentiels et organismes sur lesquels s'appuyer

6.1 Les Labels de la CNIL

Label CNIL Gouvernance Informatique et Libertés

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

1. l'organisation interne de la gestion des données personnelles ;
2. la procédure de vérification de la conformité des traitements à la loi ;
3. 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.

6.2 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 :

1. les normes de terminologie et celles portant sur les principes ;
2. les normes sur les processus/le management ;
3. les normes sur les technologies.

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 29151

Figure 22 : Normes en lien avec la protection des données 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 liberté, 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 diffusion 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 23 : Principes de la norme ISO 29100

Cette norme complète le RGPD, notamment en dessinant les contours du principe d'auditabilité, et pousse 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 stocke et traite 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) ainsi que de décrire la structure et le contenu du rapport d'EIVP. Afin de prouver sa conformité au RGPD, cette norme apporte un outil pour répondre de manière homogène au niveau international aux demandes EIVP 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 29151 - Code de bonnes pratiques pour la protection des données à caractère personnel

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 27001 - Information Security Management Systems (ISMS)

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 contrôles 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.

ISO 27018 - Code of practice for personally identifiable information protection in public clouds

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

LISO/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 » (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 de « Committee Draft » depuis décembre 2017. 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.

6.3 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.

6.4 Association d'experts

Association Française des Correspondants aux Données Personnelles (AFCDP) :

Cette association ouverte au CIL, DPO 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 DPO.

Association des Data Protection Officers :

Présidée et fondée par Alain Bensoussan, avocat, cette association a pour but de d'accompagner les Data Protection Officers 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.).

6.5 Certifications

L'Article 42 du Règlement européen sur la protection des données personnelles 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.) proposent une certification 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 démonter 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. Cette certification est basée sur un système de management ISO 9001.

Bureau Veritas propose également deux certifications : la première sur la gestion de la protection des données et la seconde sur les personnes pour les DPO. Concernant les DPO, 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, DPO, DPO 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 [8].

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

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 toutes entités 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 de la 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'atteintes 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 à 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 devant entrer en vigueur 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, e RGPD prévalent 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 vigueur 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. On ne retrouve néanmoins 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.

DPO : Data Privacy Officer ou Délégué à la protection des données 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 nationale (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 : responsable du traitement des données personnelles pour le compte, sur instruction et sous l'autorité d'un responsable de 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

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).*

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

AMRAE
L'ASSOCIATION

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