# LA VALORISATION DU TRAITEMENT DES DEMANDES D'EXERCICE DE DROITS

THESE PROFESSIONNELLE


PIERRE-YVES FABRISSIN

INSTITUT SUPERIEUR D'ÉLECTRONIQUE DE PARIS (ISEP)

MS – MANAGEMENT & PROTECTION DES DONNEES A CARACTERE PERSONNEL

PROMOTION 2023-2024

# REMERCIEMENTS

**À Rani ZAIDI**, pour m'avoir ouvert la voie vers un horizon riche de promesses et de challenges à relever, ainsi que pour ses encouragements et son soutien indéfectible au fil des années.

**À Nour HABITA**, pour une année riche en apprentissages et pour les qualités humaines dont elle fait preuve malgré les défis rencontrés.

**À Bruno RASLE**, **Valentin THEVENOT**, **Judicaël PHAN** et **Ali ALLAOUA**, pour le temps qu'ils m'ont consacré et la richesse de leurs éclairages, qui ont nourri ma réflexion et contribué à approfondir mon travail.

**À ma mère**, pour une intelligence dans la relecture qu'aucune IA ne pourrait égaler.

# RESUMME

La gestion et le traitement des demandes de droits en matière de protection des données personnelles ne doivent pas être perçus comme de simples contraintes réglementaires.

La présente thèse professionnelle se propose d'explorer – à travers le prisme du traitement des demandes de droits - en quoi les obligations imposées par la règlementation en matière de protection des données personnelles, peuvent être transformées en opportunités stratégiques permettant aux organisations d'améliorer leur gouvernance, d'optimiser leurs processus et de renforcer leur compétitivité.

Dans un premier temps, l'étude met en lumière la nécessité d'une structuration efficace de la gestion des droits, incluant notamment la mise en place de procédures claires, la formation des collaborateurs et l'organisation optimale des flux d'informations. Une bonne structuration favorise une meilleure circulation des bonnes pratiques entre les différents services et entités, rendant la conformité plus efficiente et bénéfique à l'ensemble des opérations.

La digitalisation constitue également un levier majeur. Toutefois, l'automatisation (voire l'industrialisation) des processus de traitement des droits doit être pensée avec soin pour ne pas altérer la relation humaine avec les personnes concernées. Trouver un équilibre entre automatisation et interactions humaines est essentiel pour assurer une gestion fluide et transparente, tout en renforçant la confiance des publics concernées.

Enfin, cette thèse insiste sur la dimension stratégique du RGPD : au-delà de la conformité, la gestion des droits devient un levier de différenciation sur le marché. Une approche transparente et éthique favorise la « confiance numérique », la fidélisation des clients et l'amélioration de l'image de marque. Elle permet également à l'organisation d'améliorer ou de développer des services innovants, de sécuriser son business et d'accéder à de nouveaux marchés.

Ainsi, la présente étude cherche à démontrer que le traitement des demandes de droits ne doit pas être perçu comme une contrainte mais bien comme une opportunité d'innovation, de transformation organisationnelle et de croissance durable.

# SOMMAIRE

# LEXIQUE

**Règlement général sur la protection des données** : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement Général sur la Protection des Données » ou « RGPD ».[1]

**Loi informatique et libertés** : Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée par la loi du 20 juin 2018 et son décret d'application du 1 août 2018, l'ordonnance du 12 décembre 2018, ainsi que le décret d'application de la loi, daté du 29 mai 2019 et entré en vigueur le 1er juin 2019, dite "Loi Informatique et Libertés".[2]

**Responsable du traitement** : Entité (entreprise, organisation, administration, etc.) qui détermine les objectifs et les moyens du traitement des données personnelles. En d'autres termes, c'est celui qui décide pourquoi et comment les données personnelles sont collectées, utilisées, conservées ou partagées.

**Sous-traitant** : Un sous-traitant est une entreprise ou une organisation qui traite des données personnelles pour le compte d'un responsable du traitement, sans en décider ni les finalités (le « pourquoi ») ni les moyens essentiels (le « comment »). Il agit uniquement selon les instructions du responsable du traitement et doit garantir la sécurité et la confidentialité des données qui lui sont confiées.

**Système d'information** : Ensemble des ressources technologiques et organisationnelles utilisées pour collecter, stocker, traiter et partager des informations au sein d'une organisation. Il comprend les logiciels, les bases de données, les serveurs, les réseaux informatiques, ainsi que les processus qui encadrent leur utilisation.

**Autorité de contrôle** : Organisme indépendant chargé de veiller au respect des règles de protection des données personnelles dans un pays ou une région. Dans l'Union européenne, chaque État membre dispose d'une autorité de contrôle qui applique le RGPD et protège les droits des citoyens en matière de vie privée.

[1] Texte intégral du RGPD, publié au Journal officiel de l'Union européenne, consultable via le lien suivant : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

[2] Texte intégral de la loi « Informatique et Libertés », publié au Journal Officiel, consultable via le lien suivant : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/

**Commission nationale informatique et libertés** : Autorité administrative indépendante chargée de veiller à la protection des données personnelles et des libertés individuelles en France. Elle a pour mission d'informer, d'accompagner, de contrôler et, si nécessaire, de sanctionner les organismes (entreprises, administrations, associations, etc.) qui ne respectent pas la réglementation en matière de protection des données.

**Délégué à la protection des données** : Personne désignée au sein d'une organisation pour veiller au respect des règles de protection des données personnelles, notamment celles imposées par le RGPD. Il joue un rôle clé dans l'accompagnement et la coordination des efforts déployés dans le cadre de la mise en conformité, ainsi que l'encadrement et le suivi des traitements de données personnelles réalisés par le responsable du traitement.

# LISTE DES ABREVIATIONS

**RGPD** : Règlement général sur la protection des données

**LIL** : Loi « Informatique et Libertés »

**UFADAA** : Uniform Fiduciary Access to Digital Assets Act

**BGB** : Bürgerliches Gesetzbuch (Code civil allemand)

**CJUE** : Cour de justice de l'Union européenne

**CEPD** : Comité européen de la protection des données

**CNIL** : Commission Nationale informatique et libertés

**ICO** : Information Commissioner's Office (autorité de contrôle britannique)

**DPO** : Délégué à la protection des données

**RT** : Responsable du traitement

**ST** : Sous-traitant

**SI** : Système d'Information

**API** : Application Programming Interface

# INTRODUCTION

*« Tout être humain a un droit de regard, de confidentialité et de contrôle sur ses données personnelles y compris sur celles produites du fait de ses comportements et des objets connectés à sa personne. Il a droit à la protection de son anonymat quand il le souhaite".*

***Article 4 de la « Déclaration préliminaire des droits de l'homme numérique »***
*présentée au Forum d'Avignon (édition 2014)*

Rédigé il y a maintenant une dizaine d'années, le projet de « Déclaration des Droits de l'Homme Numérique » (DDHN) n'est désormais plus disponible pour consultation sur le web. Il porte toutefois l'imaginaire de l' « homme numérique » évoluant dans une nouvelle réalité qu'est celle du « monde virtuel ».[3]

Celle-ci s'inscrit dans une vision romantique, trouvant d'ailleurs une résonance particulière dans l'aube annoncée du métavers : celle d'une humanité digitalisée, au patrimoine numérique et dont les données personnelles forment l' « ADN numérique ».[4]

Les données personnelles constituent l'essence même de l'être humain évoluant dans l'univers digital. A ce titre, elles doivent faire l'objet d'une attention particulière et d'une protection renforcée tout en tenant compte des impératifs liés à la recherche, à la compétitivité, à la libre circulation des biens, ainsi qu'à la liberté d'entreprise. Cette logique trouvera écho dans la lettre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, dit « Règlement Général sur la Protection des Données » ou « RGPD ».[5]

[3] E. DANBLON et I. MAYEUR, « La Déclaration préliminaire des Droits de l'Homme Numérique : un exercice pratique de l'utopie rhétorique ? », Rhétorique et citoyenneté, 2015 : https://journals.openedition.org/rhetorique/408

[4] Tribune du Monde du 21 novembre 2013 de L. KALTENBACH, Directrice générale et membre fondateur du Forum d'Avignon : https://www.lemonde.fr/idees/article/2013/11/21/pour-l-intimite-numerique_3518245_3232.html

[5] Texte intégral du RGPD, publié au Journal officiel de l'Union européenne, consultable via le lien suivant : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679

En effet, le RGPD, en son Chapitre 3[6], (re)consacre les droits reconnus aux personnes concernées afin de leur assurer la maîtrise de leurs données personnelles. Conformément et selon les modalités fixées aux articles 12 à 22, ces dernières disposent de la capacité de solliciter, auprès du responsable du traitement, l'accès aux données traitées, leur rectification, leur effacement (ainsi que, le cas échéant, leur déréférencement sur le web), leur portabilité, ainsi que la limitation, la suspension ou l'arrêt définitif du traitement dont elles font l'objet. Les personnes concernées disposent également d'un certain nombre de droits en présence d'un traitement visant à la prise d'une décision de manière automatisée.

# 1. Objectifs initiaux et dévoiement des droits reconnus aux personnes concernées

Les droits reconnus aux personnes concernées ont pour optique de leur permettre de mieux maîtriser l'ensemble des aspects attachés à la personne humaine et à sa vie privée. L'enjeu est considérable lorsque ces éléments constituent des assets de l'économie numérique et particulièrement à l'heure où les capacités de traitement croissent de manière exponentielle. Cela, notamment, en raison d'une course effrénée à la puissance de calcul et des promesses induites par l'informatique quantique, de l'essor des modèles d'intelligence artificielle ainsi que de la multiplication des objets connectés.

Toutefois, l'on peut également dénoter une pluralité d'objectifs sous-jacents à l'exercice de ces droits. Certains, plus légitimes, visant à dépasser le cadre du seul domaine des données personnelles, tels que la constitution d'un dossier judiciaire, la préparation et/ou la formulation d'un recours (à l'encontre d'une décision de refus de crédit, par exemple). D'autres, plus contestables, voire détournés à des fins de nuisance et visant à gêner - ou même paralyser - le responsable du traitement, tels que l'exercice systématique du droit d'accès dans le cadre d'un contentieux prudhommal, ou son exercice collectif (voire abusif) dans le cadre de la lutte syndicale ou concurrentielle.

# 2. Rappel des droits, de leur portée et des enjeux de ces derniers

## 1.1. Droit à l'information (articles 12 et suivants RGPD)

Le droit à l'information des personnes concernées est un élément fondamental de la réglementation en matière de protection des données personnelles visant à assurer la transparence de leur collecte et de leur traitement. Ce droit, prévu aux articles 12 et suivants

[6] Voir Chapitre 3 RGPD, consultable en ligne via le lien suivant : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article12

du RGPD,[7] impose au responsable du traitement d'informer de manière claire, concise et transparente les individus sur la manière dont leurs données sont traitées. L'objectif est d'assurer une compréhension complète et éclairée des personnes concernées. Elles peuvent ainsi exercer leurs droits de manière effective, tout voyant renforcée leur confiance dans les pratiques des organisations.

Lorsque les données personnelles sont collectées directement auprès de la personne concernée, l'information doit être fournie au moment de la collecte[8]. Elle peut l'être, par exemple, via des mentions d'information apposées sur les formulaires (physiques ou informatiques) de collecte de données. Elle peut également l'être, d'une manière plus globale, via un document dédié tel qu'une politique de confidentialité, disponible sur le site web du responsable de traitement. Dans les cas où les données sont obtenues indirectement (par exemple via des tiers ou des sources publiques), le responsable du traitement doit informer la personne concernée dans un délai raisonnable et au plus tard dans un délai d'un mois (ou, le cas échéant, au moment de la première communication avec la personne concernée)[9].

Ces informations comprennent a minima l'identité et les coordonnées du responsable du traitement, les finalités du traitement, la base légale justifiant le traitement, les destinataires (ou catégories de destinataires) des données, la durée de conservation des données (ou les critères utilisés pour la calculer), le rappel des droits des personnes concernées (y compris, la cas échéant, le droit à retirer son consentement à tout moment), la possibilité d'introduire une réclamation auprès de l'autorité de contrôle et, le cas échéant, l'existence de transfert des données vers un pays tiers (ainsi que les « garanties appropriées » encadrant un tel transfert). Lorsque les données sont collectées de manière indirecte, le responsable du traitement doit en outre informer la personne concernée de la source des données personnelles et des catégories de données concernées. Ces éléments doivent être mis à disposition de manière proactive, même si la personne concernée n'en fait pas la demande.

L'obligation de transparence impose de présenter et communiquer les informations de manière « accessible, compréhensible et rédigée dans un langage clair et simple »[10]. La transparence ne s'applique pas uniquement à l'étape initiale de la collecte des données, mais également à l'ensemble des interactions que le responsable du traitement peut avoir avec la

[7] Voir articles 12 à 14 RGPD, consultables via le lien suivant : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre3#Article12

[8] Article 13 RGPD

[9] Article 14 RGPD

[10] Article 12 RGPD

personne concernée. Elle perdure durant l'ensemble du cycle de vie des données et, notamment, lorsque les personnes concernées leurs droits (voir infra). En effet, pour que les individus puissent garder la maîtrise de leurs données, il est fondamental qu'ils aient conscience du contexte et des modalités des traitements qui en sont opérés.

A partir de l'article 15 du RGPD, les droits reconnus aux personnes concernées requièrent de leur part une certaine proactivité : il leur appartient de les exercer afin de produire une réaction de la part du responsable du traitement.

### 1.2. Droit d'accès (article du 15 RGPD)

Le premier de ces droits est un corollaire du droit à l'information. Il s'agit d'un des droits les plus absolus reconnus par le RGPD en ce sens qu'il ne connait que très peu de limites. Seuls certains fichiers de police ou intéressant la sûreté de l'État ne peuvent pas faire l'objet d'une demande d'accès. Dans les cas plus « communs », la seule hypothèse dans laquelle le responsable du traitement peut se dispenser de donner droit à une demande d'accès est celle dans laquelle la demande est « manifestement infondée ou excessive [entendre ici répétée] », sans que de réelles précisions n'aient été apportées par le législateur européen. Le droit d'accès n'est assorti d'aucune exigence tenant au motif de la demande (aucune justification ne peut être demandée à la personne concernée), ou à sa portée. De plus, le droit d'accès s'applique à l'ensemble des bases légales pouvant justifier le traitement.

Le responsable du traitement est tenu de « *rechercher des données à caractère personnel dans l'ensemble de ses systèmes informatiques et de ses systèmes d'archivage non informatiques* »[11]. Cela concerne donc tous types de supports dans chacun des services de l'organisme et sur l'ensemble de ses systèmes d'information.

En vertu du droit d'accès, le responsable du traitement doit apporter à la personne concernée :

- La confirmation que des données la concernant sont ou ne sont pas traitées ;
- Des informations portant, a minima, sur les éléments relatifs au droit d'information de la personne concernée (voir supra) ;
- La communication, sous une forme intelligible, des données faisant l'objet des traitements ;

[11] CEPD, Lignes directrices relatives au droit d'accès n°01/2022 du 28 mars 2023, p.48

- Le cas échéant, la logique sous-jacente à toute décision automatisée induite par le traitement des données de la personne concernée (voir infra : droit de ne pas faire l'objet d'une décision individuelle automatisée).

Le droit d'accès permet principalement à la personne concernée de savoir quelles données sont traitées la concernant, de s'assurer de la pertinence des données traitées, de la licéité du traitement[12] ainsi que de l'existence et des modalités d'exercice de ses autres droits[13].

### 1.3. Droit de rectification (article 16 RGPD)

Le droit de rectification s'applique lorsque des données personnelles sont inexactes, fausses ou obsolètes. Ce droit s'inscrit dans la continuité directe du principe d'exactitude des données[14]. Il s'agit là encore d'une approche proactive : si le responsable du traitement a failli dans l'accomplissement de cette obligation ou si la situation de la personne concernée a évolué sans qu'il n'en ait été informé, cette dernière a la possibilité de rétablir la situation en exerçant son droit de rectification.

Une marge d'interprétation existe quant à l'acception de ce droit : selon le CEPD, le droit de rectification ne s'applique qu'aux données tangibles (objectives) et non aux données intangibles (subjectives)[15]. Quoi qu'il en soit, le droit de rectification permet à la personne concernée de remettre en question le procédé à l'origine de la création de certaines données. Cela, notamment, lorsqu'il s'agit du résultat d'un procédé mis en œuvre par le responsable du traitement (informations tirées du croisement d'autres données personnelles tel qu'un indice de solvabilité ou un profil de risque tiré de donnée financières, familiales, etc.).

### 1.4. Droit à l'effacement des données (article 17 RGPD)

Le droit d'obtenir l'effacement des données (et son pendant, sur le web, qu'est le droit à l'oubli) consistent dans la possibilité pour la personne concernée d'en obtenir la suppression sous certaines conditions. En résumé, l'effacement des données pourra être obtenu lorsqu'il n'existe plus de raison légitime pour que le responsable du traitement les conserve. Il ne s'agit donc pas d'un droit absolu. Il existe six cas dans lesquels ce droit trouve à s'appliquer :

---

[12] CEPD, Lignes directrices relatives aux droits des personnes concernées, 25 fév. 2014, p.11

[13] CJUE, C-553/07, 7 mai 2009, Rotterdam/Rijkeboer, point 5, consultable via l'URL suivante : https://curia.europa.eu/juris/liste.jsf?num=C-553/07&language=fr

[14] Article 5(1)d) RGPD

[15] CEPD, dossier 2012-0598

- Les données ne sont plus nécessaires à la réalisation du traitement pour lequel elles ont été collectées ;
- Le consentement de la personne concernée est retiré et aucune autre base légale ne peut fonder le traitement ;
- La personne concernée s'est opposée à l'utilisation de ses données sans que le responsable du traitement ne soit en mesure d'invoquer des motifs légitimes et impérieux justifiant la poursuite du traitement ;
- Les données sont utilisées dans le cadre d'un traitement illicite (il sera illicite en cas d'absence de base juridique ou encore de violation de la règlementation en matière de protection des données) ;
- Une obligation légale exige l'effacement des données ;
- Les données d'un mineur (le terme « mineur » doit être ici appréhendé par analogie à la notion de « majorité numérique »,[16] qui, en France, est fixée à 15 ans[17]) ont été collectées dans le cadre de services de la société de l'information.

Enfin, le droit à l'effacement des données souffre d'un certain nombre de limitations, à savoir :

- L'exercice de la liberté d'expression et d'information ;
- L'accomplissement d'une mission d'intérêt public ;
- Le respect d'une obligation légale empêchant la suppression des données ;
- La poursuite d'un objectif de santé publique ;
- La poursuite de finalités archivistiques dans l'intérêt public, de recherche scientifique, historique ou statistiques ;
- La constatation, l'exercice ou la Défense de droits en justice.

Par conséquent, il s'agit de trouver un compromis entre la maîtrise par les personnes concernées de leurs données et les réalités économiques ou sociétales. Les libertés de l'individu quant à ses données personnelles sont ici contraintes par des intérêts que le

[16] Au sens de l'article 8 RGPD, un enfant est considéré comme un « mineur » lorsqu'il a moins de 16 ans. Les États membres peuvent décider d'abaisser le seuil de la majorité dans la limite de 13 ans.

[17] Article 4 de la loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, consultable via le lien suivant : https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000047799537#:~:text=«%20Le%20fait%20pour%20un%20fournisseur,mondial%20pour%20l'exercice%20précédent

législateur a qualifiés de « supérieurs ». Le responsable du traitement doit être en mesure d'identifier ces intérêts, de réaliser les arbitrages nécessaires en fonction du cas d'espèce et d'agir en conséquence ; cet arbitrage engageant sa responsabilité.

### 1.5. Droit à la limitation du traitement (article 18 RGPD)

Le droit à la limitation du traitement permet à la personne concernée d'obtenir le « gel » du traitement, emportant de ce fait la conservation des données pour un temps. Le traitement est suspendu : les données ne peuvent plus être utilisées pour les finalités envisagées. Elles ne sont plus accessibles aux services opérationnels du responsable du traitement et ne peuvent plus être réutilisées.

L'exercice du droit à la limitation du traitement trouve à s'appliquer dans quatre cas :

- Lorsque l'exactitude des données est contestée par la personne concernée, une limitation temporaire du traitement pourra alors être appliquée « *pendant un délai permettant au responsable du traitement de vérifier l'exactitude, y compris l'exhaustivité, des données* »[18] ;
- Lorsque le traitement est illicite mais que la personne concernée souhaite la limitation du traitement en lieu et place de l'effacement des données, auquel cas et même si la limitation « *ne peut intervenir immédiatement, elle doit néanmoins être considérée rapidement afin de préserver les droits de la personne concernée* » (au plus tard dans un délai de quinze jours ouvrables)[19] ;
- Lorsque le responsable du traitement n'a plus besoin des données mais qu'elles sont nécessaires à la personne concernée pour la défense, la constatation ou l'exercice de ses droits en justice ;
- Lorsque la personne concernée s'est opposée au traitement, une limitation temporaire du traitement pourra alors être appliquée le temps de permettre au responsable du traitement de procéder aux vérifications concernant la supériorité (ou non) de ses intérêts propres face à ceux de la personne concernée.

Il est important de noter que le responsable du traitement doit informer la personne concernée de la levée de la limitation du traitement afin de lui permettre, le cas échéant, de se prévaloir de son droit à la limitation sur un autre fondement que celui ayant initialement été invoqué.

[18] CEPD, dossier 2011-0483

[19] Ibid.

### 1.6. Droit à la portabilité des données (article 20 RGPD)

La portabilité est un doit relativement « nouveau » dans la chronologie de la protection des données personnelle. Il a été instauré par le RGPD. A l'origine, il est apparu dans certains secteurs régulés (par exemple celui des communications électroniques, ou encore du secteur bancaire)[20]. Il s'agit d'un droit dit « économique », ayant vocation à protéger le consommateur et à stimuler la concurrence, notamment, dans le secteur des technologies de l'information et de la communication (TIC). Selon le CEPD, il s'agissait d'une opportunité de « *rééquilibrer les relations entre les personnes concernées et les responsables de traitement* »[21].

Le droit à la portabilité vise à impliquer les personnes concernées dans le traitement de leurs données personnelles. Il facilite ainsi leur capacité à les déplacer, les copier ou les transmettre facilement d'un système d'information à un autre (que ce soit pour usage personnel ou dans le cadre d'une réutilisation par un autre responsable du traitement). Par exemple, il peut s'agir de récupérer les données d'un service de messagerie électronique afin de pouvoir établir une liste d'invités (via la liste des contacts), mesurer son empreinte carbone, envoyer les messages vers une plateforme d'archivage sécurisé, etc.[22] Autre exemple : il peut s'agir d'extraire, sur une plateforme de streaming musical, l'historique des titres écoutés afin de mesurer le nombre d'écoute et de pouvoir de décider quelle musique acheter ou écouter sur une autre plateforme[23], etc.

En substance, le droit à la portabilité permet de demander à un responsable du traitement de transmettre, sans obstacle, ses données personnelles directement à la personne concernée et/ou à une organisation tierce. Toutefois, ce droit ne trouve à s'appliquer que dans le cadre :

- D'un traitement automatisé ;
- D'un traitement fondé sur le consentement ou sur l'exécution d'un contrat ;

---

[20] Voir, par exemple dans le secteur des télécommunications et afin de favoriser la mobilité du consommateur d'un opérateur à un autre : loi n°2014-344 du 17 mars 2014, dite loi "Hamon", consultable via le lien suivant : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028738036, ainsi qu'en particulier l'article L. 44-4 du Code des postes et des communications électroniques (CPCE), consultable via le lien suivant : https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070987/LEGISCTA000006150688/?anchor=LEGIARTI000043538973#LEGIARTI000043538973

[21] CEPD, Lignes directrices relatives au droit de portabilité (WP242) du 13 décembre 2016, p.4

[22] CEPD, Lignes directrices relatives au droit de portabilité du 13 décembre 2016 (WP242), p.5 et p.8

[23] Ibid.

- De données activement fournies par la personne concernée ou résultant d'une simple observation de son activité (ces données étant considérées comme fournies directement par la personne concernée)[24].

Afin, semble-t-il, d'éviter que l'exercice du droit à la portabilité n'engendre des distorsions de la concurrence ou ne risquer de désinciter les investissements dans le secteur du numérique, le législateur a pris le soin d'exclure les données à valeur ajoutée du périmètre de la portabilité. Ainsi, lorsqu'elles sont générées à la suite d'un procédé technique opéré par le responsable du traitement (et parce qu'un tel procédé pourrait être innovant et/ou coûteux), les données ne pourront profiter à un autre opérateur économique. De cette manière, une organisation tierce ne pourra pas tirer indument profit des investissements réalisés par le responsable du traitement.

Outre l'aspect économique (transfert vers un autre responsable du traitement), le droit à la portabilité confère à la personne concernée le droit de recevoir les données. Cela implique que les données lui soient transmises dans un format approprié lui permettant de les utiliser.

Le droit à la portabilité cherche à inscrire les données dans le cadre d'une certaine interopérabilité des systèmes. Lorsqu'il transmet les données, le responsable du traitement doit donc privilégier un « *format structuré, couramment utilisé et lisible par machine* »[25]. Sur ce point, le législateur européen a d'ailleurs indiqué qu'il fallait « *encourager les responsables du traitement à mettre au point des formats interopérables permettant la portabilité des données* » sans toutefois « *créer, pour les responsables du traitement, d'obligation d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles* »[26].

Le RGPD incite donc à la création de formats standardisés, tout en faisant preuve d'une certaine réserve afin de ne pas imposer aux responsables du traitement les coûts - potentiellement exorbitants – de l'interopérabilité.

### 1.7. Droit d'opposition au traitement (article 21 RGPD)

A travers le droit d'opposition, la personne concernée peut requérir que ses données personnelles ne fassent pas (ou plus) l'objet d'un traitement. Ce droit trouve à s'appliquer lorsque le traitement visé repose sur l'intérêt légitime ou l'exercice d'une mission d'intérêt public. Dans le domaine du numérique, la personne concernée doit pouvoir exercer son droit

[24] CEPD, Lignes directrices relatives au droit de portabilité du 13 déc. 2016 (WP242), p.12

[25] Article 20(1) RGPD

[26] Considérant 68 RGPD

d'opposition via des « *procédés automatisés utilisant des spécifications techniques* »[27] (par exemple via un lien cliquable, un « bouton d'opposition », etc.).

Le droit d'opposition peut être exercé pour des raisons tenant « *à la situation particulière* » de la personne concernée. De son côté, le responsable du traitement peut refuser de mettre fin au traitement et faire valoir ses propres intérêts légitimes et impérieux lorsqu'ils prévalent sur les intérêts, droits et libertés de la personne concernée. Ce sera par exemple le cas lorsque le traitement est nécessaire au respect d'une obligation légale imposée au responsable du traitement, à l'exécution d'un contrat régulièrement conclu, à la sauvegarde de la vie humaine ou d'un intérêt vital, etc.

Il existe toutefois un droit d'opposition « renforcé ». En effet, lorsqu'un traitement repose sur le consentement de la personne concernée, celle-ci dispose du droit - absolu - de retirer son consentement et ce à tout moment et pour n'importe quelle raison. Seule limite : le retrait du consentement n'est pas rétroactif. Le retrait du consentement ne peut entacher la légalité des traitements réalisés antérieurement.[28] C'est la raison pour laquelle le consentement est le fondement juridique le moins préférable pour le responsable du traitement puisqu'il expose le traitement à une certaine forme d'instabilité.

### 1.8. Obligation de notification aux destinataires des données (article 19 RGPD)

La rectification ou l'effacement de données (tout comme l'opposition ou la limitation du traitement) perdraient grandement en substance s'ils n'étaient pas répercutés sur l'ensemble de la chaîne de traitement. Toutefois (et fort heureusement), la réglementation relative à la protection des données personnelles ne fait pas reposer sur la personne concernée la charge de faire valoir ses droits auprès de chacun des destinataires des données faisant l'objet d'une demande de rectification, d'effacement, d'opposition ou de limitation du traitement. C'est donc bien au responsable du traitement qu'il incombe de notifier la demande exercée par la personne concernée à l'ensemble des destinataires des données (y compris ses partenaires et sous-traitants éventuels).[29]

### 1.9. Droit de ne pas faire l'objet d'une décision individuelle automatisée (article 22 RGPD)

Avec le développement technologique, la démocratisation et la sophistication des algorithmes (et des modèles d'IA), de plus en plus de décisions sont prises de manière

[27] Article 21(5) RGPD

[28] Article 7(3) RGPD

[29] Article 19 RGPD

automatisée en se fondant sur le traitement de données personnelles. Il devient alors crucial de protéger les personnes concernées, a fortiori lorsque de telles décisions impactent leur vie quotidienne et/ou économique. Les personnes concernées doivent être en mesure de comprendre comment une telle décision est prise, sur quelles données et selon quelle logique elle est fondée.

La règlementation actuelle interdit, en principe, aux responsables de traitement de prendre, sans aucune intervention humaine, des décisions produisant des effets juridiques ou similaires pour la personne concernée. Toutefois, ces décisions automatisées sont autorisées dans certains, strictement encadrés. C'est le cas lorsque le traitement :

- Repose sur la conclusion ou l'exécution d'un contrat régulièrement conclu avec la personne concernée ;
- Est autorisé par une loi nationale comprenant des garanties adéquates ;
- Repose sur le consentement explicite de la personne concernée.

A noter qu'une décision automatisée fondée sur le traitement de données relevant d'une « catégorie particulière » (au sens de l'article 9 du RGPD) n'est licite que dans la mesure où la personne concernée a donné son consentement explicite ou si elle poursuit un intérêt public important.

Même lorsqu'elle est permise, la prise de décision automatisée est soumise à des obligations spécifiques visant à protéger les personnes concernées :

- La transparence des algorithmes, obligeant le responsable du traitement à informer la personne concernée de l'existence d'un traitement automatisé, de la logique sous-jacente au traitement et des conséquences qu'il pourrait avoir sur sa situation ;
- La mise en œuvre effective des droits à obtenir une intervention humaine, d'exprimer son point de vue, de contester la décision.

De plus, des mesures techniques et organisationnelles appropriées doivent être prises pour protéger les droits et libertés des personnes concernées, garantir une utilisation équitable des algorithmes et veiller à en limiter les biais (non-discrimination, pertinence et qualité des modèles, révision périodique, etc.).

### 1.10. Droit de disposer de ses données après le décès (article 85 LIL)

Le droit de disposer de ses données après son décès ou « *droits post-mortem* » intervient en complément du droit à l'effacement des données prévu à l'article 17 du RGPD.

Les enjeux derrière ce droit diffèrent en fonction des secteurs d'activité et de la typologie des données impliquées. Il est particulièrement important en présence de données à forte valeur patrimoniale ou émotionnelle (par exemple dans le cade des réseaux sociaux, de services de stockage « dans le cloud », etc.). Il est également très utile dans le cadre de procédures administratives (par exemple pour que les héritiers puissent effectuer démarches post-mortem) ou notariales (pour le règlement d'une succession, l'établissement d'actes notariés, la répartition d'actifs financiers, etc.). Il peut également être pertinent en présence de données relatives à la santé ou au patrimoine génétique.

Il s'agit d'un des droits les plus méconnus et les moins maitrisés. A juste titre puisqu'il n'est pas consacré par le RGPD, qui ne concerne que les données de personnes vivantes.[30] De son côté, la législation française prévoit le droit pour les personnes concernées d'organiser le sort de leurs données après leur mort.

L'article 63 de la loi pour une République numérique[31] a introduit la faculté (via des « directives anticipées »), censé permettre aux personnes concernées de déterminer, de leur vivant, ce qu'il adviendra de leurs données personnelles après leur décès. Ce mécanisme a été repris dans la loi informatique et libertés.[32] Les directives anticipées peuvent être générales et s'appliquer à l'ensemble des données personnelles (ou à certaines catégories), ou particulières et s'appliquer à des traitements spécifiques ou à des acteurs précis. En pratique, elles peuvent être transmises au(x) responsable(s) du traitement concerné(s) ou confiées à un tiers de confiance certifié par la CNIL.

Les responsables du traitement ont pour obligation de permettre aux utilisateurs de formuler de telles directives, de mettre en application ces directives (sauf disposition légale contraire) et d'informer les utilisateurs de l'existence de ce droit et des modalités de son exercice. Toutefois, en l'absence de décret d'application, un tel mécanisme reste en suspens…[33]

Certains systèmes juridiques ont, à l'instar du droit français (s'il en est), prévu des dispositions pour organiser le sort des données après le décès de la personne concernée. Par exemple, le droit allemand considère les données numériques (courriels, comptes en ligne,

---

[30] V. THEVENOT, « Anticiper sa fin de vie (numérique ou non), c'est possible ! », 2021, consultable via l'URL suivante : https://fr.linkedin.com/pulse/anticiper-sa-fin-de-vie-num%C3%A9rique-ou-non-cest-valentin-thevenot

[31] Article 63 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique

[32] Article 85 LIL, consultable via le lien suivant : https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000039280582

[33] Publication LinkedIn, V. THEVENOT, 2024, consultable via l'URL suivante : https://fr.linkedin.com/posts/vthevenot_a-quoi-bon-anticiper-la-gestion-de-ses-donn%C3%A9es-activity-7257300252292976640-GaJs

etc.) comme des biens héritables. Ainsi, la Cour fédérale de justice allemande a pu décider - sur le fondement des dispositions du code civil allemand relatives à la succession[34] - que « *les contenus numériques, comme les comptes en ligne et les messages, font partie du patrimoine du défunt et doivent être transmis aux héritiers, au même titre que d'autres biens matériels ou immatériels* ».[35]

De la même manière, la plupart des États fédérés des Etats-Unis ont adopté l' « Uniform Fiduciary Access to Digital Assets Act » (UFADAA), permettant aux représentants légaux d'accéder aux actifs numériques et aux données personnelles d'une personne décédée (sauf si celle-ci a laissé des directives contraires).[36] A ce titre, certaines plateformes numériques doivent fournir un accès aux données si cela est demandé par un représentant légal autorisé. De plus, la personne concernée peut préciser dans son testament - ou directement sur les plateformes (via des outils comme le « gestionnaire de compte inactif » de Google) - ce qu'il adviendra de ses données.[37]

D'autres systèmes juridiques ne prévoient pas (encore) de cadre législatif spécifique en matière de droits post mortem. Dans la pratique, les ayants droit doivent alors se tourner vers les responsables du traitement (entreprises et plateformes), qui appliquent leurs propres règles (Conditions Générales d'Utilisation). Ainsi, certains responsables du traitement ont mis en place des mécanismes en ce sens. C'est par exemple le cas de Facebook, qui permet de convertir un compte en « compte mémorial » ou de le supprimer sur demande des ayants droit. C'est également le cas de Google, qui offre un outil de gestionnaire de compte inactif pour planifier la gestion des données après le décès de son titulaire.

---

[34] Article 1992 du code civil allemand (BGB), consultable via le lien suivant : https://www.gesetze-im-internet.de/bgb/__1922.html

[35] BGH, Urteil vom 12.07.2018 - III ZR 183/17 du 12 juillet 2018, consultable via le lien suivant : https://op.europa.eu/en/publication-detail/-/publication/ab7f8ed2-d869-11e9-9c4e-01aa75ed71a1/language-en

[36] Voir, notamment, section 7 et 8 UFADAA, consultable via le lien suivant : https://www.uniformlaws.org/viewdocument/final-act-with-comments-40?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22&tab=librarydocuments

[37] Elizabeth SY, The revised Uniform Fiduciary Access Act : Has the law caught up with technology?, Touro Law Review, Vol.32, Nb.3, Art.7, 2016, consultable via le lien suivant : https://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2742&context=lawreview

## 3. Traitement des demandes d'exercice de droits par les responsables du traitement

Lorsqu'une personne concernée exerce un des droits qui lui sont reconnus par le RGPD, le responsable du traitement se doit d'y apporter une réponse. Selon la nature et la portée du droit exercé et lorsque ses conditions d'application sont réunies, un certain nombre d'actions doivent être mises en œuvre pour y faire droit. Il s'agit là du « traitement » des demandes d'exercice de droits.

Le traitement des demandes d'exercice de droits revêt de nombreuses implications et représente un réel « challenge » pour le responsable du traitement. En pratique, il soulève de nombreuses difficultés, tenant notamment à :

- **L'engagement de ressources** : temps, coûts, expertise, etc. ;
- **La gestion de risques juridiques** : organiser les rôles entre les différents partenaires, prestataires (y compris les Sous-traitants), procéder aux vérifications permettant de s'assurer de l'identité de la personne exerçant la demande (ou de sa légitimité lorsqu'elle est exercée par un tiers), etc. ;
- **L'organisation et la mise en place de process** : identifier les canaux possibles d'introduction des demandes (et choisir lesquels privilégier) ; former les personnels susceptibles d'être en contact avec les demandes ; identifier et localiser les données (sur des supports physiques et/ou au sein des systèmes d'information) ; être en capacité procéder, de manière efficiente, aux différentes actions requises en fonction du droit exercé ; articuler et répartir des tâches entre le DPO et les différents services impliqués, etc. ;
- **L'obligation de faciliter l'exercice des demandes pour les personnes concernées** (conformément aux dispositions de l'article 12, $2 RGPD[38]) : déployer une information claire et complète des personnes concernées concernant leurs droits et les modalités de leur exercice ; identifier les canaux et procédés leur permettant d'exercer leurs droits simplement et d'y répondre efficacement, etc. ;
- **La mise en œuvre de procédés techniques** : communiquer les informations demandées de manière sécurisée ; optimiser (voire automatiser), le traitement des demandes afin d'en réduire les coûts et de faciliter le travail des équipes concernées

[38] Voir : article 12, §2 RGPD

(par exemple pour localiser les données personnelles, supprimer les données, suspendre ou arrêter un traitement, …) etc.

Le responsable du traitement doit assurer la gestion efficace des demandes d'exercice des droits. Cela l'oblige à réfléchir en profondeur pour adapter sa stratégie. Il doit également être en mesure de réaliser les arbitrages nécessaires, en fonction du contexte et de la nature de ses activités de traitement. Les ressources allouées à la gestion et au traitement des demandes de droits vont donc varier en fonction de l'activité et de la situation propres à chaque organisation.

Il convient alors de rappeler que le traitement des demandes d'exercice de droits s'inscrit pleinement dans la logique de conformité et de responsabilisation induite par la règlementation applicable en matière de protection des données personnelles. Logique qui, à travers le RGPD, a été accentuée et réaffirmée par le législateur européen.

En effet, la méconnaissance des droits des personnes concernées (ou leur violation) est sanctionnée du plus haut pallier de sanctions prévues par le RGPD : jusqu'à 20.000.000EUR ou 4% du chiffre d'affaires annuel mondial.[39] A cela s'ajoute également le volet pénal, avec une sanction encourue s'élevant (en France) à 300.000EUR d'amende et jusqu'à 5 ans d'emprisonnement.[40] A ces sanctions vient s'ajouter le panel des sanctions administratives reconnues à l'autorité de contrôle et, notamment, l'injonction de mise en conformité sous astreinte (jusqu'à 100.000EUR par jour de retard), la suspension temporaire ou définitive du traitement et bien-sûr la publicité des sanctions (pouvant être redoutables en termes d'image).[41]

## 4. Exposition croissante des responsables du traitement aux demandes d'exercice de droits

Force est de constater que les responsables du traitement sont de plus en plus exposés aux demandes d'exercice de droits. Ce constat peut s'expliquer de plusieurs manières.

Premièrement, du fait d'une sensibilisation accrue et d'une prise de conscience croissante, par l'opinion publique, des enjeux liés à la protection des données personnelles et de la vie privée. De manière encourageante, les personnes concernées sont de plus en plus au fait de leurs droits. Deuxièmement, par une place croissante qu'occupent les traitements de données

[39] Voir : article 83, §5 RGDP

[40] Voir : articles 226-16 et suivants du code pénal

[41] Voir : Article 58, §2 RGPD et Article 20, III et IV LIL

personnelles dans la vie « courante ». Par voie de conséquence, les individus mesurent de plus en plus l'intérêt d'exercer leurs droits. Enfin, du fait de la multiplication des « proxys », acteurs visant à assister les personnes concernées dans la maîtrise de leurs données personnelles et à les représenter dans l'exercice de leurs droits.

Le marché (émergent) de l'intermédiation des demandes de droits est relativement récent et en constante évolution. Il se base sur l'automatisation des demandes et la fourniture de services diversifiés (identification des détenteurs des données, suivi des demandes et des relances, etc.). Cette diversification s'accroît avec la sophistication des outils technologiques et s'illustre, par exemple, au travers des services proposés par MINE[42]. Cette société permet à ses utilisateurs d'identifier les organisations détenant leurs données personnelles, grâce à des algorithmes analysant leurs interactions en ligne. Elle propose alors à ses utilisateurs d'exercer des demandes de droits pour leur compte et en assure le suivi.

Parmi ces intermédiaires se retrouvent notamment un certain nombre de cabinets d'avocats, ainsi que des sociétés spécialisées dans ces activités comme, par exemple, MY DATA DONE RIGHT[43], JUMBO PRIVACY[44] (solution particulièrement orientée Twitter/X), INCOGNI[45], PRIVACY BEE[46], DELETE ME[47], etc. Certaines autorités de contrôle se positionnent également comme intermédiaires, comme par exemple l'ICO (autorité britannique), proposant un portail (pédagogique) permettant le dépôt de demandes de droits.

A côté de l'intermédiation, se trouve également l'assistance des personnes concernées dans l'exercice de leurs droits. Ici, les acteurs n'agissent pas pour le compte des personnes concernées : ils n'ont pas pour vocation de déposer les demandes en leur nom, mais plutôt de les alerter, de les assister et de faciliter leurs démarches. En plus des acteurs spécialisés du domaine privée, une telle assistance peut notamment résulter d'une approche collective (via les associations), ou institutionnelle (via, par exemple, les autorités de contrôle comme c'est le cas de la CNIL).

Par ailleurs, certains acteurs peuvent mettre à disposition de leurs utilisateurs des outils visant à rendre visibles les processus de collecte et d'utilisation des données, ce qui renforce

[42] Site web de Mine, consultable via le lien suivant : https://www.saymine.com

[43] Site web de My Data Done Right, consultable via le lien suivant : https://www.mydatadoneright.eu

[44] Site web de Jumbo Privacy, consultable via le lien suivant : https://www.blog.withjumbo.com

[45] Site web d'Incogni, consultable via le lien suivant : https://www.incogni.com

[46] Site web de Privacy Bee, consultable via le lien suivant : https://www.privacybee.com

[47] Site web de Delete Me, consultable via le lien suivant : https://www.joindeleteme.com

le contrôle que vont exercer les personnes concernées sur leur environnement numérique et leur permet de comprendre l'importance que peuvent revêtir leurs droits en matière de protection des données personnelles. C'est par exemple le cas de la société HESTIALABS[48], qui développe plusieurs outils permettant une certaine transparence des publicités ciblées sur le web. A titre d'illustration, un de ses services vise à fournir à l'utilisateur des informations quant aux revenus économiques que les éditeurs tirent de la publicité ciblée (montant de l'attribution/enchère de l'espace publicitaire, annonceurs ayant ciblé l'utilisateur, informations partagées entre l'éditeur et l'annonceur, critères de ciblage utilisés, etc.).

Enfin, l'on peut citer l'UFC QUE CHOISIR, qui a lancé une opération de grande envergure au travers d'une campagne de sensibilisation intitulée « Je ne suis pas une data ». L'association a ainsi mis en place un outil facilitant l'exercice des droits des consommateurs disponible sous le nom « respectemesdatas ».[49] En réalité, cette campagne s'inscrit dans le cadre de la lutte que mène l'association de consommateurs contre le démarchage téléphonique et avait initialement vocation à cibler les principaux opérateurs français afin d'obtenir l'arrêt de la communication des données de leurs clients à des acteurs tiers. Il s'agissait donc de faire pression sur eux en mobilisant les consommateurs.

L'UFC QUE CHOISIR s'est servi de la base de données des organismes ayant désigné un DPO de la CNIL [50] (après un « effort de nettoyage » assez conséquent)[51], afin de dresser une liste de plus de 90.000 responsables du traitement pouvant être ciblés via son portail. Toutefois, le fait qu'une telle démarche contribue à diffuser, auprès du public, la maîtrise des données personnelles et la connaissance des droits RGPD fait débat. Côté DPO, il est compréhensible de ressentir une certaine irritation, par solidarité avec les DPO des organismes concernés (parfois assaillis de demandes). Certains ont même pu percevoir ce dispositif comme une forme « *d'attaque en déni de service »*, visant à « *submerger de manière ciblée* » les opérateurs, soulevant ainsi des interrogations sur son caractère excessif.[52]

---

[48] Site web de la société HestiaLabs, consultable via le lien suivant : https://hestialabs.org

[49] Outil d'assistance des consommateurs dans l'exercice de leurs droits déployé par l'UFC Que Choisir, disponible via le lien suivant : https://respectemesdatas.fr

[50] Base de données OpenCNIL « Organismes avec DPO », consultable via le lien suivant : https://www.data.gouv.fr/fr/datasets/organismes-ayant-designe-un-e-delegue-e-a-la-protection-des-donnees-dpd-dpo/

[51] Propos rapportés par Régis GHOZLAN, DPO et Directeur du département projets de l'UFC Que Choisir

[52] Bruno RASLE, "RGPD : Ils ont inventé la mitrailleuse à demandes de droit d'accès", 24 juin 2024, consultable via le lien suivant : https://www.anaxia-conseil.fr/_web/divers/MitrailleuseDroits-BR-202406.pdf

Il faut toutefois reconnaitre qu'avec 342013 demandes introduites depuis le mois de décembre 2023[53], l'objectif porter les droits RGPD à la connaissance du grand public semble être atteint. D'un autre côté, l'impact de cette campagne interroge : est-ce que les usagers de ce service ont réellement compris de quoi il s'agissait ? Dans la négative, peut-on réellement parler de « maîtrise » ou même de « connaissance » de leurs droits ? Est-ce qu'à travers ce service, le public s'attendait à ne plus faire l'objet d'aucun démarchage téléphonique (démarchage sur lequel les opérateurs n'ont en réalité que très peu de prise) ? Dans ce cas, une certaine déception (voire frustration) pourrait avoir été ressentie. Plus encore, peut être certains utilisateurs ont pu avoir la sensation que, finalement, les droits reconnus par le RGPD sont bien peu utiles. Ainsi, la pertinence d'une telle campagne pour sensibiliser le public peut interroger …

Il n'en demeure pas moins que l'augmentation du nombre d'acteurs proposant des services d'intermédiation (ou d'assistance) des personnes concernées est symptomatique d'un certain nombre d'éléments :

- la complexité des parcours d'exercice des droits : il peut être difficile pour les personnes concernées d'identifier les bons contacts, ou de s'y retrouver dans des procédures trop complexes ;
- la multiplicité des acteurs détenant des données et le manque de transparence (voire parfois l'opacité) de ces derniers ;
- le manque d'information des personnes concernées quant au traitement de leurs demandes d'exercice de droit ;
- le manque de maîtrise, de la part d'un grand nombre d'acteurs, du traitement des demandes de droits.

Or, chacun de ces points représente autant d'opportunités pour le responsable du traitement de capter de la valeur.

Ainsi, au fur et à mesure que le nombre de demandes de droits introduites auprès d'un organisme va augmenter, les coûts engendrés par le traitement de ces dernières seront lissés. Leur amortissement sera alors accéléré.

De la même manière, à mesure que l'opinion publique sera sensibilisée à la protection des données personnelles, l'exercice des droits des personnes concernées se démocratisera. L'attention du public se portera alors de plus en plus sur la manière dont les demandes sont

[53] Chiffre recueilli auprès de Régis GHOZLAN (Directeur Département des Projets et DPO) de l'UFC Que Choisir le 29 décembre 2024

traitées. Cela pourrait ainsi devenir (si ce n'est déjà le cas) un enjeu majeur en termes d'image, de différenciation sur le marché et de développement des affaires.

Au-delà de la dynamique de mise en conformité, une bonne gouvernance des demandes de droits représente donc un moyen pour le responsable du traitement de capter de la valeur et cela au travers de multiples aspects.

## 5. Valorisation du traitement des demandes d'exercice de droits

Partant, il paraît utile de s'attarder sur le terme de « *valeur* », qui peut se rapprocher de la notion de « *prix* », en ce qu'il désigne le « *caractère mesurable (d'un objet) en tant que susceptible d'être échangé, d'être désiré* »[54]. Mais au-delà d'une simple acception économique permettant d'évaluer la contrepartie financière d'un échange, le concept de la valeur s'inscrit également dans une dimension sociologique et englobe aussi bien le « *caractère de ce qui répond aux normes idéales de son type* » que « *ce en quoi une personne [morale] est digne d'estime* ».[55]

Suivant la même logique, la valorisation est le fait de « *faire prendre de la valeur* » à un bien, ou encore d' « *augmenter la valeur reconnue* »[56] d'une personne ou d'une entité.

Considérant ce qui précède, nous entendrons ici par valorisation, la capacité de transformer une logique de mise conformité réglementaire en une dynamique profitable pour une organisation (économique ou non) ; soit comme l'idée de dépasser la réglementation propre au traitement des données personnelles pour en faire émerger des externalités positives.

Ce faisant, nous tenterons tout au long de la présente thèse de démontrer **en quoi le traitement des demandes d'exercice de droit représente, au profit du Responsable de traitement (ou du Sous-traitant), l'opportunité de générer de la valeur.**

Les données représentent des actifs stratégiques d'une organisation et occupent une place centrale au sein de son activité. La gouvernance des données lui permet de s'assurer que les informations sont accessibles, fiables, de qualité et qu'elles sont utilisées de manière éthique et légale. La gouvernance représente donc un enjeu majeur en termes de protection,

[54] Définition du terme « valeur », Dictionnaire Lerobert, consultable via le lien suivant : https://dictionnaire.lerobert.com/definition/valeur

[55] Ibid.

[56] Définition du terme « valoriser », Dictionnaire Lerobert, consultable via le lien suivant : https://dictionnaire.lerobert.com/definition/valoriser

d'optimisation et de développement de l'activité. Une gouvernance efficace repose sur des principes tels que la transparence, la responsabilité, la sécurité et la conformité aux réglementations, la gestion des risques, l'optimisation des capacités organisationnelles. Le propos, ici, est d'aborder de tels principes sous le prisme du traitement des demandes de droits tout en gardant à l'esprit que les solutions envisagées par le responsable du traitement pourront avoir des répercussions positives sur l'ensemble de sa stratégie en matière de gouvernance des données et, plus globalement, sur l'ensemble des domaines de son activité.

**En effet, le responsable du traitement a tout intérêt à rechercher la gestion stratégique et optimisée du traitement des demandes de droit (I) afin de pouvoir mieux se positionner sur le marché et développer son activité (II).**

En raison de la diversité des secteurs d'activité, de la nature et de l'organisation propre à chaque organisme, le présent travail n'a nullement la prétention d'apporter une réponse générale et applicable en toute part à la question de savoir comment valoriser les processus de gestion et de traitement des demandes d'exercice de droits. Il entreprend plutôt, en se basant sur des cas observés ou théoriques, de nourrir une réflexion autour des moyens dont dispose le DPO pour démontrer au responsable du traitement la plus-value que représente cet aspect de la mise en conformité. Il s'agit donc, à travers le prisme de la gestion des demandes de droits, de présenter un certain nombre d'éléments et de solutions - encrés à la fois dans une logique de conformité et de création de valeur - permettant au DPO de « vendre » la conformité et de la rendre profitable à l'ensemble des activités de l'organisation.

**N.B.** : Plus le temps avance, plus la sanctuarisation européenne des données personnelles semble compromise. En effet, dans un contexte de globalisation, où s'entremêlent une concurrence effrénée sur fond de technologisme, des systèmes de valeurs extrêmement diversifiés, ainsi que des dynamiques de régulation pour le moins disparates, il est tentant de penser que les données personnelles ne pourront pas continuer bien longtemps à être exclues du commerce juridique. Le débat portant sur la création d'un droit de propriété sur les données personnelles n'est pas récent mais de nouveaux arguments émergent continuellement. Dans le cas où les données personnelles finiraient par être commercialisables, les droits reconnus aux personnes concernées seraient alors d'une importance capitale pour assurer leur protection dans ce qui pourrait être un « nouveau Far West » de la data. On pourrait alors penser que la gestion de ces droits prendrait, pour les responsables du traitement, une dimension supplémentaire et que les moyens de captation de valeur n'en seraient que démultipliés.

# I. UNE GESTION STRATEGIQUE ET OPTIMISEE DU TRAITEMENT DES DEMANDES DE DROIT …

La construction d'une stratégie et la maîtrise du parcours du traitement des demandes de droits, en plus de contribuer à réduire les risques juridiques, financiers et règlementaires (A), est un préalable nécessaire à l'optimisation du pilotage de ces dernières et à l'accroissement, par le responsable du traitement, de ses capacités organisationnelles (B). Une telle stratégie permet de maximiser la valeur des données pour le responsable du traitement, de minimiser les risques liés à leur utilisation, tout en produisant des bénéfices répercutés sur l'ensemble des opérations et domaines d'activité du responsable de traitement.

## A. Maîtriser le parcours du traitement des demandes de droits : vers une meilleure gestion des risques juridiques, financiers et règlementaires

Le développement qui suit se propose de dessiner un « roadmap » (ou « feuille de route ») constituant le parcours du traitement des demandes de droits composé d'un ensemble d'étapes allant de la réception des demandes (1) à la réponse finale envoyée au demandeur (3) en passant par l'instruction des demandes (2). Pour chacune de ces étapes, un certain nombre de points sont envisagés. Loin d'être exhaustif, les points de frictions et les sources de non-conformité dépendant grandement de la nature et de la réalité propre à chaque responsable du traitement, il envisage un certain nombre d'éléments pouvant orienter la stratégie du DPO en matière de traitement des demandes de droits.

Un tel parcours se doit d'être complété et adapté aux moyens du responsable de traitement, à ses activités, aux personnes concernées et à la diversité des droits qui leur sont reconnus, ainsi qu'aux cadres réglementaires sectoriels applicables, le cas échéant (telles que, par exemple, les spécificités du droit d'accès aux documents administratifs, celles de l'accès aux données de santé, celles couvertes par un secret professionnel, le cadre applicable aux dispositifs d'alerte professionnelles, à la règlementation des activités financières, etc.). L'ensemble de ces points doivent faire l'objet d'une politique interne relative au traitement des demandes de droit, ainsi qu'à la formation des collaborateurs impliqués.

En complément de ce développement, des annexes sont fournies, à toutes fins utiles, afin de proposer des étapes structurant les réflexions du responsable de traitement autour du traitement des demandes d'exercice des droits (**annexe 1**) et plus spécifiquement concernant

les droits d'accès (**annexe 2**), de rectification (**annexe 3**), d'effacement (**annexe 4**), de limitation (**annexe 5**), de portabilité (**annexe 6**) et d'opposition (**annexe 7**).

A titre liminaire, il convient de noter qu'une gestion rigoureuse des demandes de droits limite, entre autres, les risques d'amendes (conséquentes) liées à une mauvaise application du RGPD, de violation de données (par exemple, lorsque la réponse à une demande d'accès est communiquée à une personne non légitime), ainsi que des litiges coûteux et préjudiciables en termes d'image, etc. De plus, un niveau de conformité élevé peut réduire le coût des assurances liées aux risques en matière de cybersécurité et/ou à la responsabilité civile ou règlementaire.

# 1. Parcours du traitement des demandes de droits : réceptionner la demande

Le responsable du traitement doit être en mesure de répondre à la demande dans les délais impartis. La réception de la demande de droit marque ainsi une étape cruciale. Elle implique la mise en œuvre d'une stratégie axée sur un certain nombre de points cardinaux que sont l'identification des canaux de réception et la sensibilisation des collaborateurs (1.1), la remontée interne des demandes (1.2), l'envoi d'un accusé de réception de la demande (1.3). Par ailleurs, une telle stratégie peut être renforcée par une approche basée sur l' « expérience utilisateur » des personnes concernées (1.4).

## 1.1. Identifier les différents points d'entrée de la demande

Afin d'éviter que des demandes ne se « perdent », il est fondamental d'identifier l'ensemble des canaux possibles par lesquels les personnes concernées peuvent les introduire. Une réflexion poussée est donc nécessaire. Comme l'a démontré la sanction infligée par la CNIL au groupe CANAL+[57], il est primordial d'anticiper et d'identifier précisément l'ensemble des points d'entrée possibles (adresses postales, email, les réseaux sociaux du responsable de traitement, etc.).

En effet, une demande peut être introduite par n'importe quel canal. Elle oblige le responsable du traitement quelles que soient ses modalités d'introduction. Seul un nombre réduit d'exceptions peut l'en dégager : lorsque les demandes sont envoyées à des adresses « *aléatoires* », incorrectes, non fournies directement par le responsable du traitement, ou à « *tout moyen de communication qui n'est manifestement pas destiné à recevoir les*

[57] CNIL, Délibération SAN-2023-015 du 12 octobre 2023, consultable via le lien suivant : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000048222771

*demandes »* de droits, dès lors qu'un canal approprié a été fourni[58]. Toutefois, face à l'imprécision de cette grille de lecture, un doute subsiste quant à l'appréciation de la notion des « *moyens de communication manifestement pas destinés à recevoir les demandes* ». Subsiste par exemple la question de savoir si les demandes peuvent être adressées via les réseaux sociaux, même si d'autres points de contact électroniques ont été communiqués à la personne concernée.

En fonction du secteur d'activité du responsable du traitement, cela peut soulever un problème de taille : la personne concernée peut être tentée d'exercer sa demande auprès de son interlocuteur direct (conseiller, service commercial, support, etc.), ou en se déplaçant physiquement dans ses locaux, points de vente, etc. Il sera donc nécessaire pour le responsable du traitement d'identifier toute personne pouvant être amenée à recevoir les demandes de droits des personnes concernées (personnel d'accueil, commerciaux, service client, SAV, etc.). De plus, le CEPD désigne explicitement des "*moyens de communication*", ce qui n'exonère pas le responsable du traitement, quand bien même il aurait communiqué d'autres canaux d'introduction des demandes (électroniques et/ou physiques), d'être en capacité de recevoir les demandes introduites en présentiel. Le cas échéant, il sera donc nécessaire de mettre en place des process permettant le traitement des demandes introduites. Ainsi pourra être mise en place une procédure « guichet » organisant les modalités selon lesquelles la demande devra être reçue, puis remontée vers les services concernés. La sensibilisation et la formation des personnels susceptibles d'entrer en contact avec les demandes de droits sera également nécessaire.

Enfin, le responsable du traitement pourra identifier les canaux qu'il souhaite privilégier et les mettre en avant auprès des personnes concernées (par exemple via la politique de confidentialité et/ou dans les communications qu'il leur envoie). Il devra toutefois prendre garde à ce que de tels canaux n'entravent pas la personne concernée dans sa démarche. De plus, certains canaux pourront s'intégrer au sein d'une solution (technique ou opérationnelle) plus globale, voire automatisée (voir infra : Structurer la gouvernance par la digitalisation et l'automatisation). D'autres pourront être préférés par les personnes concernées car ils facilitent le dépôt et/ou le suivi des demandes, comme l'utilisation d'un QR code (notamment pour les objets connectés), du compte client, d'un tableau de bord digital (voir infra : Tableaux de bord numériques), etc.

[58] CEPD, Lignes directrices sur le droit d'accès du 28 mars 2023, p. 3 et 26

### 1.2. Remontée interne de la demande

Le responsable du traitement doit mettre en place une organisation ainsi que des mécanismes de communication internes permettant la remontée des demandes de droits à l'ensemble des services impliqués. En fonction des demandes introduites, les équipes concernées pourront différer. Il est donc essentiel de pouvoir les identifier à l'avance en tenant compte des spécificités propres à chaque droits et/ou typologies de personnes concernées. Il semble donc nécessaire de matérialiser, au sein du parcours du traitement des demandes, leurs flux en internes, ainsi que les actions spécifiques devant être mises en œuvre.

Par ailleurs, dans le cadre d'une chaîne de traitement (groupe, réseau d'entreprises ou de collectivités, sous-traitants, partenaires, etc.), il convient de prévoir des mécanismes de répartition des rôles et de transfert des demandes afin que l'ensemble des entités impliquées puissent être en mesure de traiter les demandes. Une logique d'automatisation des tâches peut être extrêmement utile au responsable du traitement dans cette tâche (voir infra : Structurer la gouvernance par l'automatisation et l'industrialisation).

### 1.3. Accuser réception de la demande

Afin de faire savoir à la personne concernée que sa demande a bien été reçue et qu'elle sera traitée dans les délais impartis, il semble bienvenu que le responsable du traitement mette en place un système (manuel ou automatique) d'accusés de réception.

S'il ne s'agit pas d'une obligation mise à sa charge, il semble opportun pour le responsable du traitement de recourir à ce type de pratique, que ce soit en termes de relationnel (maintien de la confiance, susciter chez le client le sentiment d'être écouté, etc.), ou encore d'image (montrer le sérieux de l'organisation, son engagement éthique, sa bonne foi en matière de respect des droits, etc.). Une bonne pratique en ce sens consiste à paramétrer des messages automatiques envoyés afin d'accuser réception de la demande, ou en cas de redirection (lorsque la personne à qui elle était initialement adressée est absente).

Par ailleurs, les demandes introduites en présentiel peuvent poser problème. En effet, elles peuvent s'avérer particulièrement difficiles à traiter pour le responsable du traitement. Elles requièrent que celui-ci les ait anticipées et intégrées dans sa stratégie de gestion des demandes, dispose d'un personnel adéquatement formé et, le cas échéant, ait mis en place des mécanismes pour transmettre la demande aux services compétents (voir ci-dessus). Dans le cadre de telles demandes, la personne concernée devrait se voir remis un accusé de réception lorsqu'il est impossible d'y faire droit le jour même.

## 2. Parcours du traitement des demandes de droit : instruire la demande

Toujours dans le respect des délais impartis, le responsable du traitement doit instruire un certain nombre d'éléments relatifs à la demande avant de pouvoir en initier le traitement à proprement parler. Parmi ces éléments à instruire, se retrouvent notamment : l'authentification du demandeur et, le cas échéant, la légitimité du tiers autorisé (2.1), la nature et la recevabilité de la demande (2.2), ainsi que sa portée (2.3).

### 2.1. Authentifier le demandeur

*i) Identifier la personne concernée à l'origine de la demande*

Afin d'éviter toute violation de données (du fait de l'effacement, de la rectification, ou de la communication illégitime de données), le responsable du traitement doit s'assurer que c'est bien la personne concernée qui est à l'origine de la demande et non un tiers (potentiellement malintentionné) cherchant à se faire passer pour elle. La vérification de l'identité n'est pas un prérequis obligatoire au traitement d'une demande de droit. Il n'est en effet pas nécessaire d'y procéder dès lors que le responsable de traitement est certain de l'identité de la personne qui introduit la demande. C'est par exemple le cas d'une demande d'accès effectuée par un collègue de travail que l'on connaît. Cependant, en cas de doute, il incombe au responsable de traitement de procéder à la vérification de l'identité de la personne concernée. Cette vérification peut se faire par tout moyen.

Cependant, le principe de minimisation des données[59] s'applique au dispositif de vérification de l'identité du demandeur. Les moyens déployés pour la vérification de l'identité doivent donc être proportionnés aux données traitées tout en prenant en considération les éventuels dommages pouvant résulter d'une perte de confidentialité des informations ainsi recueillies. A ce titre, la fourniture d'une copie de la pièce d'identité de la personne concernée ne peut, en principe, être exigée de manière systématique. D'autres moyens, moins intrusifs, doivent d'abord être envisagés (par exemple l'utilisation d'une authentification à double facteurs, l'envoi d'un courriel contenant un lien de confirmation, d'un SMS comportant un code de validation, l'utilisation de questions de sécurité, l'authentification via le numéro de contrat ou le numéro de client, la connexion à l'espace client, etc.). De plus, exiger la carte d'identité est contraire au principe de minimisation des données lorsque, notamment, la personne concernée a d'ores et déjà été identifiée dans le cadre de la conclusion d'un contrat. Si aucun autre moyen moins intrusif n'est envisageable, le responsable du traitement informe la

[59] Article 5(1)c du RGPD

personne concernée qu'elle a la possibilité d'obfusquer les informations non nécessaires à son authentification. D'un autre côté, le responsable du traitement doit tout de même tenir compte des cas dans lesquels la loi impose qu'une copie de la pièce d'identité de la personne concernée accompagne sa demande. Par ailleurs, il convient de noter que dans certains États membres de l'Union, demander la copie d'un document d'identité n'est licite que dans certains cas prévus par la législation nationale.

Enfin, lorsqu'il est amené à recevoir des justificatifs, le responsable du traitement doit s'assurer que la communication transite par un canal sécurisé. Il doit également mettre en place les mesures de sécurité adéquates pour encadrer ses communications avec la personne concernée. Enfin, les justificatifs reçus dans le cadre de l'authentification de la personne concernée ne peuvent en aucun cas faire l'objet d'une conservation par le responsable du traitement. Ils doivent être effacés dès lors que la vérification est effectuée.

Il est à noter que dans certains cas de figure, il n'est pas nécessaire (voire impossible) d'exiger de la personne concernée qu'elle ne révèle son identité. C'est par exemple le cas lorsque le responsable du traitement a recours à la pseudonymisation des données (par exemple lorsqu'il utilise un identifiant pour individualiser une personne).



Pour authentifier la personne concernée, le plus simple est encore le mieux. Le responsable du traitement peut ainsi s'appuyer sur des mécanismes existants (connexion à l'espace client, au compte utilisateur, courriel de validation, etc.). Cela lui évitera d'avoir à gérer la vérification de l'identité et de risquer de commettre une erreur pouvant engager sa responsabilité et/ou entacher sa réputation.

*ii) Vérifier la légitimité du tiers demandeur*

Bien que l'exercice des droits soit généralement l'apanage des personne concernées, il demeure possible qu'un tiers formule une demande de droit d'accès en leur nom et pour leur compte. Dans une telle hypothèse, la logique reste inchangée : le responsable du traitement doit vérifier la légitimité du tiers demandeur afin d'éviter toute violation de données potentielle. Parmi les tiers susceptibles d'exercer des demandes de droits pour le compte des personnes concernées se retrouvent, notamment, les représentants légaux agissant au nom des mineurs ou de majeurs incapables et les tiers mandataires (y compris les portails en ligne).

Concernant les demandes exercées pour le compte de mineurs, deux courants de pensées s'affrontent. Si pour certains, les enfants sont des personnes concernées à part entière, pour

d'autres une assistance dans l'exercice de leurs droits est impérative. Le RGPD encourage la sensibilisation des enfants aux droits dont ils disposent sur leurs données personnelles. Il recommande en effet aux responsables de traitement d'adapter l'information à l'âge et au niveau de maturité des publics concernés. Pour sa part, la législation française a confié l'exercice des droits des mineurs aux détenteurs de l'autorité parentale[60]. De son côté, la CNIL adopte une position médiane et indique que *« les mineurs peuvent exercer directement leurs droits sur leurs données personnelles lorsque cette démarche peut être regardée comme un acte courant, notamment si elle correspond à l'intérêt supérieur de l'enfant ».* Ainsi, les enfants peuvent « *exercer directement leurs droits relatifs aux données personnelles sur les réseaux sociaux, les plateformes de jeux et de partage de vidéos ».*[61] En conséquence, peu importe qu'une demande soit introduite par un mineur ou son représentant légal, elle doit être examinée et traitée par le responsable du traitement. Ce dernier aura alors la charge de vérifier la réalité de la détention de l'autorité parentale par le tiers impliqué dans la demande, conformément aux dispositions applicables du code civil.[62] Un raisonnement par analogie peut être adopté pour ce qui concerne les demandes exercées par ou pour le compte des majeurs protégés.

Pour ce qui concerne les demandes exercées par un tiers mandataire, il convient là encore de tenir compte du droit national et, plus particulièrement, des dispositions applicables en matière de représentation légale (mandat ou procuration).[63] La validité d'un mandat est subordonnée à des règles de fond et de forme prévues par le Code civil. Celles-ci ont été complétées par le cadre réglementaire du droit de la protection des données personnelles,[64] ainsi que par les recommandations de la CNIL en matière d'exercice des droits des personnes concernées.[65]

---

[60] Article 70 de la loi Informatique et Libertés, consultable via le lien suivant : https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037823040

[61] CNIL, Recommandation 2 : encourager les mineurs à exercer leurs droits, consultable via le lien suivant : https://www.cnil.fr/fr/recommandation-2-encourager-les-mineurs-exercer-leurs-droits

[62] Articles 371 et suivants C. civ.

[63] Voir : Article 1984 du Code Civil, consultable via le lien suivant : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006445236

[64] Article 77 du décret d'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, consultable via le lien suivant : https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000038568004/2020-10-17

[65] Délibération n° 2021-070 du 27 mai 2021 portant adoption d'une recommandation relative à l'exercice des droits par l'intermédiaire d'un mandataire, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation-2021-070-recommandation-exercice-droits-_mandataire.pdf

De plus, un modèle de mandat type est mis à disposition du public par la CNIL.[66] Le responsable du traitement doit alors être capable de vérifier les conditions de forme (propres à l'exercice des droits RGPD) et de fond (les capacités) encadrant la validité du mandat. A noter, concernant le cas particulier des avocats, qu'en l'absence de dispositions législatives ou règlementaires particulières du droit de la protection des données, il faut revenir au Code de déontologie des avocats, selon lequel toute demande d'accès exercée par un avocat mandaté par son client nécessite la production d'un mandat écrit.[67]

Dans le cas des demandes introduites par le biais de portails en ligne, leur légitimité à agir pour le compte des personnes concernées laisse place à la discussion. En effet, comment peut-elle être vérifiée en l'absence d'un acte de délégation ? Le CEDP indique que le responsable du traitement doit « *toujours traiter cette demande en temps utile* ».[68] Toutefois, dans le cadre de la communication de données, il lui incombe de s'assurer que le portail soit assez sécurisé. S'il juge les mesures de sécurité du portail insuffisantes, il n'est pas tenu d'y verser les données de la personne concernée mais doit envoyer les données directement à la personne concernée. C'est donc au responsable du traitement de déterminer la suffisance de la sécurité d'une technologie qu'il ne maîtrise pas nécessairement…

*iii) Vérifier la légitimité du tiers autorisé*

Dans le cadre du droit d'accès, diverses autorités détiennent, en vertu de dispositions législatives et réglementaires, le pouvoir d'exiger du responsable du traitement la communication de documents ou d'informations. Ces requêtes entraînent souvent la communication de données personnelles par l'organisation. Toutefois, il lui incombe, là encore, de vérifier la légitimé du tiers autorisé à recevoir les données de la personne concernée. Afin d'aider le responsable du traitement, la CNIL a mis en place un guide[69] et un recueil des procédures.[70] Une procédure de communication des données aux tiers autorisés peut-être rédigée afin de formaliser les vérifications à effectuer par les services concernés et les modalités de l'arbitrage à réaliser.

---

[66] Modèle CNIL de mandat type pour l'exercice des droits conférés par le règlement (UE) 2016/678, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/mandat-type_-_exercice_des_droits.pdf

[67] Article 8 du décret n° 2023-552 du 30 juin 2023 portant code de déontologie des avocats, consultable via le lien suivant : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047774060

[68] CEPD, Lignes directrices 01/2022 sur le droit d'accès, p.36

[69] CNIL, Guide pratique "Tiers autorisés", juillet 2020, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/guide_tiers_autorises.pdf

[70] CNIL, Recueil des procédures "Tiers autorisés", juillet 2020, consultable via le lien suivant : Recueil des procédures "tiers autorisés" (cnil.fr)

L'ensemble de ces éléments de vérification doit faire l'objet d'une analyse et d'une réflexion afin d'intégrer la stratégie de l'organisation en matière de gestion des demandes de droits.

### 2.2. Évaluer la nature et la recevabilité de la demande

*i) Analyse du canal d'introduction de la demande*

Dans certains cas restreins, le responsable du traitement peut arguer de l'inadéquation du canal par lequel la demande a été communiquée (voir supra : Identifier les différents points d'entrée de la demande). Il n'est alors pas tenu de traiter la demande. Toutefois, un tel arbitrage nécessite de pouvoir apprécier l'inadéquation du canal. La réflexion menée par le responsable du traitement doit être argumentée et documentée. En cas de refus de répondre à la demande, la personne concernée devra en être notifiée.

*ii) Analyse du caractère abusif de la demande*

Le responsable du traitement doit également évaluer si la demande revêt un caractère abusif (notamment en raison de son caractère répétitif), sans toutefois pouvoir se référer à un guide d'interprétation clair en la matière.[71] Afin d'assurer une certaine constance et de faciliter cette analyse, les modalités de cet arbitrage devraient être définies par l'organisation dans le cadre de sa stratégie de gestion des demandes de droits.

De plus, en présence d'une demande abusive, il faudra pouvoir en déterminer l'issue : donner droit à la demande moyennant le paiement d'un montant raisonnable ou refuser d'y donner droit (et en informer la personne concernée).

*iii) Analyse du champ d'application du droit exercé*

En tenant compte des spécificités liées à la situation de la personne concernée et du régime applicable au droit exercé (voir supra : Rappels des droits, de la portée et des enjeux de ces derniers), le responsable du traitement doit évaluer si la demande est ou non applicable dans le cas d'espèce. Lorsque la demande entre dans le cadre d'une exception ou d'une limitation prévue par la règlementation applicable, il doit également le justifier et le notifier à la personne concernée.

Il convient de rappeler que, dans le cadre du droit d'opposition, le responsable du traitement peut refuser de donner droit à la demande lorsqu'il démontre l'existence d'intérêts légitimes et impérieux à maintenir le traitement, lesdits intérêts prévalant sur les droits et libertés de la

[71] Voir, à titre d'exemple, le point relatif au dispositif "respectemesdatas" mis en œuvre par l'UFC Que Choisir abordé ci-dessus

personne concernée. Il doit alors en faire la démonstration documentée et en informer la personne concernée.

Dans le cadre de certains droits (comme le droit d'accès), la demande peut se fonder sur d'autres dispositions légales que celles du RGPD. Par exemple, la personne concernée peut exercer un droit d'accès relevant de dispositions de droit national (droit d'accès aux données de santé ou aux documents administratifs, par exemple). Les services concernés doivent alors, en tout état de cause, être en mesure de réagir à une telle demande. Par ailleurs, le responsable du traitement doit prendre en compte, le cas échéant, les spécificités des législations locales concernant, notamment, la communication des données.

*iv) Analyse du délai applicable*

A ce stade, le responsable du traitement doit déterminer le délai dans lequel il doit répondre à la demande. En principe le délai de réponse est d'un mois. Toutefois, il peut être prolongé de deux mois supplémentaires en présence de difficultés dans le traitement de la demande (difficultés tenant à sa complexité et/ou du nombre de demandes reçues) et sous réserve d'en notifier la personne concernée.

### 2.3. Évaluer la portée de la demande

*i) Identifier le périmètre des données concernées par la demande*

L'identification du périmètre des données concernées par la demande de droit constitue une étape cruciale pour en assurer un traitement conforme et pertinent. Ce périmètre peut varier en fonction du droit exercé. Le responsable du traitement doit donc, en fonction du droit exercé et du contexte du traitement, identifier les données sur lesquelles une action (effacement, limitation, rectification, etc.) devra être menée, ou celles couvertes par le droit à la portabilité. Dans le cas où il ne serait pas possible de procéder à une telle identification de manière automatique (par exemple via la segmentation des données, l'utilisation de métadonnées, etc.), une expertise juridique pourrait être nécessaire (au cas par cas).

Il est à noter que, dans le cadre d'une demande de rectification, des justificatifs peuvent être demandés à la personne concernée afin que le responsable du traitement soit en mesure de vérifier la véracité de la modification souhaitée (par exemple dans le cadre de données relatives à l'état civil).

Ensuite, le responsable du traitement doit déterminer si les informations visées par la demande entrent bien dans le champ des données personnelles. Il est donc essentiel de vérifier si les données concernées permettent d'identifier ou de singulariser la personne

concernée. Dans le cas contraire, les données peuvent être exclues du périmètre de la demande.

*ii) Respect des droits et libertés des tiers*

De plus, le responsable du traitement doit analyser si le traitement de la demande de droit est susceptible d'affecter des tiers de manière négative. Il doit ainsi s'assurer que la rectification, la suppression ou la communication de données n'entre pas en conflit avec les droits et libertés d'autres personnes (par exemple en privant une tierce personne de l'exécution d'un contrat, en communiquant les données d'un tiers, etc.). Dans ces cas, il est nécessaire de s'assurer que les actions menées en réponse à la demande de droit préservent bien les droits des tiers. Par exemple, dans le cadre d'une demande d'accès ou de portabilité, cela peut impliquer d'obfusquer certaines données pour exclure les informations non nécessaires au traitement de la demande. En effet, la communication de données personnelles à une personne non habilitée à en connaître constitue une violation de données et engage la responsabilité du responsable du traitement.

Toutefois le CEPD a pu indiquer, dans le cadre du droit à la portabilité, que les données de tiers peuvent être transmises lorsqu'elles « *se rapportent également à la personne concernée* ».[72] Cela est particulièrement vrai dans le cas où l'exercice du droit perdrait en substance du fait de l'absence de telles données. Toutefois, le RGPD dispose que le droit à la portabilité ne peut résulter en une atteinte aux droits et libertés de ces mêmes tiers.[73] En pareil cas, un équilibre doit donc être recherché par le responsable du traitement. Ainsi, il pourra organiser en amont la gestion des données de tiers susceptibles d'entrer dans le champ du droit à la portabilité des personnes concernées. Pour ce faire, il peut par exemple structurer sa base de données, segmenter les données, utiliser des métadonnées, prévoir la gestion du consentement des personnes à ce que leurs données soient impliquées dans la portabilité d'un tiers, etc.).

*iii) Conflit avec des droits protégés*

En outre, certaines données peuvent être protégées par des droits spécifiques, tels que le droit de la propriété intellectuelle, la protection du secret des affaires.[74] L'existence de ces droits peut restreindre la portée de certains droits (notamment pour ce qui concerne le droit d'accès, ou le droit à la portabilité). Ainsi, le droit d'accès (tout comme le droit de comprendre

[72] CEPD, Lignes directrices relatives au droit de portabilité du 13 déc. 2016 (WP242), p. 11

[73] Article 20, $4 RGPD

[74] Article 20(4) du RGPD

la logique sous-jacente d'une décision individuelle automatisée), ne peut justifier la communication d'algorithmes protégés par le droit d'auteur ou de détails commerciaux stratégiques couverts par le secret des affaires. Toutefois, ces restrictions ne peuvent être systématiques et abusives. Elles ne peuvent donc pas être prétextées pour refuser toute communication à la personne concernée.[75] Le responsable du traitement doit alors trouver un équilibre entre ces droits spécifiques et le respect des droits reconnus aux personnes concernées. En de pareilles circonstances, l'organisation devra donc procéder à un arbitrage et déterminer les données communicables et celles qui ne le sont pas.

A noter qu'un litige commercial ne constitue pas une restriction légitime aux droits reconnus aux personnes concernées. Par exemple, le responsable du traitement ne peut pas faire valoir une dette en suspens ou un litige commercial pour justifier du refus de faire droit à la demande d'une personne concernée.[76]

*iv) Envisager les intérêts de la personne concernée*

Le responsable du traitement peut orienter sa stratégie de gestion des demandes de droits autour de l'analyse des intérêts et des enjeux que l'exercice des droits représente pour les personnes concernées. Une approche plus centrée sur l'expérience utilisateur permet de mieux anticiper ses attentes et de concevoir des réponses adaptées, claires, exhaustives et, in fine, renforcer sa satisfaction. Par exemple, en identifiant les motivations d'une demande de portabilité des données (transfert vers un nouveau prestataire, utilisation personnelle), le responsable du traitement pourra adapter en conséquence le format des données communiquées et fournir des explications, facilitant leur réutilisation. En adoptant une telle posture proactive, le responsable du traitement est également en mesure de réduire de potentielles frustrations chez les demandeurs en raison de réponses incomplètes ou mal comprises.

Enfin, une meilleure compréhension des objectifs des personnes concernées contribue à mieux appréhender le périmètre de la demande, à optimiser les processus internes et à prioriser les actions à entreprendre en fonction des besoins réels. Bien entendu, il ne s'agit pas ici de limiter la portée de la demande de droit. Ainsi, le responsable du traitement devra s'assurer d'en avoir bien saisi le périmètre. Pour ce faire, il pourra par exemple solliciter la confirmation de la personne concernée.

[75] Considérant 63 RGPD
[76] CEPD, Lignes directrices relatives au droit de portabilité du 13 déc. 2016 (WP242), p. 15

# 3. Parcours du traitement des demandes de droits : répondre à la demande

Après avoir procédé aux vérifications nécessaires afin de s'assurer de la légitimité et de la pertinence de la demande, puis d'en avoir identifié la portée, le responsable du traitement doit y faire droit. C'est-à-dire qu'il doit la « traiter » à proprement parler (3.1). De plus, il va devoir déterminer comment répondre à la personne concernée de manière sécurisée (3.2) et, le cas échéant, déterminer le format des données communiquées (3.3), avant de notifier les destinataires des données (3.4). Enfin, il devra documenter et consigner le traitement de la demande (3.5).

## 3.1. Faire droit à la demande

En plus de devoir procéder aux différentes actions requises en fonction du droit exercé, le responsable du traitement va informer la personne concernée des actions entreprises pour donner suite à sa demande. Ainsi, une réponse doit être formalisée et communiquée. Le responsable du traitement peut ainsi chercher à mettre en place un système de réponses automatisées et personnalisables selon le type de demande.

De plus, la réponse adressée à la personne concernée revêt une importance et une complexité particulière lorsqu'elle fait suite à une demande d'accès ou de portabilité. En effet, en de pareils cas, le responsable du traitement doit fournir une copie des données. Il doit alors veiller à ce que les données transmises soient intelligibles et exploitables par la personne concernée. Une réflexion doit alors être menée quant au format dans lequel les données seront communiquées. Si nécessaire, il doit également expliciter les données « brutes » ou, le cas échéant, les extraits de code.

Enfin et comme abordé plus loin, le responsable du traitement est soumis à une obligation de transparence (Voir infra : Notion de transparence).[77] Celle-ci s'applique également aux informations communiquées aux personnes concernées en réponse à leurs demandes de droits. Dans le cadre de cette obligation et afin d'apporter une information claire mais précise à la personne concernée, le responsable du traitement peut alors adopter une approche à plusieurs niveaux (Voir infra : Véhiculer l'information via des supports accessibles). La granularité et la structure de chacun de ces niveaux peut tenir compte, par exemple, du type de traitement réalisé, des finalités poursuivies, des objectifs de la personne concernée, etc.

[77] Article 5(1)a RGPD

Afin d'enrichir sa gestion des demandes de droits et d'en faciliter le traitement, l'organisation peut chercher à catégoriser les personnes concernées. De cette manière, elle pourra identifier les données propres à chaque catégorie et adapter le parcours de traitement des demandes en fonction.

Le responsable du traitement peut par exemple prévoir des process différents selon que la personne ait souscrit à tel ou tel service, ou encore en fonction de son mode de paiement, de la nature de la relation contractuelle, etc. De cette manière, il peut mettre en place une gestion des demandes de droits plus fine et modulaire, à la fois adaptable aux spécificités de chaque demande, mais aussi ancrée dans un cadre plus global et cohérent.

L'identification et la localisation des données au sein du système d'information du responsable du traitement ne pourra alors qu'être facilitée par la cartographie des données (voir infra : Cartographie des données).

### 3.2. Sécuriser les communications avec la personne concernée

*i) Déterminer le canal de la réponse*

En principe, le responsable du traitement doit privilégier le parallélisme des formes dans la communication de sa réponse à la personne concernée. Il doit donc, en principe et dans la mesure du possible, répondre en utilisant le même canal que celui par lequel la demande a été introduite. Il est toutefois admis que la réponse soit envoyée par la voie numérique, sauf si la personne concernée a expressément demandé la communication de la réponse par un autre canal spécifique.

Par ailleurs, il convient de noter que, dans le cadre de son droit d'accès, la personne concernée doit être en mesure de conserver la copie de ses données. Les données doivent lui être accessibles par la suite (sans toutefois que l'on ne connaisse précisément la durée du maintien d'un tel accès). Le responsable de traitement doit déterminer des modalités de transmission des données respectant l'ensemble de ces conditions.

*ii) Sécuriser les communications*

Vis-à-vis de la personne concernée, le traitement de la demande de droit se solde par l'envoi d'une réponse, ne serait-ce que pour confirmer que les actions requises ont bien été menées. Quelle que soit la demande introduite, une telle réponse est susceptible de contenir

des données personnelles. Par exemple, face à une demande de rectification, la réponse peut confirmer que l'information X a bien été modifiée en Y. De la même manière, la réponse à une demande d'effacement peut mentionner directement les données supprimées (ou renvoyer vers un mail du fil de discussion dans laquelle les données effacées sont explicitement mentionnées). De la même manière, la transmission des données au titre du droit d'accès ou du droit à la portabilité peut également devenir une source de risque de violation de données par perte de confidentialité.

Le responsable du traitement doit donc sécuriser les communications avec la personne concernée. Il lui incombe ainsi de prendre toutes les mesures qui s'imposent afin de garantir la sécurité des communications (par exemple, via le chiffrement de bout en bout, la double authentification, etc.) et de s'assurer qu'elles soient adressées au bon destinataire (par exemple, en utilisant des informations d'authentification fortes).

Par ailleurs, dans le cadre des informations transmises au titre du droit d'accès ou à la portabilité, il incombe à la personne concernée d'assurer la sécurité des données transmises au sein de son propre système d'information. Toutefois, le responsable de traitement doit informer la personne concernée du risque pesant sur ses données afin qu'elle soit en mesure prendre les mesures nécessaires pour protéger les informations reçues.

*iii) Authentification par mandat*

Dans certains cas, le traitement de la demande de droit implique une transmission de données en direction d'un tiers (lui-même alors qualifié de responsable du traitement). Ce sera le cas, notamment, lorsque la demande est introduite par le biais d'un portail en ligne, ou, dans le cadre d'une demande de portabilité en direction d'un autre responsable du traitement. Bien entendu, de telles transmissions doivent faire l'objet d'un niveau de sécurité adéquat. Le CEPD indique qu' « *en cas de transmission directe de données d'un responsable du traitement à un autre, il convient d'utiliser une authentification par mandat, telle que l'authentification par jeton* ».[78]

L'authentification par mandat désigne un processus technique permettant à un tiers mandataire (avocat, représentant légal, plateformes spécialisées, etc.) d'agir pour le compte d'une personne concernée de manière sécurisée et vérifiable à travers des dispositifs électroniques (signature électronique, token, etc.). Tout comme dans un acte de mandat classique, un certain nombre d'éléments sont formalisés au sein du mandat électronique :

[78] CEPD, Lignes directrices relatives au droit à la portabilité des données du 13 décembre 2016 (version révisée du 5 avril 2017), consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp242rev01_fr.pdf

l'identité des parties, la portée du mandat, les droits du mandataire, les conditions de vérification et de validation du mandat, ainsi que les actions que le mandataire peut effectuer. Prenons l'exemple d'une plateforme en ligne de gestion des droits proposant aux personnes concernées de gérer la portabilité de leurs données. Afin de récupérer les données, le « nouveau » responsable du traitement va, avec un mandat électronique, s'adresser à l'interface de cette plateforme. Les données ne pourront lui être transférées avant que la plateforme n'ait vérifié (authentifié) le mandat. Autre exemple : dans le système d'information d'une clinique, un représentant légal (parent ou tuteur) souhaite accéder au dossier médical d'un patient dont il a la charge. Il pourrait le faire à l'aide d'un mandat numérique enregistré dans le système de la clinique en devant alors s'authentifier (via un certificat numérique ou un identifiant unique).

Il s'agit donc d'un moyen de garantir la confidentialité des données transmises qui, au-delà d'intégrer la stratégie du responsable du traitement, implique d'être implémentée par le tiers exerçant la demande de droit. L'authentification par mandat constitue un moyen d'établir la légitimité d'un portail en ligne agissant en tant que « proxy » pour le compte des personnes concernées (voir supra : Vérifier la légitimité du tiers demandeur).

### 3.3. Déterminer le format des données communiquées

Dans le cadre des demandes d'accès et de portabilité, des données personnelles sont amenées à être transmises à la personne concernée. Cela nécessite que le responsable du traitement prenne un certain nombre de dispositions.

Tout d'abord, il doit veiller à opérer une distinction entre le droit à la portabilité des données et les autres droits. Le CEPD recommande en particulier que « *les responsables du traitement expliquent clairement la différence entre les types de données qu'une personne concernée peut recevoir en exerçant son droit d'accès et son droit à la portabilité* ». En plus de fournir une information plus transparente à la personne concernée, cela permet également au responsable du traitement d'éviter de devoir traiter des demandes d'accès (plus lourdes), alors que les objectifs de la personne concernée auraient pu être remplis par le droit à la portabilité.

Ensuite, dans le cadre du droit à la portabilité, le RGPD indique que le responsable du traitement doit chercher à communiquer les données dans un format « interopérable ».[79] L'interopérabilité est définie, dans l'Union européenne, de la manière suivante : « *la capacité de diverses organisations hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus, impliquant le partage d'informations et de*

[79] Considérant 68 RGPD

*connaissances entre elles, selon les processus d'entreprise qu'elles prennent en charge, par l'échange de données entre leurs systèmes TIC respectifs* ».[80] En l'absence de précisions techniques, le responsable du traitement devra décider lui-même du format le plus approprié. Il tiendra alors compte du fait que « *les formats soumis à des contraintes de licences onéreuses ne sont pas considérés comme relevant d'une approche adéquate* ».[81] LE CEPD indique également qu'en l'absence d'autres formats plus adéquats, les formats XML, JSON et CSV sont considérés comme « classiques ».

Pour ce qui concerne les problématiques liées à l'interopérabilité des données, le responsable du traitement peut se référer, notamment, au Référentiel Général d'Interopérabilité (RGI)[82] ou à la brochure sur le cadre européen de l'interopérabilité.[83] A noter qu'un projet de règlement européen pour une Europe interopérable est actuellement en cours de discussion au sein des instances de l'Union.[84]

Enfin et lorsqu'il existe, dans le cadre de la portabilité, des échanges réguliers de données entre plusieurs responsables du traitement, ces derniers peuvent rechercher des moyens communs de synchronisation. En effet, de tels moyens, en plus de garantir la confidentialité des données et de réduire les coûts impliqués par une multitude de communications, leur permettraient de respecter leur obligation de mettre à jour les données.[85]

### 3.4. Notifier les destinataires des données

Le RGPD oblige le responsable du traitement à communiquer « *toute rectification, effacement ou limitation du traitement aux destinataire auxquels les données ont été*

[80] Article 2 de la décision n° 922/2009/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant des solutions d'interopérabilité pour les administrations publiques européennes, p.20, consultable via le lien suivant : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32009D0922

[81] Ibid.

[82] Référentiel général d'interopérabilité du 12 janvier 2016 (version du 18 décembre 2020), consultable via le lien suivant : https://www.numerique.gouv.fr/uploads/Referentiel_General_Interoperabilite_V2.pdf

[83] Commission européenne, New European Interoperability Framework, 2017, consultable via le lien suivant : https://ec.europa.eu/isa2/sites/default/files/eif_brochure_final.pdf

[84] Voir Communication du Conseil européen sur le règlement pour une Europe interopérable en date du 13 novembre 2023, consultable via le lien suivant : https://www.consilium.europa.eu/fr/press/press-releases/2023/11/13/interoperable-europe-act-council-and-parliament-strike-a-deal-for-more-efficient-digital-public-services-across-the-eu/

[85] Article 5(1)d RGPD

*communiquées* ».[86] Celui-ci est donc dans l'obligation de notifier de telles actions à l'ensemble de la chaîne de traitement. Cela permet d'assurer l'effectivité des mesures entreprises (en les répercutant sur chacun des maillons) sans que la personne concernée n'ait besoin d'exercer ses droits auprès d'une multitude d'entités.

Afin de s'assurer du respect de cette obligation, le responsable du traitement doit être en capacité de savoir exactement où se trouvent les données impliquées (et donc à qui elles ont été transmises). Il doit donc être capable d'identifier l'ensemble des destinataires (partenaires, sous-traitants, autorités publiques ou tout autre organisme public, etc.). Pour ce faire, une cartographie des données paraît pertinente, voire nécessaire (Voir infra : Cartographie des données). Cette obligation de notification s'applique également lorsque les données sont transférées au sein d'un même groupe, ce qui peut engendrer des coûts de traitement superflus lorsqu'une gestion globale et unifiée des demandes de droit n'a pas été mise en place (voir infra : Optimiser les capacités de gestion et d'organisation).

### 3.5. Documenter et consigner la demande

Au titre de l'obligation de responsabilité (principe d'accountability) que le RGPD met à sa charge,[87] le responsable du traitement doit être en mesure de démontrer à tout moment la conformité de ses pratiques. Il doit donc être capable de démontrer que chacune des demandes de droits a été traitée dans le respect de la règlementation applicable en matière de protection des données personnelles.

Ainsi les demandes (comme les réponses qui y ont été apportées) doivent être consignées au sein d'un registre tenu (par le DPO). Aucune indication n'est mentionnée quant à la durée de conservation des informations reportées dans un tel registre. Le responsable du traitement doit toutefois trouver un compromis entre le respect des droits et libertés des personnes et son obligation d'accountability. D'aucuns estiment que la limitation des accès à un tel fichier (DPO, service juridique, direction générale, etc.) et l'intérêt qu'il représente en termes juridiques et réglementaires, le place dans la catégorie de l'archivage intermédiaire.

## B. Consolider le pilotage du traitement des demandes de droits : vers une meilleure gestion de ses capacités organisationnelles

Le responsable du traitement peut utilement chercher à mettre en place différents outils dédiés à la gestion des demandes de droits afin d'améliorer l'efficacité de leur traitement et

[86] Article 19 RGPD

[87] Article 5(2) RGPD

d'en réduire les coûts opérationnels. Certes, l'implémentation de telles solutions soit conditionnée par les moyens du responsable du traitement et dépendent de son activité ainsi que de son système d'exploitation. Mais celles-ci ont l'avantage d'engendrer des répercussions positives dans de nombreux domaines opérationnels, en dehors de la seule conformité RGPD. L'organisation va alors pouvoir mesurer ces gains et anticiper leur amortissement dans le temps.

Parmi ces moyens, deux ensembles peuvent être distingués (bien qu'en réalité, ils puissent être inextricablement liés) : les outils de gouvernance en matière de données, via la digitalisation et l'automatisation des tâches (1) et les solutions portant sur les capacités de gestion et d'organisation (2).

## 1. Structurer la gouvernance par la digitalisation et l'automatisation

En effet, une approche axée autour de la digitalisation et de l'automatisation des tâches permet non seulement de se conformer aux exigences réglementaires, mais également de maximiser la valeur des données (notamment en garantissant leur fiabilité et leur disponibilité pour les équipes métiers). En outre, l'automatisation et la digitalisation ne se contentent pas d'améliorer l'efficacité de la gouvernance des données. Elles ouvrent la voie à une approche plus stratégique et proactive de la gestion de l'information, en démultipliant les capacités organisationnelles du responsable du traitement.

La gouvernance des données est un ensemble structuré de principes, de politiques, de processus et d'outils visant à garantir une gestion efficace, sécurisée et conforme du patrimoine informationnel d'une organisation. La gouvernance des données repose sur plusieurs piliers, notamment la qualité des données, la sécurité, la confidentialité et la conformité réglementaire.

En parallèle, l'automatisation et la digitalisation transforment et enrichissent profondément la gouvernance des données. Elles accroissent les capacités de gestion et de contrôle bien au-delà de ce qui peut être mis en œuvre manuellement. De plus, les solutions numériques permettent l'application systématique de règles de gouvernance à grande échelle. Ces technologies permettent donc de transformer radicalement la manière dont les organisations gèrent, contrôlent et valorisent leurs données. En effet, la digitalisation renforce la gouvernance en centralisant les données dans des écosystèmes interconnectés et accessibles, tout en appliquant des règles uniformes. De même, l'automatisation permet au responsable du traitement non seulement d'améliorer son efficacité, mais aussi de réduire

significativement le risque d'erreurs humaines, tout en libérant les équipes pour des tâches à plus forte valeur ajoutée.

Il s'agit alors pour le responsable du traitement de se doter d'outils techniques qui, ensembles, assurent une gestion cohérente et maîtrisée de l'information au sein de l'organisation. Par exemple, la stratégie de gestion des demandes de droits peut intégrer des outils de gestion avancés. Ainsi, la segmentation des données (incluant l'utilisation de métadonnées) (1.1) sert de fondation pour permettre de décrire les données et alimenter leur cartographie (1.2). Une telle cartographie constitue elle-même une base pour mettre en place une automatisation des tâches pouvant s'inscrire dans le cadre de l'industrialisation du traitement des demandes de droits (1.3).

Ainsi, la digitalisation peut, au travers d'un ensemble d'outils, créer de la valeur pour le responsable du traitement, depuis le renforcement de la conformité, de la sécurité et de la gouvernance des données, jusqu'aux gains opérationnels et à l'amélioration de la satisfaction client. Toutefois, les solutions technologiques ne sont aptes à produire des effets que si elles sont adoptées et maîtrisées par les collaborateurs. Le responsable du traitement peut donc utilement renforcer sa stratégie de digitalisation et d'automatisation en déployant des moyens autour de la conduite du changement et de la formation des équipes métiers.

Enfin, l'implémentation de ces outils peut représenter un certain coût pour le responsable du traitement. Ces coûts pourront être légitimés (et acceptés) plus aisément lorsqu'il sera possible de démontrer un retour sur investissement (économie de temps, maîtrise des risques, diminution des erreurs dues aux opérations manuelles, etc.) et la génération de bénéfices transverses pour l'organisation (qualité des données accrue, amélioration de la relation client, analyse stratégique, etc.).

### 1.1. Segmentation des données et utilisation des métadonnées

La gestion efficace des demandes de droits nécessite, au préalable, l'identification des données concernées par tel ou tel droit. Il est ainsi opportun de procéder à la segmentation des données et de recourir, pour ce faire, à l'utilisation de métadonnées.

*i) Segmentation des données*

La segmentation des données consiste à regrouper les informations en catégories (ou « *segments* ») et sous-ensembles distincts afin de faciliter leur traitement. Un tel regroupement peut s'axer autour de différents critères attachés à la donnée elle-même, tels que :

- **sa typologie** (donnée d'identification, donnée analytique, donnée financière, donnée comportementale, donnée technique, etc.) ;
- **sa source** (donnée directement fournie par la personne concernée, donnée obtenue par un tiers, donnée générée par l'utilisation d'un service, etc.) ;
- **sa sensibilité** (donnée personnelle, donnée relevant d'une catégorie particulière au sens de l'article 9 du RGPD, donnée à faible/fort impact, secret d'affaire, etc.) ;
- **son utilité métier** (donnée client, donnée RH, donnée produit, etc.) et/ou la finalité des traitements dans laquelle elle est employée (gestion contractuelle, marketing, gestion de la facturation, etc.) ;
- **son cycle de vie** (durée de conservation applicable, donnée active, donnée archivée, donné utilisée dans le cadre de tel ou tel traitement, etc.) ;
- **le type de droit RGPD dont elle peut faire l'objet** (donnée couverte par le droit à la portabilité, donnée entrant dans le cadre d'une prise de décision individuelle automatisée, donnée pouvant faire l'objet d'une demande d'effacement/d'opposition/de limitation, etc.).

La segmentation permet notamment, d'identifier rapidement des données spécifiques ; de réduire et de contrôler les risques (par exemple en limitant l'accès à certaines catégorie ou sous-ensemble aux seules personnes, ou systèmes, en ayant besoin) ; de répondre à des besoins de traitement spécifiques (en fonction par exemple de finalités marketing, de gestion des contrats, de conformité, etc.), et d'améliorer les réponses fournies aux demandes de droits et d'en réduire les coûts de traitement. L'objectif est ici d'accroître les capacités du responsable du traitement en termes de gestion et de gouvernance des données (par des données plus compréhensibles, plus sécurisées et plus facilement exploitables par les équipes métiers).

Par exemple, à l'intérieur de catégories distinctes (telles que les « données clients » et « données prospects »), une entreprise a découpé sa base de données en sous-ensembles en fonction de la zone géographique concernée, de l'âge, des intérêts des personnes pour tel ou tel produit, etc. Elle souhaite réaliser une campagne de marketing ciblé. Grâce à une segmentation des données sur plusieurs niveaux, l'entreprise sera capable d'adapter le traitement opéré selon que les personnes ciblées soient des clients ou des prospects, des particuliers ou des professionnels, majeures ou mineures, qu'elles habitent à Paris ou dans les territoires, etc. Cela lui permet de rationaliser et d'optimiser l'efficacité de la campagne, tout en facilitant la gestion des aspects liés à la conformité RGPD du traitement. En effet, le traitement des demandes de droit sera optimisé (par exemple, via des parcours différents selon les particularités propres à chaque personne concernée).

La segmentation des données emporte donc, pour l'organisation, la capacité d'adapter – à un niveau très fin - sa stratégie de gestion des demandes de droits (et les processus de traitement des demandes) en fonction des particularités propres à chacun des segments des personnes concernées. Plus les données sont segmentées et décrites de manière cohérente, plus il devient facile d'en exploiter la valeur et de développer de nouveaux services ou d'optimiser les traitements à forte valeur ajoutée. La segmentation permet également au responsable du traitement de se conformer aux exigences légales d'une manière simplifiée et plus efficace.

*ii) Utilisation de métadonnées*

Dans la mesure où la segmentation repose sur une classification des données, un référentiel ou « langage » commun à l'ensemble des métiers de l'organisation est nécessaire. En tant qu' « information sur l'information », les métadonnées (champs de classification, tags, labels, etc.) peuvent être utilisées en ce sens. Les métadonnées constituent des « étiquettes » apposées sur des données. Elles peuvent ainsi être employées pour décrire et qualifier chaque ensemble ou sous-ensemble de la segmentation, voire certaines données de manière spécifique. Les métadonnées peuvent donc venir s'attacher aux données pertinentes en fonction des critères de la segmentation.

Dans une logique d'automatisation, des solutions d'analyse automatique peuvent être utilisées pour identifier la nature d'un document ou d'une information et lui attribuer des métadonnées pertinentes en toute autonomie et sans qu'une intervention humaine ne soit nécessaire. Cela permet d'accélérer le processus de reconnaissance, de réduire les ressources temps-homme allouées et d'éviter les erreurs humaines (et le risque d'oubli). Une telle solution peut par exemple consister en la recherche, au sein de documents numérisés, de mots clés, de chaines de caractères (nom, prénom, adresse email, etc.) / de numéros (carte bleu, NIR, numéro de téléphone, etc.) …

Combinée à l'usage de métadonnées fiables et pertinentes, la segmentation constitue alors un levier essentiel pour gérer efficacement les demandes de droits, en réduire les délais de traitement et les ressources qui y sont employées. En ce sens, elle permet notamment :

- D'identifier les données concernées par la demande d'une manière plus précise et efficace (il n'est donc pas besoin de les rechercher manuellement) ;
- De distinguer les données personnelles d'autres informations ne relevant pas du RGPD, ou faisant l'objet d'autres droits protégés (droit de propriété intellectuelle, secret des affaires, etc.) ;

- D’identifier et d’exclure plus aisément les données qui pourraient entrer en conflit avec les droits de tiers ;
- De répondre de manière plus rapide et moins coûteuse aux demandes.

Enfin, une segmentation stratégique favorise la mise en place de processus et de tâches automatisés. Par exemple, le responsable du traitement pourrait mettre en place des règles de purge automatique ciblant les données pertinentes au regard des spécificités propre à différentes catégories de personnes concernées. De la même manière, il peut définir des règles de routage en fonction des différentes catégories.

La segmentation des donnés contribue donc à l'efficience globale de l'organisation. Elle représente, notamment, les avantages suivants :

- Favoriser la création de valeur : mieux exploiter les données et développer/optimiser des services à forte valeur ajoutée.
- Augmenter la réactivité et l'efficacité des processus métiers.
- Faciliter la mise en conformité et le respect des exigences légales (principe de minimisation, conservation des données, etc.).
- Traiter efficacement les demandes de droits tout en réduisant les ressources qui y sont employées (identifier les données concernées, paramétrer les actions à entreprendre en fonction du droit exercé et du contexte du traitement, personnaliser les réponses, etc.)
- Optimiser la sécurité des données : sécuriser les données en fonction de leur sensibilité et des besoins spécifiques du traitement.

### 1.2. Outils de cartographie

Les outils de cartographie se positionnent au centre de la gouvernance des données. Ils visent à assurer une visibilité en temps réel sur l'ensemble du cycle de vie des données, facilitant ainsi la conformité réglementaire et la prise de décisions éclairées (notamment dans le cadre du traitement des demandes de droits).

Ainsi, la gestion efficace des demandes de droits requiert une cartographie claire de la localisation des données au sein du système d'information du responsable du traitement (et de leurs flux). En effet, répondre à une demande de droit nécessite de savoir où se situent les données personnelles et comment elles sont reliées entre elles : le responsable du traitement

doit être capable d'identifier les modalités selon lesquelles les données sont stockées, traitées ou transférées.

Outre les outils spécialisés, la cartographie peut également passer par des outils généralistes « maison » (fichier Excel, tableaux collaboratifs, Mindmap, etc.). Si ces derniers sont faciles d'accès et peu coûteux, ils représentent toutefois des risques de duplication et de non-actualisation qu'il faudra, le cas échéant, surveiller.

*i) Cartographie des logiciels*

La cartographie des logiciels consiste à répertorier l'ensemble des logiciels, applications et services informatiques utilisés par l'organisation. Au-delà du simple inventaire, la cartographie intègre la description et la documentation des caractéristiques de chacun d'entre eux, de leurs finalités, périmètres, dépendances et des éventuels risques qu'ils peuvent représenter. Parmi ces logiciels figurent notamment le CRM (gestion de la relation client), l'ERP (gestion comptable et/ou logistique), le SIRH (pour la gestion des Ressources Humaines), les outils d'emailing (pour la communication et les campagnes marketing), etc. Ces outils sont rarement autonomes et peuvent être interconnectés dans le cadre de processus métiers et d'un partage de données.

Par l'inventaire, la cartographie permet d'identifier les logiciels utilisés par les collaborateurs, qu'ils soient autorisés par l'organisation ou non. En effet, dans un environnement informatique complexe et face à l'essor de solutions libres et/ou gratuites, la pratique du « *Shadow IT* » (notion renvoyant à des applications non validées par l'organisation) peut représenter un risque auquel le responsable du traitement se doit de remédier.

De plus, la cartographie aide à gérer le parc applicatif (nombre d'applications, obsolescence et/ou redondances des solutions logicielles, maîtrise des coûts de maintenance et des licences, etc.). Elle participe également à sécuriser l'architecture du système d'information et à faciliter la prise de décision (choix de solutions informatiques, migration, transition numérique, etc.). La cartographie permet aussi d'orienter la stratégie informatique de l'organisation en fonction des besoins réels et des priorités des équipes métiers. Sur le plan de la conformité RGPD, la cartographie des logiciels permet de vérifier que les solutions utilisées par le responsable du traitement se conforment à la règlementation applicable.

La cartographie des logiciels et applications passe par un certain nombre d'étapes, dont notamment :

- **Le recensement**, impliquant que chacune des équipes métiers identifie les solutions utilisées. Des outils d'analyse spécialisés peuvent également améliorer et approfondir

l'inventaire. Dans un premier temps, les efforts peuvent être priorisés autour des logiciels critiques pour l'activité de l'organisation.

- **La documentation**, impliquant de rassembler des informations pertinentes sur l'ensemble des solutions répertoriées (notamment leur finalités, périmètres fonctionnels, modes d'hébergement, risques et dépendances, etc.). Le niveau de risque (ou de sensibilité) peut ainsi permettre d'identifier les applications critiques pour l'activité d'un métier et celles relevant plutôt de fonctions support.
- **La modélisation visuelle**, pour représenter l'inventaire et matérialiser les liens qu'entretiennent les solutions logicielles les unes avec les autres. Ces dernières peuvent utilement être regroupées par domaine fonctionnel (finance, RH, marketing, etc.).
- **La mise à jour**, impliquant de savoir selon quelles modalités des applications pourront être ajoutées ou retirées de l'inventaire. Une procédure de gestion des logiciels et applications peut ainsi utilement indiquer quelles personnes devront être impliquées lorsqu'une nouvelle solution informatique est envisagée (afin, par exemple, de vérifier si des données personnelles sont impliquées, d'analyser les risques qu'elle représente, sa pertinence, etc.).

*ii) Cartographie des données*

Une couche supplémentaire peut être ajoutée à la cartographie des logiciels : la cartographie des données. Davantage focalisée sur les actifs informationnels de l'organisation, celle-ci s'applique à inventorier les données et à déterminer où (sur quels serveurs, dans quelles bases de données, au sein de quels fichiers, etc.) et comment (sous quels formats, quelle structure et selon quelles règles) les données sont stockées au sein du système d'information. En ce sens, la cartographie des données met l'accent sur l'aspect « statique » de l'information en s'attachant à démontrer comment les données sont organisées, classées et segmentées (voir supra : Segmentation des données et utilisation des métadonnées). Il s'agit d'un outil essentiel dans le cadre de la conformité et de la gouvernance des données (notamment pour la gestion des demandes de droits) puisqu'elle permet de localiser précisément l'information en fonction de sa nature, de sa fonction et de sa typologie.

La cartographie des données s'appuie sur la cartographie des logiciels et applications. Elle passe par un certain nombre d'étapes, dont notamment :

- **La localisation des données** au sein du parc applicatif. Il est important de consulter les équipes métiers, qui traitent quotidiennement les données dans le cadre de leurs

activités. Cela permet de ne pas passer à côté d'emplacements « moins évidents » (fichiers Excel, poste de travail, stockage en cloud, type Google Drive, etc.).

- **L'identification du périmètre fonctionnel des données**.
- **La description des données**, via la collecte d'un certain nombre de renseignements pertinents (propriété, règles de conservation, sécurité, sauvegardes, etc.). En ce sens, la cartographie peut également s'avérer très utile pour construire et mettre à jour le registre des traitements, mais également pour réaliser des analyses d'impact sur la protection des données.
- **La représentation visuelle** des données au sein du système d'information et des intrications qu'elles entretiennent entre elles.
- **La mise à jour** impliquant, lorsqu'un nouveau traitement (ou la modification d'un traitement existant) est envisagé, de déterminer quelles personnes doivent être consultées et, le cas échéant, quelles règles devront être modifiées. Une procédure de gestion des nouveaux projets peut utilement être mise en place en ce sens.

Il est important de noter que la cartographie doit s'attacher au cycle de vie complet des données. En effet, un tel exercice nécessite d'envisager la donnée personnelle depuis sa collecte jusqu'à sa destruction (ou son effacement), en passant par l'utilisation qui en est faite par les équipes métiers, ainsi que son stockage (et éventuellement son archivage).

Pour résumer, l'objectif de la cartographie des données est donc de visualiser la localisation des données au sein des systèmes d'information du responsable du traitement. Elle vise à répertorier certaines caractéristiques propres à l'information, comme le format, la sensibilité et l'accès, les règles de conservation (durées, formats, supports, etc.), … Il s'agit de fournir un référentiel utile pour la gouvernance des données (conformité, sécurité, qualité, analyse, etc.). La cartographie permet également de repérer des redondances, des incohérences et d'accompagner la stratégie déployée autour de la qualité des données. En somme, elle représente pour l'organisation l'opportunité d'accroître la connaissance de ses actifs informationnels et de les valoriser.

De plus, la cartographie des données constitue un prérequis indispensable pour permettre à l'organisation de traiter les demandes de droits de manière efficace. En effet, cela nécessite de savoir où les données se trouvent, comment elles sont reliées entre elles et qui peut valider les actions à entreprendre en ce qui les concerne. Elle permet ainsi de réduire les coûts de traitement des demandes en accélérant l'identification et la recherche des données, tout en diminuant le risque de laisser des « trous dans la raquette ».

*iii) Cartographie des flux de données*

Pour une approche encore plus complète de la cartographie, celle-ci peut venir s'inscrire dans une approche « *dynamique* ». Ainsi, en complément de la cartographie des données, l'organisation peut chercher à identifier leurs flux, d'un point A vers un point B ; au sein de son système d'information, ainsi qu'à l'extérieur de celui-ci. Il s'agira alors de déterminer comment (et à quelle fréquence) les données circulent entre les différents systèmes, applications, services, etc.

Par exemple, un flux peut s'articuler de la manière suivante : dans le cadre d'un traitement ayant pour finalité d'analyser les achats réalisés par les clients, les données issues du CRM (point A - plateforme de gestion de la relation client) sont envoyées vers la solution d'analytique (point C - permettant de rassembler des données pour en extraire des informations utiles à l'optimisation des activités), en passant au préalable par l'outil de « *marketing automation* » (Point B - permettant d'automatiser des tâches marketing répétitives).

La cartographie des flux représente donc l'ensemble des étapes par lesquelles passent les données dans le cadre de leur traitement. Elle permet de prendre conscience d'étapes superflues ou manquantes, ou encore de risques d'erreurs et/ou de perte de données (par exemple lorsqu'il existe un flux manuel via un fichier Excel). De plus, chaque fois que la donnée est transférée, des risques peuvent exister en termes confidentialité et de sécurité. C'est notamment le cas lorsqu'un transfert est réalisé vers un partenaire/prestataire sans qu'un contrat ne formalise les relations qu'il entretient avec le responsable du traitement. C'est également le cas lorsque les données sont transférées en dehors du territoire de l'Union européenne. Il s'agit donc d'une couche supplémentaire dans la maîtrise des risques permettant d'identifier les risques et les mesures de sécurité et garanties à y apporter.

La cartographie des flux de données présente ainsi l'intérêt de pouvoir repérer rapidement l'ensemble des acteurs impliqués dans le traitement d'une (catégorie de) donnée. Elle permet donc à l'organisation de traiter de manière efficiente les demandes de droit et, dans le cadre de la rectification et de l'effacement de données et de l'opposition ou de la limitation d'un traitement, d'accomplir son obligation de notifier l'ensemble des destinataires des données concernées.

La cartographie des flux de données s'appuie sur la cartographie des données et passe par un certain nombre d'étapes, dont notamment :

- **Le recensement des flux de données** au sein du système d'information et à l'extérieur de celui-ci. Il est important de consulter les équipes métiers afin d'explorer

les différentes interfaces qu'elles utilisent quotidiennement et les liens existants entre celles-ci.

- **La description des flux** : répertoriant l'origine, la destination, la nature et la sensibilité des données, ainsi que les protocoles modalités et fréquences de leurs transferts.
- **La représentation visuelle des flux** au sein du système d'information et vers d'autres maillons de la chaîne de traitement.
- **La documentation du niveau d'automatisation des transferts** de données (par exemple API, transfert manuel par mail, par copier-coller depuis un fichier Excel, par exportation d'un fichier ou d'une base de données, etc.).
- **La mise à jour** impliquant, dès lors qu'une nouvelle solution logicielle ou qu'un nouveau transfert de données est envisagé, de savoir quelles personnes doivent intégrer le processus de décision.

La cartographie des flux de données peut donc produire un ensemble de bénéfices pour l'organisation tout en lui assurant une visibilité globale sur l'ensemble de son système d'information et sur les flux de données qui s'y déroulent. Elle accroît également la maîtrise de la chaîne du traitement et des transferts de données personnelles à l'extérieur de l'organisation. De plus, l'analyse des flux et les mécanismes de monitoring permettent le suivi des transferts en temps réel et la détection d'anomalies.

Enfin, la cartographie des flux de données génère une certaine capacité à préparer l'automation des tâches (notamment pour ce qui concerne le traitement des demandes de droits). En effet, connaître précisément les données (et leurs flux), les différents acteurs (et destinataires), ainsi que l'ensemble des logiciels et applications impliqués, permet de mettre en place des workflows automatisés de façon rapide et fiable. Ainsi, la connaissance des flux permet d'orienter l'automatisation : on repère les flux redondants ou manuels pour les automatiser (Voir infra : Automatisation : vers l'industrialisation du traitement des demandes de droits).

*iv) Data lineage*

Une approche encore plus poussée du recensement des données se formalise autour de la notion de « data lineage ». Cette approche consiste, en plus d'identifier les données détenues par l'organisation (et leurs flux), à détailler leur parcours au sein des systèmes tout au long du cycle de vie de la donnée. Il s'agit ici de retracer l'historique complet des transformations subies par la donnée. La cartographie des flux de données est alors un intermédiaire entre la cartographie « statique » des données et le « data lineage ».

Le « data lineage » permet de mieux comprendre l'évolution des données ; non seulement leurs flux, mais aussi les étapes et procédés de transformation (nettoyage, enrichissement, structuration, pseudonymisation/anonymisation, etc.), ainsi que les conditions de la mise en œuvre de ces procédés et les différents acteurs impliqués. Cela permet également de mesurer les implications que pourront avoir les changements opérés sur une base de données (ou encore au niveau d'un logiciel ou d'une application) et d'être plus réactif dans la mise en place des actions adéquates (notamment dans le cadre du traitement des demandes de droits).

### 1.3. Automatisation : vers l'industrialisation du traitement des demandes de droits

Face à l'implication croissante qu'occupent les données personnelles dans les activités des organisations et à la multiplication des services numériques, le nombre des sources et des traitements de données personnelles augmente fortement. La complexité croissante des systèmes d'information, la pression réglementaire et l'augmentation des demandes de droits imposent l'adoption d'une gouvernance solide et de stratégies de gestion réfléchies. Un tel contexte encourage également les responsables du traitement à privilégier l'automatisation des tâches plutôt qu'une gestion manuelle, plus laborieuse et sujette aux erreurs humaines.

Au-delà de la simple conformité, fluidifier le traitement des demandes de droits devient alors un réel enjeu concurrentiel. Cela peut permettre l'économie de ressources pouvant être mieux employées ailleurs tout en améliorant l'efficacité du traitement des demandes de droits (et ainsi que la satisfaction et la confiance des clients/utilisateurs).

Cependant l'automatisation du traitement des demandes de droit ne saurait se réduire au déploiement de solutions ou d'outils techniques. Elle s'inscrit au sein d'une stratégie plus globale et s'intègre pleinement dans la gouvernance des données. Ainsi, il est essentiel de définir les rôles et responsabilités, Dans le cadre de la prise de décision autour des solutions à déployer (prioriser, allouer les ressources, mesurer l'efficacité, etc.), il convient de déterminer qui va décider, qui va valider, qui va contrôler. Pour ce qui est de l'automatisation des actions entreprises dans le cadre du traitement des demandes de droits, il est nécessaire de savoir qui va valider le respect de la règlementation, qui va s'assurer que les règles d'effacement ou rectification sont bien définies et appliquées, qui va contrôler les outils (et selon quelle fréquence), etc. Il est également crucial de souligner que les métiers doivent être en mesure de prendre en main les solutions mises à leur disposition : la conduite du changement et la formation des équipes sont donc primordiales. Enfin, pour certaines organisations, la mise en place d'une gestion automatisée des tâches en matière de conformité peut être appréhendée comme un tremplin vers une transformation digitale plus large.

Il s'agit donc, au travers des solutions d'automatisation et d'industrialisation, de rechercher le même triptyque que dans le cadre de la cartographie ou de la segmentation : conformité, efficience (interne et transverse) et valorisation des données.

Dans la logique d'une industrialisation du traitement des demandes de droit, un certain nombre de solutions techniques coexistent. S'y retrouvent notamment les API (qui permettent une communication fluide et directe entre les bases de données, systèmes et applications), ainsi que les workflows (qui orchestrent l'ensemble des étapes d'un processus). D'autres solutions existent par ailleurs et peuvent s'avérer intéressantes en fonction des besoins et de la situation propre à chaque responsable du traitement.

*i) API : centraliser la gestion des demandes*

Une interface de programmation d'application (« *Application Programming Interface* » ou API) est un ensemble de définitions et de protocoles permettant à différents logiciels et/ou systèmes de communiquer entre eux. L'API sert d'interface pour permettre à un site web, une application, un logiciel d'envoyer des requêtes à un système ou une base de données tiers. À titre d'illustration, une analogie peut être faite avec les annuaires téléphoniques.[88] Un annuaire téléphonique permet à une personne de téléphoner à une autre pour lui demander des informations. Dans le contexte du numérique, une API joue le même rôle. Le téléphone est remplacé par des protocoles et les personnes par des systèmes, des logiciels, des applications, etc.

L'API peut ainsi connecter les outils numériques de l'organisme afin de centraliser et d'automatiser la gestion de certaines tâches et/ou flux de données. Bien que complexe, l'intégration peut ainsi permettre d'automatiser efficacement la gestion d'un grand nombre de tâches et de les appliquer sur un ensemble de systèmes interconnectés (donc potentiellement sur l'ensemble du système d'information de l'organisation). Elle nécessite toutefois une planification minutieuse et une collaboration étroite entre les différentes équipes impliquées.

Par ailleurs, une API doit pouvoir se connecter de manière sécurisée aux différentes bases de données contenant des données personnelles. Cette connexion nécessite la mise en place d'un système de cartographie précis des données, permettant d'identifier la localisation des informations pertinentes dans le système d'information. Un point critique toutefois : la gestion des droits d'accès. L'API ne doit avoir accès qu'aux données strictement nécessaires à sa fonction, conformément au principe de minimisation.

[88] Analogie reprise du site api.gouv.fr, disponible via l'URL suivante : https://api.gouv.fr/guides/api-definition

Une API peut permettre d'accroître considérablement l'efficacité du responsable du traitement dans le cadre de la gestion des demandes de droits. Par exemple, lorsqu'une personne concernée exerce son droit à l'effacement des données : il faudrait d'abord ouvrir chaque application (messagerie, CRM, ERP, solution marketing) et, le cas échéant, rechercher les documents papiers comportant ses données personnelles. Ensuite, les données concernées devraient être identifiées avant qu'il ne soit procédé à leur effacement. Grâce à l'API, un script ou un portail central peut appeler l'ensemble des API de chacune des applications concernées par la demande et introduire une requête entrainant la suppression des données concernées. Il en va de même pour la rectification des données ou la limitation du traitement. Autre exemple : dans le cadre du droit d'accès, une interface sur laquelle se connecte la personne concernée pourrait (via un bouton « télécharger mes données ») se loguer au système d'information du responsable de traitement qui lui fournirait en retour un fichier (JSON, CSV, etc.) contenant toutes les données couvertes par le droit d'accès. Du fait de la structuration de la base de données, la segmentation, ou encore la mise en place de règles de validation, l'identification des données pourraient être automatiques et l'intervention humaine réduite au minimum. Des procédés d'autorisation manuelle ou de limitation des actions pourraient toutefois être prévus dans le cadre de certains droits et demandes spécifiques (notamment pour ce qui concerne le droit d'opposition et le droit d'effacement).

Cependant, l'API présente un certain nombre d'inconvénients, notamment en termes de sécurité. En effet, son implémentation introduit de nouveaux risques sur le système d'information. Les API doivent donc être protégées afin d'éviter, par exemple, qu'une requête malintentionnée ne puisse venir supprimer des données. Des mesures telles que le chiffrement des données, l'authentification, le contrôle des accès, peuvent utilement être mises en œuvre en ce sens. D'autre part, la journalisation peut instaurer la traçabilité des actions (qui est à l'origine de la requête ? Quand a-t-elle été introduite ? Quelles données étaient concernées ?). Par ailleurs, le déploiement d'une API peut entrainer des coûts de développement (investissement initial) et de maintenance (mise à jour, surveillance, support) conséquents. L'analyse de l'efficience et l'évaluation des gains générés par une telle solution peuvent alors permettre d'en vérifier la rentabilité. Enfin, la formation des utilisateurs constitue un autre point d'attention. Bien que les API aient vocation à simplifier les processus, elles peuvent se révéler peu accessibles pour les utilisateurs finaux (tant pour les collaborateurs que pour les personnes concernées).

Les API représentent donc une solution innovante et efficace pour répondre aux exigences du RGPD, particulièrement adaptées aux organisations disposant de volumes importants de données, de solutions logicielles imbriquées et de processus complexes. Cependant, leur

déploiement requiert une analyse approfondie des besoins, des risques et des ressources disponibles. Le succès de cette approche dépend largement de la qualité de sa conception, de son implémentation et de son maintien dans la durée.

*ii) Workflow : automatiser l'enchaînement de tâches*

Un « workflow » (ou flux de travail) est la représentation d'un processus en plusieurs tâches ordonnées dont l'accomplissement est soumis à un ensemble de règles et de conditions. Il décrit l'enchaînement de ces tâches pour parvenir à un résultat recherché. Toutes ces étapes forment un parcours dont le cheminement peut varier selon des hypothèses prévues à l'avance. Par exemple, il peut être paramétré pour ajouter une étape de validation supplémentaire pour les données relevant d'une catégorie spécifique.

La notion de tâche se positionne donc au cœur du concept de workflow. Elle peut être une action humaine (instruire une demande, valider un document, etc.) ou une action système (envoyer une requête à une API, envoyer une notification à un opérateur, etc.). Des transitions relient les tâches entre elles et peuvent inclure des déclencheurs et des conditions afin d'orienter le cheminement du processus. Le déclenchement d'une tâche peut être occasionné par un évènement déterminé (par exemple la réception d'une demande de droit).

La mise en place de workflows (avec un niveau d'automatisation variable) - comprenant des étapes de validation ainsi que les responsabilités et les règles d'affectation afférentes - favorise la formalisation d'un processus clair et commun à l'ensemble des équipes qui y participent. Il permet également de tracer l'ensemble des actions réalisées. De plus, il est tout à fait envisageable d'automatiser l'exécution de tout ou partie des étapes composant le workflow et/ou de synchroniser les systèmes impliqués (API, logiciels, applications, bases de données, etc.). D'autre part, un workflow peut s'intégrer dans d'autres solutions (API, RPA, ESB, portail self-service) pour créer un écosystème complet d'automatisation.

Un processus pourrait être décrit, dans la logique d'un workflow, comme suit :

- Déclencheur : réception d'une demande d'effacement par email.
- Tâche 1 (déclenchement automatique) : Vérifier l'identité de la personne concernée (envoi d'un email/SMS pour double authentification)
- Tâche 2 (déclenchement conditionné à la réussite du test d'authentification) : Examiner la validité de la demande d'effacement en fonction des règles définies en amont par le responsable du traitement

- Tâche 3A (déclenchement conditionné à la réussite de la tâche précédente) : lancer la suppression des données
- Tâche 3B (déclenchement conditionné à l'échec de la tâche précédente) : notifier le DPO pour validation
- Tâche 4 (déclenchement conditionné à la validation de la tâche précédente soit par le système, soit par le DPO) : Effacer les données
    - Sous-tâche 4.1 (automatique) : Envoyer une requête à l'API du CRM
    - Sous-tâche 4.2 (automatique) : Envoyer par mail une notification de l'effacement au sous-traitant
    - Sous-tâche 4.3 (automatique) : Envoyer par mail une réponse à la personne concernée pour confirmer l'effacement des données
- Tâche 5 (déclenchement automatique) : Générer un rapport et consigner le traitement de la demande dans le registre des demandes de droits.

Une demande de droit peut ainsi être traitée en quelques secondes, sans que cela ne requière d'intervention humaine.

Toutefois, la mise en place d'un workflow nécessite d'identifier clairement l'ensemble du processus et de couvrir toutes les hypothèses possibles. Un travail de collaboration entre l'ensemble des parties prenantes (équipes métiers, support, service informatique, DPO, etc.) est indispensable. Une logique de workflow doit également prévoir la gestion des erreurs ou blocages. L'enjeu est donc de trouver un équilibre entre l'automatisation des séquences répétitives et le contrôle humain. Par ailleurs, le workflow nécessite une mise à jour continue afin, par exemple, de pouvoir s'adapter aux modifications d'un traitement, à l'implémentation d'un nouveau logiciel, etc.

Il s'agit donc d'un outil de pilotage permettant de centraliser la gestion d'un ensemble complexe de tâches nécessitant l'intervention de multiples acteurs. Il constitue une solution puissante pour industrialiser le traitement des demandes de droit et, plus largement, la gestion des données personnelles.

*iii) Tableaux de bord numériques*

Dans le cadre de l'automatisation des tâches et des processus de traitement des demandes de droits, les tableaux de bord numériques peuvent offrir une vision globale et en temps réel des flux et des opérations. Ils permettent à l'organisation de superviser ces processus et d'être capable de réagir rapidement en cas de problème. Il s'agit d'une interface regroupant des

indicateurs, des statistiques et des statuts opérationnels pour les présenter de manière intuitive aux équipes en charge de la gestion des demandes de droits.

Les tableaux de bord numériques permettent donc au responsable du traitement de :

- Surveiller les tâches et processus automatisés, via le statut des demandes en cours de traitement ;
- Identifier les anomalies : repérer les retards dans le traitement, les tâches bloquées, les systèmes « en panne » ;
- Faciliter le reporting : fournir des données d'analyse et assurer la traçabilité des actions menées par chacun des systèmes.

Le tableau de bord numérique représente l'avantage de centraliser (en temps réel) toutes les informations pertinentes pour la gestion efficace des demandes de droits. Ils peuvent également inclure des alertes automatiques pour signaler des anomalies aux métiers impliqués dans le traitement des demandes. Pour les personnes concernées, il représente également une solution ergonomique et efficace afin de recevoir l'information communiquée par le responsable du traitement et mener un certain nombre d'actions concernant la protection de ses données telles que, par exemple le paramétrage de ses choix, l'exercice des demandes de droits, etc. (Voir infra : L'amélioration et la personnalisation des services autour de la gestion des droits au travers d'une approche centrée sur l'utilisateur).

*iv) Autres solutions*

En plus des API et workflows, d'autres solutions techniques peuvent, dans une logique d'automatisation, répondre à des besoins spécifiques de l'organisation. Ainsi, le RPA (« Robotic Process Automation ») permet d'automatiser des tâches notamment dans un environnement informatique vieillissant. Il s'agit d'une alternative possible lorsqu'il n'est pas envisageable de mettre en place une API ou de moderniser les systèmes existants. Cette solution consiste à utiliser un logiciel « robot » agissant en tant qu'utilisateur virtuel.

Il pourra alors simuler les actions d'un utilisateur humain (cliquer dans l'interface, effectuer des saisies clavier, copier-coller des éléments) dans un logiciel ou une application utilisée par les équipes métiers. Il s'agit là encore de réduire les erreurs humaines tout en libérant les collaborateurs de tâches chronophages afin qu'ils puissent se concentrer sur des activités à plus forte valeur ajoutée. Par exemple, une personne concernée demande par mail l'effacement de ses données. Le logiciel « robot » va - tout comme le ferait un opérateur humain - analyser le mail et identifier les informations pertinentes (nom, adresse email, type de demande, etc.), ouvrir le CRM (où se trouvent les données à effacer), rechercher la fiche

client (via saisie clavier), procéder à la suppression des données (en cliquant sur le bouton de suppression) et enregistrer le message de confirmation, puis générer un rapport de suppression. Autre exemple : le support reçoit régulièrement des demandes de rectifications. Le RPA peut alors procéder à la rectification sur plusieurs systèmes successivement (CRM, base de facturation, base de données marketing, etc.), automatisant ainsi ce qui serait autrement un long travail manuel. Le RPA peut également intégrer un workflow afin que ses actions s'imbriquent au sein d'un processus plus global.

Une autre solution possible : l'ESB (« Enterprise Service Bus »), permettant de centraliser les échanges de données entre différents logiciels et applications via un « bus » commun. Plutôt que de connecter directement plusieurs systèmes (comme le ferait une API), l'ESB centralise les instructions, transforme les informations si nécessaire et les transmet à chacun des systèmes « embarqués à bord du bus ». Le bus peut transmettre des requêtes à plusieurs logiciels et applications en parallèle et en assurer le suivi. Chaque système va alors appliquer les instructions reçues selon sa propre logique. Par exemple, lorsque des données sont rectifiées sur l'espace client, l'ESB va analyser ces modifications et relayer les informations mises à jour à toutes les applications concernées (CRM, facturation, logistique, etc.). Ces systèmes ne prenant pas en compte le même format de données, L'ESB va alors « transformer » les informations afin de pouvoir les véhiculer à chacun d'entre eux dans le format adéquat.

L'ESB permet de synchroniser les mises à jour à travers l'ensemble du système d'information de l'organisation. L'un des principaux avantages de l'ESB est sa scalabilité : un nouveau logiciel ou une nouvelle application peut rejoindre le bus à tout moment, sans qu'il soit nécessaire de recoder l'ensemble du système.

Enfin, une autre alternative : le portail self-service. Il s'agit d'une interface utilisateur permettant à la personne concernée de gérer ses données et d'exercer ses droits directement, sans avoir à contacter le responsable du traitement. Il peut notamment s'agir d'un formulaire, d'un chatbot, etc. Ce point d'entrée unique facilite l'exercice des droits pour les personnes concernées et peut intégrer le statut de la demande pour plus de transparence. Dans une logique d'automatisation, il peut être relié à une API ou à un workflow pour déclencher les tâches requises. De plus, le portail peut conserver la trace de chaque demande reçue et de leur résultat et les consigner dans le registre de traitement des demandes. Par exemple, une personne concernée exerce son droit d'accès via un bouton « J'accède à mes données » ou en discutant avec le chatbot disponible depuis son espace client. Le portail appelle les API des systèmes concernés ou bien déclenche le workflow connexe. Il centralise ensuite les données

retournées par chacun des systèmes, les compile et renvoie un fichier téléchargeable au demandeur.

L'implémentation de solutions et d'outils visant à automatiser les tâches et processus offre ainsi au responsable du traitement plusieurs avantages.

Premièrement, des gains d'efficacité et de temps pour les équipes chargées de traiter les demandes : l'automatisation permet de réduire les interventions manuelles, d'accélérer la réponse aux demandes et d'éviter les retards. Ensuite, des gains en termes de sécurisation et de fiabilité des données : l'automatisation permet d'éviter les erreurs manuelles et assure une certaine traçabilité (via les journaux de logs des outils utilisés). L'automatisation engendre également des réductions de coûts (libérer des ressources jour-homme, minimiser les actions correctives, etc.). De plus, elle permet d'améliorer la satisfaction des personnes concernées, leur perception de l'organisation et la confiance qu'elles lui vouent. Enfin, elle augmente l'agilité du responsable du traitement, qui devient plus apte à intégrer de nouveaux traitements et flux de données, tout en étant mieux préparé aux évolutions réglementaires.

Les solutions présentées constituent des briques modulaires participant à la construction d'une logique d'automatisation et d'industrialisation du traitement des demandes de droits. Le responsable du traitement peut ainsi piocher des éléments au sein de chacune de ces briques pour bâtir un système adapté aux réalités du système d'information (caractéristiques, architecture, logiciels et applications utilisés). Ainsi, le niveau d'automatisation et les solutions déployées pourront s'intégrer efficacement à l'activité de l'organisation et répondre au mieux aux besoins exprimés par les équipes métiers. En plus de renforcer la gouvernance des données et la gestion des processus, elles peuvent aussi contribuer à accroître les capacités de gestion et d'organisation du responsable du traitement.

L'ensemble de ces outils de gouvernance (segmentation, cartographie, automatisation, tableaux de bord) renforce la gestion des demandes de droits tout en ayant un impact positif sur l'ensemble de l'activité de l'organisation. Ces outils ne sont pas une fin en soi : ils peuvent être intégrés dans un processus plus large visant à accroître les capacités organisationnelles du responsable du traitement.

## 2. Optimiser les capacités de gestion et d'organisation

La gouvernance des données et la gestion efficiente du traitement des demandes de droits peuvent également être renforcées par l'accroissement des capacités de gestion et d'organisation du responsable du traitement. L'adoption d'une approche proactive en la

matière constitue une opportunité pour celui-ci : un levier de création de valeur sur des plans opérationnels (2.1), organisationnels (2.2) et humains (2.3).

### 2.1. Dimension opérationnelle

*i) Amélioration continue*

Pour commencer, le responsable du traitement peut rechercher à améliorer ses capacités opérationnelles par la mise en place d'une logique d'amélioration continue. Il s'agit d'une approche reposant sur un processus cyclique (itératif) visant à améliorer - de manière progressive et dans la durée - les processus, outils et pratiques mis en œuvre par l'organisation. Ces améliorations font l'objet d'une réévaluation et d'ajustements réguliers en fonction de l'évolution de l'activité, des besoins des équipes métiers et des résultats observés.

Dans une logique d'amélioration continue, les « échecs » alimentent la base de connaissances de l'organisation et contribuent à bâtir une solution chaque fois plus robuste. Par exemple, l'analyse des retards dans le traitement des demandes révèle un goulet d'étranglement (processus inadaptés ou perfectibles, manque de ressources, etc.). De la même manière, une récurrence de retours d'expérience négatifs de la part des personnes concernées souligne des axes d'amélioration. Chaque difficulté rencontrée devient une occasion d'optimiser les processus déployés par l'organisation. Le retour d'expérience est donc un élément fondamental de l'amélioration continue. Il peut être collecté lors de débriefings après des évènements spécifiques (audit, violation de données, plainte, demande complexe, etc.), par le biais de commentaires des équipes métiers, par des enquêtes de satisfaction, etc. L'analyse des causes sous-jacentes de ces problèmes (par exemple via l' « Analyse Ishikawa »,[89] la « Méthode des 5 Pourquoi »,[90] ou encore la « Méthode QQOQCCP »[91]) est essentielle pour orienter les actions correctives.

Cette amélioration continue peut reposer sur des méthodologies telles que le cycle PDCA (« Plan-Do-Check-Act » ou « Roue de Deming »)[92] ou encore sur un système de gestion de la

[89] Axel LEFEBRE, “Le diagramme d'Ishikawa”, Le Blog du dirigeant, 8 novembre 2024, consultable via le lien suivant : https://www.leblogdudirigeant.com/diagramme-ishikawa/

[90] Axel LEFEBRE, “L'hexamètre de Quintilien ou méthode QQOQCCP”, Le Blog du Dirigeant, 8 novembre 2024, consultable via le lien suivant : https://www.leblogdudirigeant.com/hexametre-de-quintilien-methode-qqoqccp/

[91] Axel LEFEBRE, “Les 5 pourquoi : Définition été exemple d'un outil de résolution de problème”, Le Blog du Dirigeant, 8 novembre 2024, consultable via le lien suivant : https://www.leblogdudirigeant.com/les-5-pourquoi/

[92] Laurent DUFOUR, “La roue de Deming pour améliorer le pilotage de votre entreprise”, Le Blog du Dirigeant, 20 novembre 2024 : Illustration et explication de la “roue de Deming”, consultable via l'URL suivante : https://www.leblogdudirigeant.com/la-roue-de-deming/

qualité (norme ISO 9001, référence mondiale pour l'amélioration continue).[93] Le cycle PDCA est itératif et répète les actions suivantes :

- **Plan** (Prévoir) : identifier les axes problématiques et/ou les opportunités d'amélioration, définir des objectifs clairs et planifier les actions correctives nécessaires.
- **Do** (Faire) : mettre en œuvre les actions planifiées à petite échelle pour tester leur efficacité (plus l'action est ciblée, plus elle peut être réalisée rapidement et augmente la maitrise du processus itératif).
- **Check** (Mesurer) : évaluer les résultats obtenus par rapport aux objectifs initiaux en mesurant les performances et en analysant les écarts.
- **Act** (Réagir) : appliquer les correctifs à une plus grande échelle si les résultats sont concluants, ou ajuster les actions en cas d'échec.

Une fois le cycle terminé, il recommence en intégrant les enseignements tirés de l'itération précédente. L'apprentissage est donc constant, tout comme la marge de progression.

Dans le cadre de la gestion des demandes de droits, un cadre itératif est particulièrement appréciable. Il permet de s'assurer de l'efficacité des processus (automatisés ou non), de révéler des étapes manquantes ou au contraire superflues, des goulets d'étranglement ou des « trous dans la raquette ». Il favorise également une adaptation plus aisée à d'éventuelles évolutions règlementaires ou attentes des autorités de contrôle.

Par conséquent, l'amélioration continue permet à l'organisation de s'adapter aux évolutions de son environnement (réglementaires, technologiques, attentes des clients, des collaborateurs, des partenaires, etc.). Elle permet également d'identifier et de corriger les inefficacités, les coûts inutiles et les erreurs dans les processus. Elle assure également la pérennité des gains d'efficacité ainsi obtenus et renforce la résilience organisationnelle du responsable du traitement.

*ii) Métriques et indicateurs*

Les indicateurs de performance jouent un rôle crucial dans la prise de décision. Ils peuvent également servir de levier puissant pour la transformation, en mesurant la création de valeur. Ces outils constituent également des « armes » affutées (surtout lorsqu'ils prennent une forme visuelle) pour le DPO. A fortiori lorsqu'il doit « défendre le bout de gras » devant un CODIR, COMEX, COPIL ou autre COMOP. Plus convaincante qu'un long argumentaire axé sur la

[93] ISO 9001:2015. (2015). Quality Management Systems – Requirements. International Organization for Standardization, accessible via l'URL suivante : https://www.iso.org/fr/standard/62085.html

conformité, une diapositive bien illustrée et soigneusement chiffrée est un excellent moyen de démontrer le bien-fondé d'une nouvelle stratégie…

Quel que soit le degré d'automatisation du traitement des demandes de droits, des systèmes de mesure peuvent être mis en place pour obtenir des données d'analyse. Ces métriques et indicateurs constituent un élément essentiel pour évaluer l'efficacité des processus et outils (automatiques ou manuels) déployés pour la gestion des demandes de droits. Ils permettent de mesurer l'efficacité, les blocages et inefficiences et, le cas échéant, d'améliorer les outils et processus mis en place par le responsable du traitement. Ils permettent également de démontrer la valeur ajoutée des efforts menés - au-delà de la conformité réglementaire - et leur impact positif sur les autres fonctions de l'organisation. Il s'agit également d'un puissant outil de communication sur les performances, en interne (direction, équipes métiers, etc.), comme en externe (clients, partenaires, etc.).

Parmi ces métriques, on peut notamment citer les « indicateurs de performance clés » (KPIs), soit des « *indicateurs utilisés pour l'aide à la décision dans les organisations.* Ces indicateurs *« sont utilisés particulièrement en gestion de la performance organisationnelle* » [94]. On retrouve, notamment, les KPIs suivants :

- **KPIs temporels**, tels que les délais moyens de traitement (par type de demande), le taux de satisfaction, le temps moyen passé par étape du parcours, le temps écoulé entre la réception de la demande et la première action entreprise, etc...
- **KPIs volumétriques**, tels que le volume des demandes en cours de traitement, le nombre de demandes reçues et traitées, la répartition des demandes reçues par type, la répartition des demandes par canal de réception, le taux de demande par catégorie de personnes concernées volume par type, etc.
- **KPIs qualitatifs**, tels que le taux de satisfaction des demandeurs, le nombre de réponses contestées, le nombre de recours / plaintes reçus, etc.

Un KPI intervient en réponse à un objectif (spécifique), pour mesurer ou calculer (quantifier) l'accomplissement (atteignable) de cet objectif (pertinent) selon une fréquence déterminée (temporalité).

Par exemple, dans le cadre de la gestion du traitement des demandes d'exercice de droit, un KPI pourrait viser à s'assurer que le délai légal de traitement est respecté. Il s'agira de

[94] Définition de la notion de Key Performance Indicator (KPI) disponible sur Wikipédia via le lien suivant : https://fr.wikipedia.org/wiki/Indicateur_clé_de_performance , que l'on peut séparer en trois familles :

mesurer, à une fréquence mensuelle, le rapport entre les demandes traitées dans les délais et celles traitées hors délai. L'évolution de ce chiffre à la hausse montrera une détérioration des process de traitement mis en œuvre par l'organisme. Celui-ci pourra alors, via des analyses complémentaires, trouver l'origine d'une telle détérioration et y remédier.

D'une manière plus globale, les métriques et indicateurs peuvent se décomposer en plusieurs catégories, en fonction de leur objectif, de la performance qu'ils visent à mesurer ou de la problématique qu'ils entendent mettre en lumière, soit :

- **L'efficacité opérationnelle**, par exemple : mesurer les délais moyens de traitement pour identifier les goulets d'étranglement ; évaluer le pourcentage de demandes traitées dans les délais ; mesurer le taux d'automatisation des demandes (pourcentage des demandes traitées via workflow, sans intervention humaine) pour dégager les gains d'efficience dus à l'automatisation, etc.
- **La qualité des processus et des données**, par exemple : mesurer le taux de demandes nécessitant une information complémentaire (car mal formulées ou incomplètes) pour améliorer le canal d'introduction ; mesurer le nombre d'incidents liés à la qualité des données (nombre de doublons ou d'incohérences détectés lors du traitement d'une demande de droit) pour évaluer l'impact de la qualité des données sur l'efficacité des processus.
- **Le retour sur investissement et la réduction des coûts**, par exemple : mesurer le coût de traitement d'une demande avant et après l'amélioration/l'automatisation des processus pour justifier les investissements réalisés dans les solutions déployées ; mesurer le ratio entre les économies réalisées (en temps et en coût financier) et les dépenses engagées pour l'implémentation de nouveaux outils (API, ESB, portail self-service, etc.) pour évaluer leur rentabilité et le retour sur investissement réalisé.
- **L'expérience utilisateur et la satisfaction**, par exemple : mesurer le nombre de plaintes reçues ou de recours déposés pour identifier et solutionner les points d'insatisfaction et les dysfonctionnements observés ; évaluer la satisfaction des personnes concernées quant au traitement de leurs demandes (notamment par des enquêtes, recueil d'avis, etc.) pour s'assurer que les processus respectent la règlementation mais aussi leurs attentes. Sur ce point, le responsable du traitement doit veiller à identifier le moment opportun pour solliciter l'avis de la personne concernée sans risquer de générer de frictions. En effet, il peut être frustrant de se voir demandé si l'on est satisfait alors que sa demande n'a pas encore été traitée ou qu'elle l'a été de manière incomplète…

Par ailleurs, dans le cadre d'une telle approche, des objectifs de performance peuvent être définis à différents termes. Par exemple, les objectifs du responsable de traitement pourraient être de mesurer :

- **A court terme** (1 à 12 mois) : la réduction du temps de traitement ;
- **A moyen terme** (1 à 3 ans) : la réduction des coûts de traitement des demandes, l'augmentation de la satisfaction des personnes concernées ;
- **A long terme** (+3ans) : l'amélioration du positionnement sur le marché.

Ces données d'analyse peuvent donc être utilement employées afin de démontrer que la gestion des demandes de droit ne se limite pas à la seule conformité mais créée également des opportunités pour le responsable du traitement en termes d'optimisation des ressources, de renforcement de la satisfaction client et de réduction des risques de sanction ou de plaintes.

*iii) Qualité des données*

Selon une récente étude menée par l'Observatoire de la Maturité Data des Entreprises, les principaux objectifs des entreprises interrogées en 2024 concernant l'utilisation des données sont l'optimisation des performances et l'amélioration du pilotage organisationnel. Elles soulignent également que la qualité des données est leur principale préoccupation, car elle constitue un obstacle à l'atteinte de ces objectifs et, plus largement, au développement de leur « potentiel data ».[95]

**La qualité des données représente un véritable enjeu pour toute organisation souhaitant mettre à profit les informations dont elle dispose afin d' optimiser et améliorer sa gouvernance, sa résilience, ses capacités d'organisation et sa compétitivité.**

La « qualité » représente la capacité d'une information à être utilisée pour atteindre les objectifs (opérationnels, réglementaires et stratégiques) qu'une organisation s'est fixée. Elle revêt plusieurs dimensions, à savoir :

- **L'exactitude** : la donnée doit être capable de retranscrire la réalité.
- **La complétude** : la donnée doit être complète, aucun champ critique ne doit manquer.

[95] Observatoire de la Maturité Data des Entreprises, résultat de l'enquête 2024, accessible via l'URL suivante : https://observatoire-data.fr/resultats

- **La cohérence** : la donnée doit pouvoir être exploitée au regard des activités de l'organisation.
- **L'actualisation** : la donnée doit être mise à jour régulièrement pour être capable de continuer à refléter la réalité sur le temps long.
- **La fiabilité** : la donnée doit pouvoir être utilisée pour remplir un objectif déterminé quel que soit le contexte de son utilisation. Une donnée exacte peut ne pas être fiable (par exemple une adresse électronique exacte arrête d'être fiable dès lors qu'elle n'est plus utilisée par la personne concernée).

Dans le contexte de la conformité RGPD, une dimension supplémentaire peut être prise en compte : celle de la traçabilité. En effet, les obligations s'imposant au responsable du traitement impliquent que l'origine et l'évolution de la donnée puissent faire l'objet d'un suivi. En ce sens, les métadonnées constituent un outil très efficace (voir supra : Segmentation des données et utilisation de métadonnées).

Un manque de qualité des données peut affecter l'ensemble des métiers d'une organisation. Elle peut avoir des conséquences négatives sur le plan de la conformité certes, mais également sur l'efficacité opérationnelle et sur la fiabilité des mesures de performance et des analyses stratégiques menées par l'organisation. En ce qui concerne les fonctions commerciales et marketing, des données erronées ou obsolètes peuvent entraîner des campagnes mal ciblées, des offres inadaptées et réduire l'efficacité des efforts de prospection (taux de conversion) et fidélisation. Côté opérationnel, cela peut nuire à la planification et à la gestion des ressources (par exemple en provoquant des erreurs au niveau de la chaîne logistique, des retards de préparation, d'acheminement, de livraison, etc.). Dans le domaine des Ressources Humaines, des bases de données incorrectes peuvent conduire à des erreurs dans la gestion des paies, des contrats, des compétences, etc. Certains éléments représentent une source fréquente de manque/perte de qualité des données. A ce titre, l'attention du responsable du traitement doit alors se porter sur :

- La collecte non standardisée de données (les données sont collectées par plusieurs canaux dont les formats ne sont pas harmonisés) ;
- Les doublons et/ou incohérences (par exemple, à la suite d'une erreur de saisie, une personne concernée est enregistrée plusieurs fois dans les systèmes du responsable du traitement mais les informations différent) ;
- Les systèmes non synchronisés (les bases de données ne communiquent pas entre elles et la donnée n'est pas mise à jour sur l'ensemble des systèmes de l'organisation) ;

- L'absence de validation (les processus de collecte ne permettent pas une vérification systématique de l'exactitude et/ou de la complétude des données) ;
- Le manque de mise à jour (avec le temps, les données peuvent devenir obsolètes en l'absence d'un processus permettant de s'assurer de leur pérennité).

Pour améliorer la qualité des données, l'organisation peut engager un certain nombre d'actions et notamment :

- **La détection et la correction des anomalies**, par la mise en place de contrôle en amont de la collecte ou la correction via des solutions technologiques (par exemple via outils de « Data Cleaning ») ;
- **L'optimisation des processus de collecte**, par la standardisation des formulaires ou la vérification de la cohérence des saisies (par exemple via des champs obligatoires et des chaines de caractères programmées) ;
- **La cartographie et la segmentation des données** (Voir supra : Structurer la gouvernance par la digitalisation et l'automatisation).
- **La synchronisation et l'intégration des systèmes** (Voir supra : Automatisation : vers l'industrialisation du traitement des demandes de droits).

Par ailleurs, le responsable du traitement peut voir dans le traitement des demandes de droits, l'opportunité de s'assurer de la qualité des données. Par exemple, les demandes de rectification constituent une source gratuite et fiable de mise à jour des données. La concentration de demandes similaires peut mettre en lumière des failles ou erreurs potentielles, telles qu'un défaut de mise à jour lors de la déclaration d'un changement de situation, une mauvaise synchronisation entre les systèmes, ou encore des erreurs dans la saisie des données. Ainsi, le responsable du traitement pourra procéder aux ajustements nécessaires, comme la modification des processus de collecte et de mise à jour des données, l'amélioration de l'interface utilisateur pour faciliter la saisie, ou l'ajout de contrôles de validation. De plus, l'observation d'une récurrence de ce type de demandes pourrait l'amener à instaurer un processus de vérification régulier des données. Un tel dispositif pourrait, à son tour, générer de la valeur et des bénéfices pour les métiers, par exemple en évitant le coût de communications mal adressées ou en augmentant le taux de conversion des campagnes marketing.

### 2.2. Dimension organisationnelle

*i) Structuration et coordination*

Lorsque le responsable du traitement évolue dans un écosystème collectif (regroupements d'entités, d'intérêts, etc.), il est essentiel de déployer une approche stratégique systémique, définie au niveau collectif (groupe, réseau, communauté de collectivités, etc.). Cela peut inclure, par exemple, la mutualisation d'une politique commune, d'un registre des traitements consolidé, d'outils et de processus de gouvernance, ainsi que l'assignation des différentes responsabilités et la mise en place d'un « réseau RGPD » composé de DPO et de relais.

Au-delà d'un cadre global, des processus peuvent être mis en place afin de faciliter, d'harmoniser et d'assurer la cohérence du traitement des demandes de droits. De tels processus doivent permettre à chaque entité de traiter les demandes de droits conformément au dispositif d'ensemble tout en tenant compte d'éventuelles spécificités qui lui sont propres. Ces processus doivent couvrir l'ensemble des étapes identifiées dans le cadre du parcours du traitement des demandes, en considérant le fait que les réalités économiques et juridiques de chaque entité peuvent diverger (spécificités réglementaires locales, natures des activités exercées, typologies de personnes concernées, etc.). La structuration organisationnelle du traitement des demandes de droits doit ainsi équilibrer cohérence et efficacité locale (là où une organisation purement centralisée pourrait générer des goulets d'étranglement et la décentralisation des incohérences).

Dans une telle configuration, une architecture doit donc être bâtie et les différentes responsabilités doivent être assignées de manière claire et précise, entre les différentes entités constituant un tel groupe ou réseau. Par exemple, à un niveau global, une supervision générale et commune des mécanismes de contrôle et de reporting peut être organisée, tandis que chaque entité se verrait déléguée la responsabilité opérationnelle de répondre aux demandes de droits. De plus, des outils de gouvernance communs (tableaux de bord, API, cartographie des données, etc.) permettraient alors la mise en place de process automatisés, d'outils de gouvernance (incluant la gestion des demandes de droits).

Pour ce qui est de la personne concernée, un « guichet unique » (ou du moins indifférencié) devrait lui être proposé afin qu'elle puisse y déposer facilement sa demande. A défaut, les informations communiquées devraient être suffisamment claires et précises pour lui permettre de savoir auprès de quelle entité introduire sa demande.

D'autre part, des mécanismes de coordination pourraient être mis en place afin de s'assurer de l'efficacité et de l'harmonisation du traitement des demandes de droits. Il s'agit, pour le responsable de traitement d'un point fondamental car il pourrait lui permettre, notamment, d'éviter la « perte » des demandes, les retards dans le traitement, des erreurs de transmission, d'assurer la qualité et la conformité des réponses aux exigences règlementaires, de réaliser

des économies en termes de coûts de gestion, etc. En effet, en fonction des relations entretenues avec la personne concernée, de la nature et de la portée de sa demande de droit, des répercussions pourraient affecter plusieurs entités. Il est donc nécessaire de pouvoir identifier rapidement les entités impliquées dans le traitement de la demande et d'unifier leur réponse.

Pour ce faire, il est possible de mettre en place un système structuré de supervision et de partage d'expérience afin de centraliser le suivi des demandes et de surveiller les performances de chaque entité. En ce sens, des outils de reporting mutualisés et adaptés peuvent permettre :

- L'identification des sources de problèmes récurrents et la correction de ces problèmes ;
- L'identification des entités les moins « performantes » et l'accompagnement vers l'amélioration de leurs pratiques ;
- La remontée et le partage de bonnes idées et/ou pratiques ;
- La poursuite d'une logique d'amélioration continue (voir supra : Amélioration continue) applicable à l'ensemble des entités du groupe, réseau, etc.

*ii) Collaboration transverse*

**Pilotage transversal et approche holistique.** La gestion des demandes de droits impose la coopération et l'harmonisation des pratiques de la part de l'ensemble des services et équipes impliqués, chacun ayant un rôle précis à jouer. Le pilotage transversal consiste à mettre en place une gouvernance centralisée pour coordonner leurs efforts. Une organisation trop segmentée et des services trop cloisonnés peuvent gêner la circulation de l'information et réduire la fluidité des processus de gestion des demandes de droits. Cela peut également entraîner des doublons inutiles, des retards dans le traitement des demandes, etc.

Pour résoudre ou anticiper cette problématique, l'organisation peut créer des comités de gouvernance des données. Ces derniers regroupent des représentants de chaque service impliqué et ont pour mission d'aligner les priorités, d'harmoniser et de rationaliser les pratiques et fluidifier la communication interservices. De plus, une approche holistique permet d'obtenir une vision d'ensemble sur un sujet/problème et de dégager des approches/solutions plus complètes et efficaces. L'organisation peut également développer une vision partagée par l'ensemble des équipes afin, par exemple, de s'assurer que les enjeux liés à la protection des données personnelles sont compris par tous.

Prenons le cas d'un responsable du traitement qui met en place un comité réunissant le DPO, le responsable IT, ainsi que des représentants des équipes marketing et des Ressources Humaines. Lors de réunions bimensuelles, ce comité examinera les indicateurs clés de la gestion des demandes de droits, identifiera les points bloquants, les axes d'amélioration, les problèmes rencontrés par les équipes et proposera des ajustements pour améliorer/corriger les processus déployés.

**Procédures interservices.** La centralisation des demandes de droits nécessite des échanges fluides entre les équipes. En effet, il arrive souvent au sein d'une organisation que chaque service dispose de ses propres outils et pratiques. Cela peut entraîner des incohérences, des contradictions et des blocages dans les processus. Des outils collaboratifs peuvent alors utilement être mis en place. Des procédures interservices permettent ainsi d'instaurer une méthodologie claire et harmonisée permettant d'éviter la perte d'informations ou les retards d'exécution. La mise en œuvre de procédures réalisées collectivement (prenant en compte la réalité des pratiques et les spécificités des équipes) permet, au-delà d'une meilleure adhésion par les collaborateurs, de remplir cet objectif de cohérence.

De plus, les processus peuvent intégrer certains mécanismes de communication entre différentes équipes dans des cas spécifiques. Par exemple, un processus clairement formalisé pourrait prévoir le fait que le service marketing informe le service IT lorsqu'une demande d'opposition est reçue afin que celui-ci puisse s'assurer que les actions entreprises dans le cadre du traitement de la demande soient bien répercutées sur l'ensemble des systèmes concernés. En fonction du type de traitements impliqués, ce même processus pourrait prévoir que le service IT prenne contact avec le service juridique afin de pouvoir déterminer les traitements concernés et les systèmes impactés par la demande d'opposition.

Autre exemple : un collaborateur exerce son droit d'accès. Un processus interservices est mis en place pour que le service des Ressources Humaines fournisse les données collectées dans le cadre de l'exécution du contrat de travail, que le service commercial extraie, le cas échéant, ses données clients du CRM, que le service IT récupère les informations relatives à son utilisation des outils numériques et que le service marketing vérifie l'existence de données relatives à d'éventuelles campagnes promotionnelles le concernant (ventes privées pour le salarié, participation à des événements, etc.). Un tel processus évite que chaque service ne réponde de manière isolée ou contradictoire, tout en permettant une supervision centralisée et simplifiée du traitement de la demande.

**Partage des bonnes pratiques et partenariats stratégiques.** L'efficacité globale de l'organisation peut être accrue par le partage de bonnes pratiques entre les équipes ou les

différentes entités composant un groupe, un réseau, etc. Cela inclut les retours d'expérience sur les incidents, l'adoption d'outils performants ou la mise en œuvre de processus et de workflows. En pratique, dans des structures internationales ou multisites, chaque entité peut développer ses propres solutions, sans toutefois communiquer avec les autres. Un tel cloisonnement peut représenter une perte lorsqu'il empêche l'application de méthodes éprouvées ailleurs et qui ont démontré leur efficacité. Par exemple, au sein d'un groupe multinational, une filiale européenne optimiserait la gestion des demandes d'effacement grâce à un workflow automatisé qui intègrerait directement les règles du RGPD. Elle partagerait cette solution avec ses filiales en Amérique latine, qui l'adapteraient pour répondre aux exigences des règlementations locales.

Afin de favoriser le partage de bonnes pratiques, des sessions de retour d'expérience peuvent être organisées. De telles sessions pourraient réunir différentes équipes afin qu'elles é les problèmes rencontrés et les solutions dégagées, leur efficacité, etc. Il est également possible de créer une base de connaissances commune à l'ensemble des équipes et/ou filiales. Une telle base pourrait répertorier les processus efficaces et les erreurs à éviter de manière à être facilement consultée par tous les services.

Enfin, l'organisation pourrait choisir de collaborer avec d'autres entités évoluant dans le même secteur d'activité, ou dans un secteur complémentaire. Des partenariats sectoriels permettraient de mutualiser certains efforts, comme le recours à des experts ou des prestataires externes et de partager des contacts, des ressources ainsi que des bonnes pratiques. De tels partenariats offriraient également l'opportunité de développer des solutions standardisées, avantageuses pour tous les partenaires et ce, à moindre coût.

*iii) Résilience et adaptation*

La capacité d'une organisation à anticiper, s'adapter et gérer les changements et perturbations de son environnement (crises, changements structurels, etc.) est une qualité fondamentale dans un contexte concurrentiel, réglementaire et technologique en constante évolution. Dans le cadre de la protection des données personnelles et de la gestion des droits des personnes concernées, la résilience organisationnelle et la capacité d'adaptation du responsable du traitement vont bien au-delà de la simple conformité. Elles s'inscrivent dans une stratégie globale visant à maintenir les performances, l'agilité et la compétitivité tout en assurant une maîtrise efficiente des risques. En effet, une organisation résiliente dispose de la capacité de réduire les impacts négatifs de tout changement imprévu. Celle-ci s'appuie sur une gestion proactive des risques, sur l'anticipation règlementaire et une certaine agilité organisationnelle.

**Gestion proactive des risques.** Les risques liés aux données sont multiples : erreur humaine, incident technique, cyberattaque, sanction réglementaire, etc. Se placer dans une démarche de gestion proactive des risques permet à l'organisation de se préparer à l'occurrence de tels risques pour renforcer sa résistance tout en en limitant ses vulnérabilités. Identifier les risques constitue donc une étape nécessaire à la mise en œuvre de moyens préventifs et correctifs. Il s'agit de détecter les potentielles faiblesses ou menaces qui pourraient nuire à l'organisation ou aux relations qu'elle entretient avec les parties concernées (clients, partenaires, etc.). Parmi ces menaces potentielles, se retrouvent des risques :

- **Humains**, par l'erreur, le manque de formation, ou encore la malveillance. Ces risques représentent l'une des principales causes de la vulnérabilité des organisations ;
- **Techniques**, par la défaillance des systèmes (bug, panne, mauvaise intégration des systèmes), l'obsolescence des infrastructures, logiciels et applications, la défaillance de sécurité (incluant les cyberattaques) ;
- **Organisationnels**, par le manque de clarté ou de compréhension des processus, l'absence de supervision et/ou de leur suivi, le manque de coordination entre les services ;
- **Règlementaires**, par l'évolution des textes et/ou des positions des autorités de contrôle, ou encore le manque de traçabilité (empêchant le responsable du traitement de prouver sa conformité).

Identifier les risques est crucial pour l'organisme. Un certain nombre de mécanismes peuvent être activés pour mettre en lumière les vulnérabilités, dont notamment l'audit des processus, l'analyse des systèmes techniques (audit de sécurité, test de pénétration, simulation de crises), la collecte des retours des parties prenantes (retours des collaborateurs, feedbacks des clients/utilisateurs). Dans une logique de maîtrise des risques, la priorisation est également un élément clé de la stratégie : il s'agit de classer les risques identifiés en fonction de la probabilité de leur occurrence, de leur impact potentiel, puis de planifier les actions à mener en fonction.

Une fois ces risques identifiés et catégorisés, l'organisation peut entreprendre des actions à des fins de prévention. Ainsi, elle peut utilement s'employer à :

- La recherche des causes, via des méthodologies de gestion ;
- La mise en place de mécanismes de contrôle, plus ou moins automatisés, pour identifier les écarts par rapport aux objectifs ou aux normes réglementaires ;
- La formation des équipes ;

- Le déploiement de tableaux de bord numériques permettant le suivi d'indicateurs clés ;
- L'anticipation réglementaire.

La règlementation applicable à la protection des données personnelles peut évoluer rapidement et différer d'un pays à l'autre. Les organisations doivent alors être capables de l'anticiper et de s'y adapter pour éviter des retards coûteux en termes de mise en conformité. La capacité d'anticiper de telles évolutions permet d'éviter des ajustements précipités et onéreux. Par ailleurs, l'anticipation des risques peut renforcer la crédibilité de l'organisation auprès des parties prenantes tout en préservant l'efficacité de ses pratiques. Un tel atout peut représenter un avantage stratégique important dans un marché concurrentiel.

La veille juridique (que ce soit à l'échelle locale, régionale ou internationale) et technologique (car des solutions techniques et des pratiques nouvelles émergent constamment) peut ainsi devenir un atout majeur. Pour plus d'efficacité, la veille peut être consolidée par l'analyse des impacts des évolutions sur l'organisation afin d'envisager et de prioriser les ajustements nécessaires. De la même manière, les collaborateurs impliqués dans la gestion des données personnelles doivent être sensibilisés et formés afin de comprendre les nouvelles obligations et savoir comment les mettre en œuvre au quotidien.

**Agilité organisationnelle.** Toujours dans une logique de résilience et d'adaptabilité, l'organisation peut chercher à construire des structures et des processus flexibles afin de s'adapter au changement sans compromettre ses performances. Cette agilité organisationnelle repose sur des structures flexibles et collaboratives au sein desquelles les rôles et responsabilités sont clairement définis tout en restant adaptables. Des rôles tels que ceux de « Data steward » ou « GDPR Champion » peuvent être définis pour renforcer la gestion des données personnelles à l'échelle locale ou au sein de services et/ou de filiales. Cette agilité peut aussi reposer sur la capacité à intégrer rapidement des innovations technologiques (solutions SaaS, outils d'automatisation, etc.) sans perturber les opérations.

En complément, le déploiement de processus évolutifs, inscrits dans une logique de collaboration transversale, renforce l'agilité. Il peut s'agir de solutions techniques (workflows, plateformes d'intégration, etc.) ou de méthodologies « agiles » de gestion des projets, afin d'introduire les changements par itérations successives. Par exemple, lors de la mise en place d'un nouveau portail dédié à l'exercice de leurs droits par les personnes concernées, le responsable du traitement peut tester et améliorer la solution étape par étape, en impliquant les utilisateurs finaux à chaque phase.

La gestion proactive des risques, l'anticipation réglementaire et l'agilité organisationnelle permettent aux organisations d'évoluer avec stabilité dans un environnement complexe et changeant. Cette capacité d'adaptation ne se limite pas à la gestion des données personnelles, mais impacte positivement toutes les fonctions de l'organisation, en garantissant une meilleure efficacité et une certaine capacité d'adaptation stratégique.

### 2.3. Dimension humaine

La dimension humaine est un pilier central dans l'accroissement des capacités organisationnelles du responsable du traitement. Au-delà des outils et processus techniques, ce sont bien les individus, qui se trouvent au cœur des processus métiers, incarnent les changements et en garantissent le succès. Gérer les risques humains, développer le capital humain, responsabiliser les collaborateurs permet ainsi d'améliorer la gestion des droits, mais également de renforcer l'organisation dans son ensemble.

*i) Gestion des risques humains*

Les risques humains constituent un des facteurs les plus critiques dans la gestion des droits et des données personnelles. Ils incluent des erreurs, des omissions, ou des actes malveillants pouvant compromettre la conformité réglementaire, l'intégrité des données, la réputation de l'organisation, etc. Une gestion proactive de ces risques est donc essentielle pour assurer la résilience organisationnelle.

Les erreurs ou omissions (particulièrement problématiques dans le cadre du traitement des demandes de droits) proviennent souvent d'un manque de compréhension de la logique et des enjeux liés à la protection des données personnelles. Elles peuvent également résulter de processus mal définis. L'organisation peut donc chercher à corriger les erreurs fréquentes (par exemple dans le cadre d'une logique d'amélioration continue) et à former les équipes impliquées.

L'organisation doit également (il s'agit d'ailleurs d'une obligation imposée par le RGPD) chercher à prévenir les comportements malveillants pouvant représenter un risque majeur et engendrer une violation de données.[96] Le responsable du traitement va ainsi devoir renforcer la formalisation contractuelle des obligations mises à la charge des personnes amenées à entrer en contact avec les données. Il doit également instaurer des contrôles et des restrictions pour limiter l'accès aux données personnelles. Ainsi, il va s'assurer que seuls les

[96] Article 32 RGPD relatif à l'obligation de sécurité imposée au responsable du traitement

collaborateurs impliqués dans les processus de traitement des demandes de droits puissent effectuer certaines actions (notamment la modification ou la suppression de données).

*ii) Développement du capital humain*

En développant les compétences des collaborateurs, l'organisation peut à la fois améliorer sa performance et réduire ses vulnérabilités. La sensibilisation et la formation des équipes doivent être mis en œuvre par le responsable du traitement, qui peut également chercher à diffuser, en interne, une culture de la protection des données. Des programmes de formation réguliers permettent d'augmenter l'adhésion des collaborateurs aux processus et mécanismes mis en place pour la protection des données personnelles. De plus, ils leur permettent de s'emparer de ces thématiques à la faveur d'approches basées sur les notions de « Privacy by Design » ou de « Privacy by Default » (Voir infra : Mettre à profit le traitement des demandes de droits pour améliorer l'offre et la qualité des services). Afin de renforcer la résilience de l'organisation, ces programmes peuvent également intégrer une sensibilisation autour des enjeux liés à la cybersécurité et à l'hygiène informatique.

En parallèle, il peut être bénéfique pour le responsable du traitement de disposer de collaborateurs capables de comprendre et d'interagir avec des disciplines variées (juridique, IT, conformité, métier, etc.) et de tirer un maximum de profit de la perméabilité entre les différents services. Aussi, il peut avoir pour objectif de recruter ou de former des profils multi-expertises, capables de naviguer dans la diversité des enjeux sous-tendus par la gestion des données personnelles. Ce type de profil peut se révéler particulièrement utile pour superviser des projets complexes et multidisciplinaires ou encore afin d'établir des passerelles entre les différentes compétences impliquées (internes et, le cas échéant, externes).

*iii) Responsabilisation et culture « data-driven »*

En plus de renforcer leur capital humain, les collaborateurs peuvent être responsabilisés. Pour ce faire, elles peuvent nommer, dans chaque service, des référents chargés de superviser la gestion des données personnelles et de garantir la conformité des pratiques opérationnelles. Ces référents peuvent avoir pour mission de surveiller la qualité des données et d'identifier les failles, d'être un point relai entre les équipes métiers et le DPO, de promouvoir les bonnes pratiques RGPD, etc. Par ailleurs, une organisation assurant la promotion d'une culture de la protection de la vie privée, renforce son attractivité auprès des talents, notamment ceux cherchant à travailler dans des environnements éthiques et responsables. Une telle démarche participe à intégrer la protection de la vie privée dans les processus décisionnels. Les structures organisationnelles du responsable du traitement doivent ainsi prévoir l'implication du DPO et des collaborateurs dans les thématiques relatives à la protection des

données dès lors que de nouveaux projets, de nouvelles solutions, ou de nouveaux process, sont envisagés.

Enfin, le responsable du traitement peut placer les données au centre de ses processus décisionnels et rechercher à développer une organisation dite « data-driven », qui favorise une prise de décision basée sur des données fiables et conformes. Les données ne sont plus seulement un support pour les opérations. Elles constituent également un actif stratégique central. La conformité, la qualité et l'accessibilité des données représentent donc ici des enjeux majeurs. Il en va de même de l'utilisation d'outils d'analyse, de tableaux de bord et l'amélioration continue.

En développant ses capacités organisationnelles sur les plans opérationnels (amélioration continue, qualité des données), organisationnels (mécanismes de coordination, de collaboration, de résilience) et humains (formation, responsabilisation), l'organisation ne se contente donc pas de répondre aux seules obligations réglementaires. Elle crée une culture d’entreprise tournée vers l’adaptation, l’efficacité et l’éthique. Cette approche renforce non seulement la conformité, mais aussi la compétitivité et la pérennité de l’organisation. Elle peut alors s'attacher à développer son activité tout en renforçant son positionnement sur le marché.

# II. … POUR MIEUX SE POSITIONNER SUR LE MARCHE ET DEVELOPPER SON ACTIVITE

En complément de la maîtrise des risques (juridiques, financiers, etc.), la gestion des demandes d'exercice de droit créée un grand nombre d'opportunités pour le responsable du traitement. Ainsi, elle représente l'occasion d'approfondir ses pratiques et d'améliorer la gouvernance des données, de mieux maîtriser son système d'information, d'améliorer (en continu) ses processus, de lancer une dynamique d'automatisation, d'accroître ses capacités organisationnelles, de former ses équipes. Autant de bénéfices pouvant ruisseler sur l'ensemble de son activité.

Elle peut également constituer un véritable levier concurrentiel, à l'aire de l'information où les données captent de plus en plus de valeur et d'attention. Ainsi, par la transparence et l'innovation, l'organisation peut capitaliser sur la gouvernance et la conformité afin de se différencier et développer son activité (B), améliorer son image et générer la confiance de ses clients et partenaires (A) pour, finalement, mieux se positionner sur le marché.

## A. Accroître la transparence envers les personnes concernées : levier de création de confiance

La transparence est l'un des principes directeurs du RGPD. Elle est une base de l'ensemble de la structure fondant la protection des données personnelles. Ainsi, la transparence ne doit pas être considérée uniquement dans le cadre de la gestion des demandes de droits. En effet, l'information communiquée dans le cadre de l'exercice de ces droits ne constitue qu'un petit ensemble dans l'étendue bien plus vaste que représente l'obligation de transparence. La gestion des demandes de droit est certes englobée dans la transparence mais cette dernière ne saurait s'y réduire. En pratique, il s'agit d'un véritable droit (même s'il n'est pas explicitement proclamé) qu'ont les personnes concernées à recevoir une information transparente. Un tel droit se matérialise aussi bien en amont qu'au cours du traitement.

Ainsi, la notion d'« information » s'entend ici comme l'ensemble des éléments prévus aux articles 12 à 14 du RGPD. Elle inclue donc les informations relatives aux droits des personnes concernées et aux modalités d'exercice de ces derniers (que le responsable du traitement se doit de faciliter), ainsi que toutes les communications et éléments intervenant en réponse à une demande de droit.

Elle constitue non seulement une exigence légale mais également un levier stratégique venant renforcer les droits des personnes concernées et favoriser la confiance que le public porte à l'organisation. Ainsi, au travers de l'obligation de transparence qui lui est imposée, le responsable du traitement peut voir l'opportunité de protéger et développer sa réputation (1), dès lors que sont déployés les efforts nécessaires pour communiquer l'information la plus transparente possible (2).

# 1. Mettre à profit la transparence pour protéger et développer sa réputation

La transparence mène à la confiance, la confiance mène à l'adhésion et l'adhésion mène à l'accroissement du chiffre d'affaires. A travers une logique de transparence (1) réelle et non d'apparat (2), le responsable du traitement peut chercher à créer de la confiance et, par-là, créer de la valeur (3).

## 1.1. Notion de transparence

Le principe de transparence est à la fois une obligation imposée au responsable du traitement et un droit reconnu à la personne concernée. Il s'agit donc pour cette dernière du droit à recevoir une information pertinente, loyale et accessible. La transparence doit permettre aux personnes concernées de conserver la maîtrise de leurs données personnelles. Une telle maîtrise implique la capacité pour la personne de savoir ce que les différents acteurs font de ses données, de part et d'autre de la chaîne de traitement.

*i) Portée de la transparence*

L'article 12 du RGPD impose une obligation de transparence au responsable du traitement (voir supra : Droit à l'information). La transparence joue un rôle prépondérant tout au long du processus de traitement des demandes de droit : depuis le rappel des droits à la personne concernée jusqu'à la réponse qui lui est adressée. Selon le CEPD, l'obligation de transparence « *s'applique à trois domaines centraux :*

- *La communication aux personnes concernées d'informations relatives au traitement équitable de leurs données ;*
- *La façon dont les responsables du traitement communiquent avec les personnes concernées sur leurs droits au titre du RGPD ;*

- *La façon dont les responsables du traitement facilitent l'exercice par les personnes concernées de leurs droits »*.[97]

Par ailleurs, le législateur européen a pris soin de souligner que *« le principe de transparence exige que toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples »*.[98] Le CEPD rappelle quant à lui que « *la qualité, l'accessibilité et l'intelligibilité des informations sont aussi importantes que le contenu réel des informations en matière de transparence devant être fournies aux personnes concernées »*.[99] La transparence repose donc sur une information claire, accessible et compréhensible. Elle permet aux personnes concernées de savoir comment leurs données sont traitées, par qui, pour quelles finalités et pendant combien de temps.

*ii) Caractéristiques de la transparence*

En premier lieu, l'information doit être facilement accessible aux personnes concernées. Cette accessibilité englobe à la fois les canaux et formats de la communication. Elle s'applique également à la communication elle-même, qui doit pouvoir être comprise sans difficulté par son destinataire. Ainsi, une diversité de supports peut être envisagée pour véhiculer l'information (format écrit, format visuel, interactions directes, etc.). De plus, le langage et la terminologie employés ne doivent pas être destinés à une personne initiée, dotée d'un profil technique : tout le monde doit pouvoir comprendre l'information.

La transparence oblige également le responsable du traitement à prendre en compte les particularités dues au public concerné (niveau de connaissance de l'informatique et des technologies, capacités d'accès et de connectivité, capacités cognitives, etc.). Il convient donc d'adopter des modes de communication adaptés en fonction du public, en utilisant des canaux appropriés pour chaque situation, qu'il s'agisse d'une personne âgée, d'un enfant ou d'une personne en situation de handicap (par exemple en état de cécité visuelle, ou de handicap mental, etc…).

Ensuite, la transparence obéit à des impératifs de loyauté. L'information ne doit donc pas être ambiguë ou présentée de manière à manipuler les personnes concernées. Si le « Dark pattern » est fréquemment utilisé lorsqu'une action positive est attendue de l'utilisateur,

---

[97] CEPD, Lignes directrices sur la transparence du 11 avril 2018 (WP260), p.3, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf

[98] *Considérant 39 RGPD*

[99] CEPD, Lignes directrices sur la transparence du 11 avril 2018 (WP260), p.6, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf

il peut aussi consister à rendre difficile pour la personne concernée la compréhension claire de l'utilisation de ses données, voire à l'empêcher d'agir, par exemple en dissimulant les adresses de contact pour l'empêcher d'exercer ses droits.

De la même manière, l'information ne doit pas non plus se noyer dans un déversement d'éléments juridiques et/ou techniques. Pour autant et selon une étude menée par l'UFC QUE CHOSIR, il faudrait environ 34 minutes pour lire les Conditions Générales d'Utilisation d'un site web.[100] Une autre étude, bien que menée il y a une quinzaine d'années, démontre qu'il faudrait en moyenne 244 heures à un internaute pour lire les politiques de confidentialité de l'ensemble des sites visités en une année. Cette étude a été publiée en 2008, soit avant l'entrée en vigueur du RGPD avec lequel la consistance de telles politiques s'est vue renforcée.[101] Cela conforte bien l'idée que les Conditions Générales d'Utilisation et les politiques de confidentialité, lorsqu'elles existent, ne garantissent nécessairement une information suffisante des personnes concernées.

La transparence est également granulaire et dynamique. Granulaire, parce que les informations fournies sont pertinentes et adaptées au contexte de l'interaction avec la personne concernée. Par exemple, au moment de l'inscription sur une plateforme en ligne et avant que des données personnelles ne soient saisies, l'utilisateur doit avoir accès à l'information. Dynamique, parce que l'information doit faire l'objet d'une mise à jour régulière et proactive en fonction des modifications du contexte dans lequel s'inscrit le traitement (changement de base légale, ajout de destinataires des données, nouvelles finalités, etc…).

*iii) Limites de la transparence : un équilibre nécessaire*

Le CEPD indique que « *les informations devraient être concrètes et fiables ; elles ne devraient pas être formulées dans des termes abstraits ou ambigus ni laisser de place à différentes interprétations* ». L'accent est particulièrement mis sur les finalités et fondements juridiques du traitement.[102] L'utilisation de termes vagues doit être limitée aux cas dans lesquels il ne peut en être autrement. A titre d'exemple, le CEPD indique que des notions telles que la "*mise au point de nouveaux services*", la « *recherche* », ou encore les « *services personnalisés* » sont trop vagues et générales. En effet, elles ne permettent pas à la personne concernée de savoir précisément quelles activités et/ou services sont englobés par ces notions.

[100] Conditions générales : À l'épreuve du chrono, UFC-Que Choisir, 2022

[101] The Cost of Reading Privacy Policies, Aleecia M. McDonald, Lorrie F. Cranor, 2008

[102] CEPD, Lignes directrices sur la transparence du 11 avril 2018 (WP260), p.10, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf

Pour autant, aucune définition précise n'existe concernant la notion d' « *information compréhensible* » : elle doit être recherchée au cas par cas. Fournir trop d'informations peut avoir l'effet inverse de celui recherché. Les utilisateurs peuvent se sentir dépassés et ignorer les messages, même si ceux-ci contiennent des éléments importants. Il est alors crucial de rechercher à structurer l'information pour la rendre digeste, de trouver un équilibre entre accessibilité et complétude de l'information. Une telle approche demande des efforts de la part du responsable du traitement, notamment en termes de création de contenus, de formation des collaborateurs, etc. Ainsi, l'organisation doit documenter son approche, ses réflexions ainsi que les arbitrages réalisés dans le cadre de l'accomplissement de son obligation de transparence. Elle doit être en mesure de démontrer que les efforts nécessaires ont été entrepris et qu'elle n'a pas simplement ignoré les exigences règlementaires applicables en la matière, voire cherché à tromper les personnes concernées.

*iv) Indicateurs et mesure de la transparence*

Dans une démarche similaire à celle de l'amélioration continue (Voir supra : Amélioration continue), le responsable du traitement peut utilement chercher à mesurer l'efficacité des efforts menés dans le sens de la transparence. Il pourra ainsi mettre en place des indicateurs spécifiques (voir supra : Métriques et indicateurs), tels que des indicateurs de compréhension et des mesures de satisfaction des personnes concernées.

Par exemple, pour s'assurer de l'accessibilité et/ou de la bonne compréhension de l'information, il pourra chercher à déployer des métriques (quantitatives et/ou qualitatives) s'attachant à :

- La lecture des informations (temps passé, taux de défilement, nombre de clics sur les liens renvoyant vers l'information, etc.) ;
- La compréhension (score moyen à un quizz de vérification, taux de réussite par catégorie de personnes concernées, évolution des scores dans le temps ou en fonction de modification des supports et/ou formats de l'information, etc.) ;
- L'utilisation ou non d'un outil en particulier (fréquence d'utilisation d'un chatbot, types de questions posées, taux de résolution des demandes, etc.) ;
- La satisfaction (enquêtes concernant la clarté, la pertinence et la facilité d'accès aux informations, analyse des retours des utilisateurs, etc.).

### 1.2. Transparence réelle et « transparence washing »

La transparence repose sur les informations et engagements affichés, les efforts de communication et les déclarations publiques. Cependant, elle risque de rester purement symbolique si elle ne s'intègre pas dans une véritable gouvernance, dans des actions concrètes ou dans des capacités organisationnelles réelles. À l'inverse, la transparence réelle se base sur des pratiques concrètes, effectives et mesurables. Elle démontre que l'organisation est capable de traiter les demandes de droits des personnes concernées et d'assurer la protection de leurs données personnelles conformément aux exigences réglementaires.

La distinction entre transparence perçue et transparence réelle est cruciale dans la recherche de la confiance et de la création de valeur. Si la transparence perçue peut apporter des bénéfices à court terme, elle devient contre-productive lorsqu'elle est démasquée comme étant superficielle (méfiance accrue, impact sur la réputation, sanctions, etc.). La transparence ne doit donc pas résulter en un « effet washing », selon lequel l'organisation semble faciliter l'accès à l'information mais qu'elle la filtre en fonction de ce qu'elle souhaite communiquer ou cacher. Ce serait par exemple le cas d'une politique de confidentialité détaillée mais difficilement compréhensible, dont l'objectif serait davantage de « cocher une case réglementaire » qu'informer réellement les personnes concernées. Ce serait également le cas si, par exemple, le responsable du traitement communiquait autour de principes éthiques ou de mesures de sécurité fortes sans toutefois que les outils et/ou processus idoines ne soient implémentés.

### 1.3. Transparence, confiance et création de valeur

*i) Les enjeux liés à la protection des données personnelles dans l'opinion publique*

Selon une étude de la CNIL, 87 % des français se déclarent sensibles à l'enjeu de la protection des données.[103] D'après une étude menée par l'association GENERATION NUMERIQUE, 77,64% des mineurs paramètrent leur sécurité en ligne pour protéger leurs informations personnelles et/ou les contenus qu'ils publient (souvent aidés par des membres de leur famille).[104] Selon cette même étude, 58 % des employés de bureau de la génération Z (nés entre 1997 et 2012) déclarent (très bien) connaître les protocoles de cybersécurité de

[103] CNIL, "Scènes de la vie numérique", Cahiers IP n°8, avril 2021, consultable via le lien suivant : https://linc.cnil.fr/sites/linc/files/2023-02/cnil_cahier_ip8.pdf

[104] Etude en ligne menée par l'association Génération Numérique auprès de 6417 mineurs de 11 à 18 ans de mai à juin 2017

leur entreprise, contre 46 % des milléniaux (nés entre le début des années 80 et le milieu des années 90).[105]

Ces chiffres démontrent une prise de conscience et un intérêt croissant pour les enjeux liés à la vie privée et à la sécurité des données de la part des nouvelles générations. Informer et rassurer ses (potentiels) clients/utilisateurs devient ainsi un élément non négligeable pour attirer le public et participe à la construction d'une image positive. Cela peut permettre à une organisation d'améliorer son positionnement sur le marché et de se distinguer de la concurrence (Voir infra : Confiance numérique : un pallier stratégique). En fournissant des informations claires et en adoptant des outils transparents, l'organisation renforce la satisfaction de ses clients/utilisateurs. Ces derniers apprécient une expérience fluide et compréhensible, ce qui peut pousser leur engagement et encourager leur fidélité.

Par ailleurs, dans certains secteurs (finance, banque, santé, etc.), il est essentiel de bâtir une relation fondée sur la confiance et la transparence. Dans ces domaines, la protection des données personnelles peut devenir un critère décisif. Pour les organisations de ces secteurs, la confiance du public est fondamentale : elle impacte directement le chiffre d'affaires. A titre d'illustration, de plus en plus de banques (en ligne) mettent en avant leur transparence sur les frais bancaires et les données collectées. Cela rassure les clients et encourage leur fidélisation.

*ii) Renforcer les liens avec le public*

Il paraît raisonnable de dire qu'il est essentiel de véhiculer l'image d'une entité proche de son public, accessible et bienveillante. Cela n'a pas toujours été le cas. En des temps plus lointains, il était d'usage d'utiliser un langage formel et procédural afin d'affirmer la hauteur et la noblesse de l'exercice du pouvoir. Aujourd'hui, les temps ont changé. Le public souhaite une certaine proximité et exige de la transparence, tant de la part de la sphère publique que des acteurs privés. La manière de communiquer a été adaptée en conséquence et elle continue de l'être constamment. Dans la plupart des secteurs d'activité et à quelques exceptions près, la tendance est à créer une sensation de proximité chez le public. Le langage employé ainsi que les formes et supports de communication retenus revêtent donc un enjeu majeur en termes d'image : celui de paraître accessible et bienveillant et, surtout, de ne pas renvoyer une image froide, technique ou austère, susceptible de provoquer la méfiance, voire la défiance.

[105] Étude en ligne menée par l'institut d'études YouGov pour le compte de l'entreprise Splunk entre le 28 août et le 3 septembre 2024. Elle a interrogé 2 059 employés de bureau en France qui effectuent leur travail sur un ordinateur

Cela peut se résumer à un principe simple : tout ce que nous écrivons et publions pour une organisation impacte inévitablement son image.

## 2. Communiquer l'information de manière transparente

Le responsable du traitement doit chercher à communiquer l'information de manière transparente. Il s'agit toutefois d'une notion complexe, devant s'adapter au cas par cas et revêtant plusieurs dimensions. Le responsable du traitement devra ainsi véhiculer l'information en des termes clairs et simples (2.1), via des supports accessibles (2.2), de manière didactique et permettant de capter l'attention (2.3), tout en s'adaptant au public concerné (2.4). Enfin, il devra documenter les réflexions menées autour de l'approche retenue (2.5).

### 2.1. Véhiculer l'information en des termes clairs et simples

La transparence implique une forme de communication simple, permettant à l'information d'être comprise par tous. Cela peut se retrouver aussi bien dans la dimension verbale et sémantique que dans la dimension cognitive, propre à la personne humaine. Quoi qu'il en soit, il s'agira de présenter l'information avec clarté et de chercher à en faciliter la compréhension par les personnes concernées.

*i) Terminologie simple et accessible*

Le jargon est un langage propre à des spécialistes d'un même domaine. S'il peut leur être utile pour communiquer entre eux de manière plus efficace, il n'est pas adapté à n'importe quel public. En effet, il peut induire une perte de temps, des incompréhensions, voire une certaine frustration chez un public non averti. Il est donc à proscrire dans les communications destinées aux personnes concernées. Lorsqu'ils doivent être utilisés malgré tout, les termes techniques doivent être définis (par exemple via un glossaire, un hyperlien, une infobulle au survol, etc.).

Utiliser des titres et sous-titres informatifs, mettant en valeur les points les plus importants du document, est également un moyen de faciliter la lecture d'un document. Ces énoncés synthétiques permettent au lecteur d'anticiper le contenu du développement qu'il pourra y trouver et de se diriger directement vers les parties qui l'intéressent. A contrario, les titres vagues tels que « *Remarque* » ou « *Ce que vous devez savoir* » sont à proscrire. Par exemple, « *Comment exercer vos droits ?* » est un titre plus informatif que « *L'exercice de ses droits par la personne concernée* ». De la même manière, un court résumé du développement à venir, positionné juste en dessous du titre, peut être utile en ce sens.

De plus, recourir à des titres reprenant une structure identique peut aider le lecteur à s'orienter dans la communication. Enfin, la forme interrogative peut, en plus d'accroître son attention, l'aider à mieux appréhender la communication.

*ii) Le « plain language »*

La pratique du « plain language » vise à démocratiser l'accès à l'information et à réduire les malentendus. L'objectif est de rendre l'information intelligible dès la première lecture, ce qui s'avère particulièrement utile dans les communications juridiques et/ou techniques. Cette méthode s'appuie sur un certain nombre de principes, dont notamment :

- La simplicité du vocabulaire (utiliser des mots courants, éviter le jargon, définir les mots techniques lorsqu'ils sont inévitables) ;
- Des phrases courtes (une vingtaine de mots maximum) et directes (voix active) ;
- Une structure claire (utiliser une structure logique, des titres explicites, découper le contenu en paragraphes courts) ;
- Prendre en considération les besoins du lecteur (illustrer le propos à l'aide d'exemples concrets, organiser l'information en fonction de ses intérêts) ;
- Faire ressortir les éléments essentiels (police, listes à puces, encadrés, espacements suffisants entre les différentes sections).

Par ailleurs, des outils ou des grilles d'évaluation peuvent être utilisés pour vérifier la lisibilité, comme par exemple le « Test FLESCH-KINCAID » (pour les textes en langue anglaise), [106] ou un outil similaire adapté au français.

*iii) Usage de sigles et abréviations*

Une information transparente devrait éviter le recours aux sigles sans être certain qu'ils fassent sens pour le public ciblé (soit parce que le sigle est extrêmement commun, soit parce qu'il a au préalable été introduit dans la communication). Par exemple, le sigle « DPO » peut paraître une évidence pour des professionnels du domaine juridique ou de la conformité mais il ne permet pas forcément au large public de faire un lien avec la protection des données personnelles. À titre d'exemple « contact DPO » peut être remplacé par « contact vie privée ».

Par ailleurs, le responsable du traitement devrait préférer le recours à des abréviations aux intitulés officiels complets dès lors qu'il n'existe aucun risque de confusion. Ainsi, le

[106] Page Wikipedia (en anglais) concernant les tests Flesch-Kincaid, consultable via l'URL suivante : https://en.wikipedia.org/wiki/Flesch–Kincaid_readability_tests

« règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE » - après avoir été mentionné pour la première fois en tant que tel (« dit RGPD ») - peut ensuite être désigné au long de la communication comme le « Règlement Général sur la Protection des Données » ou « RGPD ». En effet, dès lors qu'il a été identifié une première fois en début de document et qu'il est repris par la suite sous une forme simplifiée plus aucun risque de confusion ne subsiste dans l'esprit du lecteur. Cependant, des formulations comme « le règlement » ou « la loi » sont à proscrire car trop générales et susceptibles d'introduire une confusion lorsque la communication cite plusieurs sources juridiques.

*iv) Réduire la charge cognitive*

La théorie de la charge cognitive (ou « *Cognitive Load Theory* ») a été développée par SWELLER dans les années 1980.[107] Elle se concentre sur la manière dont le cerveau humain (et notamment la mémoire) traite les informations. Elle théorise le cadre dans lequel l'information doit être présentée pour maximiser l'apprentissage et la compréhension par son destinataire. Elle est particulièrement pertinente en présence d'informations complexes et/ou techniques. Selon cette théorie, le cerveau subit trois types de charges cognitives lorsqu'il traite de l'information :

- Une charge intrinsèque, liée à la complexité de l'information, dépendant de la difficulté du concept et de l'expérience de l'utilisateur ;
- Une charge extrinsèque, liée à la façon dont l'information est présentée ;
- Une charge essentielle, liée à l'effort cognitif investi dans la compréhension et dans l'apprentissage.

Par ailleurs, la théorie de la charge cognitive indique que la capacité de la « *mémoire de travail* » (interface entre l'environnement extérieur et la mémoire à long terme, servant à l'assimilation de connaissances) est limitée. En effet, selon la loi de Miller, [108] une personne moyenne ne peut conserver que 7 (plus ou moins 2) éléments dans sa mémoire de travail.[109] Le cerveau humain ne peut en effet traiter que quelques éléments d'information à la

[107] Académie d'Aix-Marseille, La Théorie de la charge coginitive, 30 octobre 2022, consultable via l'URL suivante : https://www.pedagogie.ac-aix-marseille.fr/jcms/c_11061280/en/la-theorie-de-la-charge-cognitive

[108] Page du site Laws of UX dédiée à la Loi de Miller, consultable via l'URL suivante : https://lawsofux.com/fr/loi-de-miller/

[109] Page wikipedia : The Magical Number Seven, Plus or Minus Two, consultable (en anglais) via l'URL suivante : https://en.wikipedia.org/wiki/The_Magical_Number_Seven,_Plus_or_Minus_Two

fois. Si cette capacité est dépassée, l'apprentissage et la compréhension en sont impactés de manière négative. Par exemple, un numéro de téléphone « 457812309 » est plus facile à retenir lorsqu'il est segmenté : « 457-812-309 ».

Pour une information accessible, rechercher à réduire la charge cognitive est alors un prérequis nécessaire. Le responsable du traitement peut ainsi chercher à minimiser la charge extrinsèque (organiser et structurer l'information, réduire les informations superflues, etc…) et à optimiser la charge essentielle (rationaliser les efforts investis par les personnes concernées dans l'assimilation de l'information).

*v) Le « chuncking »*

Directement issu des travaux de Miller,[110] le terme de « chuncking » renvoi à une pratique consistant à morceler l'information. Présentée en petites unités de blocs logiques, l'information est plus facilement traitée par la « *mémoire de travail* ». En effet, « *lorsqu'on lit un texte, on ne déchiffre pas chaque caractère l'un après l'autre ni même chaque mot l'un après l'autre. L'œil perçoit les choses de manière plus globale. Il balaie le texte et enregistre des blocs, des ensembles textuels. Il transmet alors ces ensembles successifs au cerveau qui les interprète afin d'en dégager une signification ».* Il est donc de mise de veiller à ce que « chaque ensemble visuel coïncide avec un ensemble de sens ».[111]

Illustration du « Phénomène des ensembles textuels » : Parvenez-vous à déceler l'erreur ?

*Pour leur sécurité, placez*
*Les enfants à l'arrière de*
*de votre voiture*

Pour schématiser, la « *mémoire de travail* » (traitant un nombre limité d'éléments simultanément) se distingue de la mémoire à long terme (rassemblant des éléments de connaissance préexistants et les rappelant dans le cadre des activités de la mémoire de travail). Le « chuncking » vise à réduire la quantité d'éléments à traiter en les regroupant de manière significative et à faciliter le rappel d'éléments stockés dans la mémoire à long terme. Il associe les informations à des « schémas » préexistants et les rend plus faciles à intégrer.

[110] Page du site Laws of UX dédiée au « chunking » sur le site Laws of UX, consultable via l'URL suivante : https://lawsofux.com/fr/morceau/

[111] Ecrire pour être lu, Ministère de la communauté française de Belgique, 2009, p.31, consultable via le lien suivant : https://www.federation-wallonie-bruxelles.be/index.php?id=detail_article&no_cache=1&tx_cfwbarticlefe_cfwbarticlefront[action]=show&tx_cfwbarticlefe_cfwbarticlefront[controller]=Document&tx_cfwbarticlefe_cfwbarticlefront[publication]=1272&cHash=7b620588f5b77ee8d5b49df426095388

Le découpage en blocs d'information permet au cerveau d'en organiser et d'en hiérarchiser le traitement. Il peut s'agir de découper le texte selon des catégories logiques, des thématiques ou encore des étapes.

Le « chuncking » permet de suivre le rythme naturel de lecture et donc de respecter le mécanisme de lecture. En évitant les entraves cognitives (retour à la ligne découpant un ensemble textuel logique, insertion de parenthèses pour marquer les possibilités d'accord en genre et en nombre, etc.), il cherche à réduire la charge cognitive pesant sur le lecteur. Celui-ci dispose donc de plus de ressources qu'il peut alors consacrer à la compréhension ou l'assimilation des informations.

Cette technique est utilisée dans de nombreux contextes, comme l'apprentissage, la lecture, la mémorisation ou la prise de décision. Elle l'est particulièrement dans le cadre de la conception d'interfaces « user friendly » et dans la communication d'une information accessible aux personnes concernées.

Illustration du « chuncking » :

« Les droits des individus garantissent l'accès aux données personnelles. Vous pouvez demander la rectification, l'effacement ou la limitation des traitements ».

Devient, une fois cette technique appliquée :

« **Vos droits** :

- Accès à vos données personnelles.
- Rectification de vos informations.
- Effacement ou limitation des traitements ».

*vi) Bionic Reading*

Le « Bionic Reading » est une méthode de mise en forme des caractères dans l'objectif de faciliter la compréhension et la lecture du texte. Une telle méthode consiste à mettre en évidence certaines parties des mots. Il s'agit d'accentuer (mettre en gras) certaines lettres ou

parties de mots afin de guider les yeux et le cerveau. Cela permet d'accentuer le traitement visuel et cognitif.[112]

Bien qu'elle n'ait pas fait l'objet d'études approfondies, ni de publication scientifique, elle s'appuie sur certaines théories de la science cognitive et des neurosciences. Ainsi, cette approche résulte du constat que notre cerveau ne lit pas des lettres mais des mots, en les reconnaissant d'une manière globale à partir des premières lettres qui le composent : il s'agit de la théorie de la reconnaissance des mots (« Effet de supériorité du mot »[113] ; « Modèle d'activation interactive »[114] ; « Effet de prévisibilité du mot »[115] ; « Recherches sur les zones cérébrales impliquées dans la lecture »,[116] notamment).

Dans la continuité de ces théories, la technique du « Bionic Reading » permettrait de :

- Faciliter la lecture pour certains publics, comme les dyslexiques (dont certains ont pu témoigner que cela aidait à guider les yeux et permettait de réduire la confusion entre les lettres), ou ceux souffrant de troubles de l'attention (TDAH) ;
- Gagner en vitesse de lecture, l'information pouvant être parcourue et comprise plus rapidement (aspect non négligeable au vu de nos pratiques en termes de navigation sur le web).

Le « Bionic Reading » est donc une méthode intéressante bien qu'elle manque encore de validation scientifique. Elle peut être utile pour certains publics, mais pas pour tous. Un certain nombre d'approches alternatives existent. Pour cette raison, le responsable du traitement devrait tester plusieurs approches adaptées aux catégories de personnes concernées pour pouvoir évaluer l'impact et l'efficacité des méthodes entreprises en termes de transparence de l'information.

---

[112] Voir du site Bionic Reading dédiée à la méthode employée, consultable via l'URL suivante : https://bionic-reading.com/br-method/

[113] REICHER, 1969, voir : https://www.guichetdusavoir.org/question/voir/21788

[114] RUMELHART & MCCLELLAND, 1981, voir : https://www.researchgate.net/figure/Schema-du-modele-a-Activation-Interactive-de-McClelland-et-Rumelhart-1981-A-gauche-la_fig1_311743821

[115] RAYNER, 1999, voir à ce sujet Andréanne PLAMONDON ,Thèse de recherche intitulée Le traitement lexical préliminaire est-il suffisant pour sauter un mot de fonction lors de la lecture des phrases, présentée à l'Université de Moncton, 2015, p.1, consultable via l'URL suivante : https://udmscholar.cairnrepo.org/fr/islandora/object/umir%3A1923/datastream/PDF/view/citation.pdf

[116] DEHAENE & COHEN, 2007, voir en ce sens : Sylviane Valdois. L'apprentissage de la lecture. Nicolas Poirel. Neurosciences Cognitives Développe- mentales, De Boeck, 2020, p.15, consultable via l'URL suivante : https://hal.science/hal-04548984/document

### 2.2. Véhiculer l'information via des supports accessibles

*i) Emplacement des informations non liées à la protection de la vie privée*

La transparence s'applique aussi bien au contenu de l'information qu'à l'emplacement où les personnes concernées peuvent la trouver. Elle doit ainsi pouvoir être consultée à tout moment sans que cela exige d'effort particulier de leur part. Selon la position du CEPD, cela implique de présenter une information relative aux données personnelles de façon distincte et « *clairement différenciée des autres informations non liées à la vie privée telles que des clauses contractuelles ou des modalités d'utilisation générale* ».[117] Il est par exemple explicitement proscrit d'insérer la politique de confidentialité à l'intérieur des Conditions Générales d'Utilisation d'un site web, au même titre qu'il paraît très peu utile d' « *informer* » une personne concernée en recourant à une pancarte affichée tout en haut d'un des murs d'un supermarché ou d'une gare. Dans la même logique, les informations relatives aux modalités d'exercice des droits doivent pouvoir être facilement consultées par la personne concernée et ne doivent donc pas se fondre au sein d'un flux d'éléments textuels.[118]

> Une bonne pratique, sur les sites web et applications, consiste à ne jamais séparer de plus de deux clics la personne concernée de l'information. Par exemple, un lien vers la politique de confidentialité peut être inséré en bas de page du site web ou de l'interface de l'application afin de permettre à l'utilisateur de pouvoir accéder à l'information quand il le souhaite, tout au long de la navigation ou de l'utilisation.

*ii) Mise à jour de l'information*

Lors de la communication d'une mise à jour (par exemple une nouvelle version de la politique de confidentialité), il est de bon aloi de mettre en avant les modifications qui ont été introduites par la nouvelle version. Afin de mettre en valeur les différents points et les informations qui ont été modifiées, le responsable du traitement peut, par exemple, utiliser un code couleur ou une police spécifique ou les reporter au sein d'un encadré ayant un titre comme « *Quelles sont les modifications introduites par cette nouvelle version ?* », etc.

[117] CEPD, Lignes directrices sur la transparence du 11 avril 2018 (WP260), p.6, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf

[118] Ibid.

Le CEPD recommande de communiquer de telles modifications à la personne concernée d'une manière spécifique, par exemple au moyen d'une communication Adhoc.[119]

*iii) Supports techniques*

Lorsqu'il déploie des interfaces destinées à être utilisées par les personnes concernées (telles que des API ou des tableaux de bord numériques), le responsable du traitement doit veiller à les rendre intuitifs et simples d'utilisation. Ainsi - et suivant la logique décrite plus en avant - il s'assurera que les informations sont facilement accessibles et que l'exercice des droits n'est en rien entravé par la conception, la présentation et/ou l'aspect de l'interface.

Par ailleurs, il peut être judicieux d'utiliser un QR Code afin de renvoyer les personnes concernées vers la communication appropriée. Ce sera le cas en présence d'objets connectés dénués d'écran. Il faut toutefois noter que l'utilisation de QR Code peut représenter un risque, pour les utilisateurs, en termes de sécurité (« Quishing »). Par conséquent, ce support ne devrait pas être utilisé en toutes situations.

*iv) Approche à plusieurs niveaux*

Lorsque la densité de l'information le nécessite, il est possible d'en faciliter l'accès par les personnes concernées, en adoptant une approche à plusieurs niveaux, prenant en considération « *les informations que la personne concernée considère en général comme les plus pertinentes* ».[120]

Cette approche consiste dans le fait de structurer et de présenter l'information en plusieurs temps. En premier lieu, la personne concernée va bénéficier d'un aperçu clair des informations relatives au traitement de ses données. Les informations les plus significatives (en considération de ses droits et libertés) lui seront alors présentées. Le CEPD les qualifie d'informations ayant « *le plus d'incidence pour la personne concernée* ».[121] Elle sera également informée qu'il lui est possible de trouver des informations plus détaillées concernant l'utilisation de ses données. L'emplacement de ces informations complémentaires et l'articulation des différentes couches d'information doivent lui être précisés.

Bien qu'elle permette de concilier la complétude et la concision d'une information complexe et/ou longue, cette approche n'est pas envisageable dans n'importe quel cas de figure. En

[119] CEPD, Lignes directrices sur la transparence du 11 avril 2018 (WP260), p.19, consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf

[120] CEPD, Lignes directrices relatives au droit d'accès n°01/2022 du 28 mars 2023, p.54

[121] Ibid.

effet, elle ne doit pas conduire à entraver l'accès des personnes concernées à une information pertinente. L'approche à plusieurs niveaux doit donc créer une valeur ajoutée. Son utilisation par le responsable du traitement doit dépendre de la nature et de l'ampleur des traitements qu'il met en œuvre.

Une approche à plusieurs niveaux n'est pas exclusive à un environnement numérique et peut très bien s'imaginer dans des hypothèses où l'information est véhiculée via des supports physiques ou à l'oral. Ainsi, des informations d'une importance supérieure peuvent être communiquées à la personne concernée à un premier niveau d'information (discussion téléphonique, document papier), alors que les informations complémentaires lui seront transmises par un autre canal (document papier plus conséquent, courriel, boite vocale).

Dans le cadre d'une communication comportant un grand nombre de données (par exemple au titre du droit d'accès ou à la portabilité), une approche à plusieurs niveaux peut s'avérer nécessaire. Les différents niveaux peuvent être présentés comme des options parmi lesquelles la personne concernée peut choisir, par exemple :

- Option 1 : données relatives au traitement A ;
- Option 2 : données relatives au service optionnel X ;
- Option 3 : données brutes ou techniques)

*v) FAQ*

Les "Foires aux Questions" (FAQ) constituent un outil clé pour favoriser la transparence de l'information. Elles permettent de rendre les informations complexes plus claires, accessibles et compréhensibles pour un large public. Le format interrogatif permet de provoquer un certain nombre de réactions cognitives et notamment :

- Un « Effet de curiosité naturelle » (« Curiosity gap »), théorisé par LOEWENSTEIN (1994), agissant comme un « déclencheur cognitif » poussant le cerveau à chercher une réponse.[122]
- Un « Effet de questionnement actif », théorisé par MEISTER & CHAPMAN (1996), dont les études ont démontré que la forme interrogative (et particulièrement l'auto-

[122] Voir ce sens la page dédiée aux travaux de Georges LOEWENSTEIN du site web The Décision Lab, consultable via le lien suivant : https://thedecisionlab.com/fr/thinkers/economics/george-lowenstein

questionnement) permet de traiter activement l'information et d'améliorer les processus de compréhension.[123]

- Un « Effet de génération », théorisé par SLAMECKA & GRAF (1987), dont les travaux ont démontré que les individus retiennent mieux les informations lorsqu'ils sont amenés à générer activement des réponses plutôt qu'en lisant passivement une déclaration.[124]

Les FAQ représentent ainsi un certain nombre d'avantages pouvant se révéler particulièrement utiles dans le contexte de la transparence de l'information, à savoir :

- Traduire le langage juridique en langage simple et clair ;
- Créer une connexion émotionnelle avec l'utilisateur afin de capter son attention et de rendre l'information plus engageante ;
- Stimuler la curiosité et motiver les utilisateurs à explorer les réponses ;
- Rendre l'information accessible et compréhensible en la reliant aux préoccupations concrètes des lecteurs (mise en situation concrète, réponses spécifiques à leur situation) ;
- Structurer l'information, réduire la charge cognitive et aider à trouver rapidement les réponses que les utilisateurs cherchent.

Elles ont pour objectif de simplifier les échanges entre les organisations et les utilisateurs, de renforcer la confiance et de montrer que l'organisation est engagée dans une démarche de conformité proactive. En réduisant les incompréhensions et en facilitant l'exercice des droits, elles contribuent directement à de meilleures relations entre les parties prenantes et le responsable du traitement.

Toutefois, ce dernier doit veiller à encadrer la FAQ de manière à limiter les questions non pertinentes et à réduire au maximum la complexité des échanges (réponses courtes, simples et adaptées au public concerné). En effet, une FAQ surchargée peut voir son efficacité réduite de manière significative, augmenter la charge cognitive pesant sur les personnes concernées et, finalement, s'avérer contre-productive.

[123] Rosenshine, B., Meister, C., & Chapman, S. (1996). Teaching Students to Generate Questions: A Review of the Intervention Studies. Review of Educational Research, consultable (en anglais) via l'URL suivante : https://www.scirp.org/reference/referencespapers?referenceid=2714637

[124] J. SLAMECKA, The Generation Effect: Delineation of a Phenomenon, Journal of Experimental _ Human Learning & Memory, 1978

Par ailleurs, l'utilisation d'un chatbot constitue une forme plus aboutie de la FAQ. La personne concernée peut ainsi poser ses questions d'une manière directe et y trouver une réponse, par une voie automatisée.

**Exemples de questions d'une FAQ :**

- Quelles données personnelles collectez-vous ?
- Pourquoi collectez-vous mes données ?
- Pendant combien de temps conservez-vous mes données ?
- Comment puis-je accéder à mes données ?
- Puis-je demander la suppression de mes données ?
- Je ne suis plus intéressé.e par le service X, comment puis-je l'arrêter ?
- Puis-je transmettre mes données vers une autre plateforme ?
- Que se passe-t-il si je décide de retirer mon consentement ?

### 2.3. Véhiculer l'information de manière didactique / capter l'attention

Au même titre que l'utilisation de la forme interrogative, le responsable du traitement peut chercher à capter l'attention de la personne concernée et à rendre l'information didactique (et donc plus facilement assimilable), que ce soit par la structure ou le support véhiculant l'information, l'utilisation d'éléments graphiques et visuels, etc.

Selon la « Théorie du double codage » (PAIVIO, 1969), le fait d'associer un texte à un visuel/une illustration permet de mieux assimiler l'information.[125] De plus, la « Théorie cognitive de l'apprentissage multimédia » (MAYER, 2009)[126] affirme que des supports d'information combinant des visuels et des textes succincts améliorent la compréhension, car ils répartissent la charge cognitive entre les différentes modalités sensorielles (verbales et picturales).[127] Le responsable du traitement peut donc utilement recourir à des éléments visuels afin de compléter et d'enrichir l'information communiquée aux personnes concernées.

---

[125] A. Paivio, Mental imagery in associative learning and memory. Psychological Review, 1969, consultable via l'URL suivante : https://loterre.istex.fr/P66/fr/page/-R0V3S7S8-W

[126] Vidéo de la Chaîne YouTube Jean-Paul GOURDANT, intitulée "Modèle multimédia - Richard Mayer" expliquant le modèle de Mayer et les fondements de la Théorie cognitive multimédias, accessible via l'URL suivante : https://www.youtube.com/watch?v=gIi4kPJUDbM

[127] Publication autour du modèle Mayer, Université de Génève, disponible via l'URL suivante : https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=http://tecfaetu.unige.ch/staf/staf-i/sangin/CLEAP/memoire/Introduction_cyril&ved=2ahUKEwjYr5-upYeLAxVkUaQEHXPCPbwQFnoECBYQAQ&usg=AOvVaw3n-2dF55SmH7DKZUxtooR_

Toutefois, trop d'éléments visuels peuvent se révéler contre-productifs, alourdissant la charge cognitive pesant sur la mémoire de travail de la personne concernée. Le responsable du traitement devra donc s'assurer de la pertinence et de la plus-value apportée par les illustrations.

Ainsi, il peut, dans un objectif de transparence, proposer aux personnes concernées des représentations visuelles du cycle de vie ou des flux de données. A noter que dans le cadre des traitements reposant sur le consentement, cela peut permettre de les projeter dans une simulation ou de leur offrir un aperçu des conséquences du partage ou non de leurs données personnelles (ex. : « Voici ce qui se passe si vous autorisez l'accès à votre géolocalisation »).

Par ailleurs, le RGPD[128] et le CEPD invitent les responsables du traitement à utiliser une iconographie dans le but d'alléger la charge d'information textuelle et de permettre à la personne concernée d'être informée d'un simple coup d'œil. Toutefois, cela requiert l'existence de symboles universels (à tout le moins communément admis par le public de l'ensemble de l'espace européen). C'est à la Commission européenne que le RGPD dévolue le rôle de créer de telles icônes. Mais à ce jour, aucun travail en ce sens n'a été publié. Toutefois, des initiatives en la matière ont été entreprises aussi bien par des autorités, notamment la CNIL (via son centre de recherche : le LINC),[129] que par le secteur privé (par exemple l'initiative suisse « Privacy Icons », réunissant MIGROS, SWISSCOM, CFF et le CREDIT SUISSE).[130]

Dans un même temps, certaines illustrations peuvent paraître relativement naturelles et évocatrices. Elles peuvent être utilisées, notamment dans le cadre de l'information relative au droit des personnes. Par exemple : un œil pour « regarder » (droit d'accès), un crayon pour « corriger » (droit de rectification), un symbole de poubelle pour « supprimer » (droit à l'effacement), un panneau « sens interdit » ou une main levée pour « s'opposer »).

*vi) Storytelling*

Le « *storytelling* », ou l'art de raconter des histoires, est une technique puissante pour capter l'attention et favoriser la mémorisation. Il part du principe que les histoires captent davantage l'attention des lecteurs que les textes simplement factuels. La forme narrative permet également de transformer des concepts complexes en exemples concrets et humanisés. De plus, les histoires génèrent de l'empathie et favorisent l'adhésion du public aux

[128] Considérant 60 RGPD

[129] Voir les travaux du LINC en ce sens, consultables via l'URL suivant : https://design.cnil.fr/design-patterns/utiliser-des-icones/

[130] Voir en ce sens le site web Privacy Icons, consultable via l'URL suivante : https://privacy-icons.ch/fr/panneaux-de-signalisation-pour-la-protection-des-donnees/

messages communiqués. Par ailleurs, les bénéfices positifs de l'approche narrative dans un contexte pédagogique sont communément admis.

Sur le plan scientifique, les bénéfices du « *storytelling* » ont fait l'objet d'un certain nombre de travaux dont, notamment :

- La « Théorie des transports narratifs », selon laquelle les histoires persuasives permettent d'augmenter la réceptivité des destinataires et d'ancrer des messages plus facilement (GREEN & BROCK, 2000). Cela s'explique par l'engagement émotionnel et l'immersion narrative (mécanisme d'identification, activation des zones émotionnelles di cerveau, etc.).[131]
- Une recherche menée par ZAK (2013) dans le domaine des neurosciences a révélé que les histoires augmentent la production d'ocytocine (hormone de la confiance et de l'empathie), rendant les individus plus réceptifs et plus enclins à agir.[132]

Concrètement, le responsable du traitement peut utilement chercher à véhiculer l'information aux personnes concernées à travers une histoire. Celle-ci pourrait mettre en scène un personnage (avatar) et un contexte narratif (problème, solution, message clé) auxquels les personnes concernées peuvent s'identifier. Plutôt que d'énumérer les droits, l'histoire pourrait par exemple illustrer chacun d'entre eux. Cela peut aussi bien s'appliquer au cycle de vie des données, qu'au contexte du/des traitement(s) mis en œuvre par le responsable du traitement, ou encore aux droits reconnus aux personnes concernées. L'effet d'identification peut être recherché en fonction des catégories de personnes concernées (par exemple une histoire avec une grand-mère et son petit-fils, un étudiant, des parents, etc.).

*vii) Supports ludiques*

Tout un ensemble de supports ludiques peuvent être employés par le responsable du traitement pour accroître la réceptivité des personnes concernées à l'information qu'il souhaite communiquer. Il peut ainsi chercher à les encourager à s'approprier ses services, à renforcer

[131] Voir à ce sujet l'article P. DE PECHPEYROU, P. NICHOLSON et S. EMERIAU, "Les histoires des marques sur leur site Internet : une histoire de transport narratif", Décisions Marketing n°95 57-76, 2019, p.58, disponible via l'URL suivant : https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://shs.cairn.info/article/DM_095_0057/pdf%3Flang%3Dfr&ved=2ahUKEwjOtrjI_4mLAxXLLPsDHQbQJIAQFnoECCAQAQ&usg=AOvVaw0ZDKUc4oL4aFAS261x3-ut

[132] Voir en ce sens la conférence TED de Paul ZAK intitulée "Trust, morality -- and oxytocin?", consultable via l'URL suivante : https://www.ted.com/talks/paul_zak_trust_morality_and_oxytocin

leur implication et, par conséquent, à accroître leur implication, leur confiance et leur engagement.

Les BD ou « *Webtoon*s », constituent un support ludique parfait pour vulgariser et rendre accessibles les concepts communiqués concernant la protection des données personnelles. Quelques exemples démontrent l'efficacité de ce support. Ainsi, un format BD peut expliquer le règlement DORA[133] ou encore, dans un autre domaine, la célèbre BD “Le Monde sans fin”, traitant du sujet de l'urgence climatique.[134] Dans une même logique, ce format pourrait mettre en scène des personnages confrontés à des problématiques de confidentialité sous la forme d'un scénario court et illustré.

D'autres formats peuvent également permettre au responsable du traitement de créer un effet similaire et de renforcer l'impact de l'information communiquée aux personnes concernées :

- « *Serious games* » ou mini-jeux en ligne, où l'utilisateur peut s'informer quant à la protection de ses données par exemple, au travers d'un jeu de question-réponse ou encore d'un « escape-game ».
- Quizz interactifs, permettant également de vérifier la bonne compréhension des informations par les personnes concernées.

### 2.4. Véhiculer l'information adaptée au public concerné

Dans le cadre de la transparence, le responsable du traitement doit adapter le format et le contenu de l'information en fonction des spécificités propres à chaque catégorie de personnes concernées. En effet, la manière de recevoir et d'assimiler l'information, les capacités cognitives, la « vulnérabilité », la connaissance des enjeux et la maîtrise de l'environnement numérique peuvent différer d'une personne à l'autre, notamment en fonction de son âge, de son état de santé, etc. Le fait que le responsable du traitement informe des enfants, des personnes âgées, des personnes en situations de handicap, des personnes malades, étrangères, etc. doit donc être pris en considération pour modeler l'information communiquée.

Par ailleurs, dans le cadre de la navigation sur le web, il est nécessaire de prendre en considération les pratiques des internautes en termes de concentration et de lecture des

[133] Voir Marc LEDIEU, “Le Règlement UE DORA du 14 décembre 2022 en 100 slides !”, 2023, disponible via l'URL suivante : https://technique-et-droit-du-numerique.fr/439-le-reglement-ue-dora-2022-2554-du-14-decembre-2022-en-100-slides/

[134] C. BLAIN & J.M. JANCOVICI, “*Le Monde sans fin”, DARGAUD, 2021

informations. En effet, le temps moyen passé sur un même site web diminue[135] et les utilisateurs passent de moins en moins de temps sur une même page. Ce temps est en moyenne de 2 minutes et 17 secondes en 2025 (même s'il fluctue en fonction du secteur d'activité).[136]

Ce constat laisse donc entrevoir l'existence d'un déficit d'attention du public dans le cadre de la navigation sur Internet. Un tel déficit d'attention peut-il conduire à considérer l'internaute moyen comme « vulnérable » ? Un parallèle peut ici être fait avec la protection des consommateurs, fixant un certain nombre de règles en matière d'information des clients dans le cadre de la grande distribution. C'est en tout cas une particularité non négligeable lorsqu'il s'agit d'informer les personnes concernées via, par exemple, une politique de confidentialité insérée sur le site web de l'organisation.

*i) Information destinée aux enfants*

Une lecture conjointe des considérants 38 et 58 du RGPD laisse apparaître une volonté forte du législateur européen de conférer une protection spécifique aux enfants. A ce titre, le vocable, le style et le ton de l'information doivent être adaptés aux capacités cognitives propres aux enfants et à leur faible conscience des enjeux propres à la protection des données personnelles. Ces derniers doivent, au même titre que n'importe quelle autre personne concernée, être en mesure d'exercer leurs droits. De plus, comme pour n'importe quelle autre personne concernée, le responsable du traitement doit faciliter l'exercice de leurs droits.

D'autre part, pouvoir capter la confiance des parents est un enjeu majeur. Ainsi, la vague de sanctions prononcées à l'encontre de TIKTOK par les autorités de contrôle de nombreux pays européens à l'encontre des pratiques du réseau social en matière d'ouverture de comptes à des mineurs - et la reprise de celle-ci dans par les médias - a été dommageable pour sa réputation. Le consentement des parents / titulaires de l'autorité parentale est nécessaire lorsqu'il s'agit de fournir des services / collecter des données concernant des mineurs (enfants d'un âge minimal situé entre treize (13) et seize (16) ans au sens du RGPD[137] et les enfants

[135] Voir en ce sens les résultats de l'étude menée par ContentSquare en 2022 et consultable via le lien suivant : https://contentsquare.com/fr-fr/blog/temps-moyen-passe-page-web/?utm_source=chatgpt.com

[136] Etude menée par SiteW, consultable via l'URL suivante : https://www.sitew.com/Comment-developper-son-entreprise-en-ligne/Analyse-et-statistiques-de-votre-site?utm_source=chatgpt.com

[137] Article 8 RGPD

de moins de quinze (15) ans au sens de la législation française).[138] Il semble donc raisonnable de penser que le fait de ne pas s'attirer la méfiance des parents est un prérequis fondamental pour pouvoir toucher ce public.

Afin de s'adapter aux spécificités d'un public composé d'enfants, le responsable du traitement peut décider d'adopter une approche exploitant le mécanisme du renforcement positif. Dans la mesure où des informations complexes pouvant leur paraître intimidantes ou trop abstraites leur sont présentées, les enfants doivent être encouragés. Le renforcement positif vise à développer leur confiance en eux-mêmes en soulignant leur capacité à comprendre les enjeux de la protection de leurs données et à agir pour exercer leurs droits, retirer leur consentement, etc. Il vise à transformer l'apprentissage en une expérience agréable et motivante et à montrer aux enfants les bénéfices directs de leurs actions. Le renforcement positif aspire également à favoriser l'autonomie et à valoriser les actions positives de l'enfant.

Une telle approche d'encouragement (« *empowerment* ») peut prendre la forme d'une formulation valorisante et amusante pour les enfants, du style : « *en posant des questions sur les données, tu prends soin de ta vie privée et de celle de ta famille, comme un pirate protège son trésor, comme un super héros protège Gotham City* » ; « C'est grâce à toi que tes données sont en sécurité, plus tu poses de question, plus tu es protégé » ; « *Quand tu demandes comment tes données sont utilisées, tu montres que tu intelligent et attentif, que tu es un grand* », etc. Elle peut également prendre la forme d'une histoire inspirante en insistant par exemple sur les bénéfices de la responsabilité dont a fait preuve le héros, d'une activité interactive (quizz, jeux de rôle, etc.) et s'appuyer sur des supports ludiques.

*ii) Information destinée à des personnes vulnérables*

Lorsque l'information est destinée à un public vulnérable, notamment des personnes âgées ou en situation de handicap, le support, le formalisme de la communication et la terminologie utilisée doivent être adaptés aux spécificités et aux besoins particuliers de ces catégories de personnes concernées. De la même manière, les modalités d'exercice de leurs droits se doivent d'être envisagées depuis leur perspective. Ainsi, le responsable du traitement peut démontrer qu'il s'insère dans une dimension éthique et réduire la « fracture numérique » concernant les services qu'il dispense. Ainsi, les personnes âgées sont souvent non familiarisées avec l'informatique et les concepts y afférents. Elles peuvent également connaître des troubles cognitifs liés à l'âge (problèmes de vue, d'audition, etc.). Les supports de

[138] Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (et notamment son article 4), consultable via l'URL suivante : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047799533

l'information peuvent donc être adaptés à ces spécificités : le responsable du traitement adapte la taille de la police et les contrastes, diffuse l'information via des médias plus traditionnels (papier, affiches pour les personnes qui ne seraient pas à l'aise avec Internet), voire met en place une solution téléphonique (assistance téléphonique et/ou boîte vocale).

De la même manière, les personnes en situation de handicap peuvent également avoir besoin que l'information soit adaptée à certaines déficiences qui pourraient entraver leur capacité à recevoir l'information (par exemple mal ou non-voyance). L'organisation peut ainsi s'inscrire dans une démarche d'inclusivité - moderne et socialement valorisée - et renforcer son image auprès du public.

Par ailleurs, une obligation d'accessibilité numérique[139] a été imposée à un certain nombre d'acteurs en France (administration et collectivités territoriales, entreprise réalisant un chiffre d'affaires annuel supérieur à deux-cent millions d'euros (250M EUR).[140] En ce qui concerne le secteur privé, l'on peut se risquer à anticiper que ce seuil constitue une base de départ (aujourd'hui élevé et concernant donc des services d'une certaine importance dans la vie quotidienne) et qu'il sera amené à être réduit par la suite. L'accessibilité numérique peut donc être pensée dès à présent par les responsables du traitement. Elle peut également s'envisager en parallèle de l'obligation de transparence.

Certaines méthodologies et principes peuvent aider le responsable du traitement à présenter et adapter l'information et les vecteurs de sa communication. On peut notamment citer la méthode FALC et les principes portés par le Référentiel Général d'Amélioration de l'Accessibilité (RGAA).[141]

La méthodologie FALC (pour "Facile à Lire et à Comprendre")[142] permet d'adapter l'information de manière à la rendre accessible au plus grand nombre. Elle est particulièrement adaptée aux personnes connaissant des difficultés de lecture ou des handicaps cognitifs. Elle peut également profiter à toute personne mal à l'aise avec l'écrit d'une manière générale (personnes

[139] Article 47 Loi du 11 février 2005 pour légalité des chances, la participation et la citoyenneté des personnes handicapées, consultable via l'URL suivante : https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000809647

[140] Décret n° 2019-768 du 24 juillet 2019 relatif à l'accessibilité aux personnes handicapées des services de communication au public en ligne (notamment ses articles 1 et 2), consultable via l'URL suivante : https://www.legifrance.gouv.fr/loda/id/LEGIARTI000038956842/2019-07-26/#LEGIARTI000038956842

[141] RGGA 4, publié le 16 septembre 2019, dans sa version du 18 avril 2023, consultable via l'URL suivante : https://accessibilite.numerique.gouv.fr.

[142] Voir la page du ministère de la Culture dédiée à la méthodologie FALC, consultable via l'URL suivante: https://www.culture.gouv.fr/Thematiques/developpement-culturel/Culture-et-handicap/Facile-a-lire-et-a-comprendre-FALC-une-methode-utile

ne parlant pas le français, personnes illettrées). La méthode FALC prévoit plusieurs principes clés et notamment de :

- Simplifier le vocabulaire (utiliser des mots courants, toujours employer un même mot pour désigner une même chose) ;
- Utiliser des phrases courtes (construction linéaire et directe) ;
- Utiliser des images ou des pictogrammes ;
- Aérer la mise en page (espacement des paragraphes, alignement du texte à gauche, usage de listes à puces, etc.) ;
- Utiliser des titres courts et explicites ;
- Tester le contenu avec des personnes appartenant à la catégorie concernée.

Il est possible de faire valider les pages web, ou autres documents par des associations spécialisées (par exemple l'UNAPEI en France).[143]

D'autre part, le RGAA (s'inscrivant dans le cadre réglementaire français en matière d'inclusivité et d'accessibilité numérique) recommande un certain nombre de pratiques spécifiques pour répondre aux besoins des personnes en situation de handicap et notamment de :

- Fournir des alternatives aux contenus non textuels (textes de remplacement pour les images, icônes, graphiques, vidéos). Par exemple, une image représentant un formulaire doit être accompagnée d'une balise indiquant « Formulaire d'inscription » ;
- Faciliter la navigation : (contenus et fonctionnalités accessibles par clavier, description des liens et boutons : par exemple « télécharger le formulaire d'inscription » au lieu de « cliquer ici ») ;
- Assurer la compatibilité du contenu avec les lecteurs d'écran ;
- Structurer et hiérarchiser le contenu (balise HTML appropriée pour les titres, les listes, etc.) ;
- Rendre les formulaires accessibles (identifier les formulaires via des labels, fournir des messages d'erreur clairs, adapter les aides contextuelles, etc.) ;

[143] Association départementale de parents et d'amis des personnes handicapées mentales, dont le site web est accessible via l'URL suivante : https://www.unapei.org

- Contraster les couleurs (entre texte et arrière-plan) et adapter la lisibilité (polices ajustables via le navigateur, compatibilité avec les systèmes de zoom des navigateurs, etc.) ;
- Tester les différentes solutions déployées avec les personnes concernées.

D'une manière générale, la transparence implique donc que le responsable du traitement adapte l'information en fonction des spécificités propres à chaque catégorie de personnes concernées dont il traite les données personnelles. Il doit ainsi s'assurer de rendre l'information accessible et de faciliter l'exercice des droits pour le plus grand nombre. Idéalement, le parcours du traitement d'une demande de droit (voir supra : Maîtriser le parcours du traitement des demandes de droits : vers une meilleure gestion des risques juridiques, financiers et règlementaires) devrait prévoir des ramifications différentes en fonction de la situation particulière de la personne concernée.

D'un autre côté, cela reviendrait à ajouter une couche d'intrication dans des processus déjà complexes. Un tel effort peut sembler déraisonnable, voire impossible, selon la réalité et les activités de l'organisation. Un nivellement par le haut peut donc constituer une solution adaptée. Le responsable du traitement pourrait ainsi concentrer ses efforts sur un parcours de traitement des demandes unique certes, mais offrant un niveau de transparence et de qualité suffisant pour chacune des particularités représentées parmi les personnes concernées. Il en va de même concernant l'information des personnes concernées. Il semble peu réaliste d'imaginer la coexistence d'une multitude de politiques de confidentialité, de mentions d'information (donc de formulaires), spécifiques. La tâche du DPO consiste alors à trouver, avec l'aide des opérationnels, un compromis garantissant un haut niveau d'information à toutes les personnes concernées.

### 2.5. Documenter l'approche retenue

Quelles que soient les solutions retenues, le responsable du traitement devrait documenter l'ensemble des études et réflexions ayant guidé son choix (que cela concerne l'information des personnes concernées ou la facilitation et le traitement des demandes d'exercice de droits) afin d'être en mesure de se conformer à son obligation d'accountability, conformément à l'article 5(2) du RGPD.

Par ailleurs, il est également nécessaire de conserver la preuve de l'information des personnes concernées, dont les modalités d'archivage pourront dépendre du format et de l'instrument déployé. Ainsi, il est de bon aloi de conserver chacune des versions de la politique de confidentialité, de la politique cookies, de consigner une trace de chacune des mentions d'information utilisées sur les formulaires de collecte de données, etc.

En conclusion, pour accroître la transparence, le responsable du traitement peut chercher à simplifier l'information, choisir des formats et supports qui la rendent facilement accessible, capter l'attention des personnes concernées, transmettre l'information d'une manière didactique, l'adapter en fonction des caractéristiques d'un public spécifique, des besoins et de l'expérience utilisateur, valider les moyens et canaux de communication avec les parties prenantes et documenter le processus mis en place.

De tels efforts peuvent donc s'inscrire dans une démarche de création de valeur pour l'organisation. En effet, une information transparente génère de la confiance et de l'adhésion parmi le public.

Mais au-delà de la confiance générée par la transparence, la gestion et le traitement des demandes de droits constituent également une opportunité pour le responsable de traitement de protéger et de développer son activité.

## B. Communiquer et innover autour du traitement des demandes de droits : levier de différenciation sur le marché

En plus de capitaliser sur la transparence et la confiance qu'elle permet de générer, le responsable du traitement peut mettre à profit ses pratiques en matière de protection des données personnelles et, plus spécifiquement en matière de gestion des demandes de droits pour se différencier sur le marché.

Ainsi, il peut non seulement mettre à profit le traitement des demandes de droits pour protéger et développer son activité (1), mais également y voir l'opportunité d'améliorer l'offre et la qualité des services qu'il propose (2).

### 1. Mettre à profit le traitement des demandes de droits pour protéger et développer son activité

Face à une prise de conscience accrue des enjeux liés à la protection des données personnelles, une bonne gestion des demandes de droits des personnes concernées représente pour le responsable du traitement l'occasion d'améliorer la perception des parties prenantes, de renforcer son positionnement sur un marché concurrentiel et de développer (ou de maintenir) des opportunités d'affaires (2). Pour cela il peut capitaliser sur la "confiance numérique" qu'il inspire (1), ou encore adopter une approche proactive et collaborative du traitement des demandes de droit (3). Le traitement optimal des demandes de droits devient alors un marqueur de la qualité et de la maturité organisationnelle de l'entreprise.

### 1.1. Confiance numérique : un pallier stratégique

*i) Notion de confiance numérique*

La confiance numérique est une notion aux dimensions multiples. Elle reflète la perception (positive) des clients, des utilisateurs, des partenaires et autres parties prenantes, quant à la capacité d'une organisation à évoluer dans un environnement numérique de manière sécurisée, pérenne et durable. Au cœur de ce concept, se retrouvent :

- **La sécurité des données et des systèmes** (protection contre les attaques cyber, les violations de données et autres risques numériques, en mettant en œuvre les mesures préventives et correctives adéquates) ;
- **La confidentialité et la protection de la vie privée** (conformité réglementaire, transparence sur l'usage des données, respect des droits des personnes concernées, etc…) ;
- **La résilience des infrastructure** (maintien des services en contexte de crise) ;
- **L'éthique numérique** (utilisation responsable des technologies et outils numériques : encadrement des algorithmes, lutte contre la désinformation, inclusion numérique, etc…).

C'est une notion qui se place au cœur des interactions entre les organisations et leurs publics. De plus, elle raisonne de plus en plus à mesure que le temps passe et que l'actualité numérique s'intensifie (violations massives de données, crises cyber, encadrement des grandes plateformes du commerce électronique et des réseaux sociaux, débats sur la souveraineté numérique européenne, etc.). La confiance numérique devient un enjeu stratégique pour les organisations à mesure que les citoyens et organisations prennent conscience des défis liés à leurs données personnelles et à leur sécurité. Cette montée en puissance de la confiance numérique s'explique également par le fait que les modèles économiques évoluent pour intégrer des critères éthiques, de différenciation et de fidélisation fondés sur la protection de la vie privée. Les organisations doivent être en mesure de démontrer une maturité numérique accrue pour répondre aux attentes des régulateurs et des consommateurs.

Ainsi, investir dans la gestion et le traitement des demandes de droits, c'est capitaliser dans la confiance numérique de l'organisation et donc dans sa pérennité et sa compétitivité. Placer la sécurité, la transparence et l'éthique au centre de la stratégie d'une organisation lui permet d'être mieux armée pour anticiper les crises, fidéliser ses publics et se différencier sur un marché où la méfiance envers les usages numériques reste forte.

*ii) Preuve de confiance*

Mais pour instaurer et développer cette confiance, il ne suffit pas d'affirmer ses engagements. Il est essentiel d'être capable de rassurer les parties prenantes sur la rigueur de son engagement. L'organisation doit ainsi pouvoir en apporter la preuve, par des actions concrètes, des certifications et des communications régulières, autant de gages de sa gouvernance, de sa maturité numérique et de ses bonnes pratiques. Cela peut se traduire par l'obtention de certifications et de labels attestant de la conformité et/ou de la solidité des pratiques en matière de sécurité (comme le label ISO 27001)[144] et de protection des données (tel que le label EuroPriSe).[145]

D'autre part, faire réaliser des audits réguliers par des cabinets tiers permet de valider la conformité aux réglementations et de démontrer une gouvernance rigoureuse. Ces audits, lorsqu'ils sont partagés avec des partenaires ou rendus publics, deviennent des outils de communication précieux pour asseoir la fiabilité et la transparence de l'organisation. De la même manière, le fait de collaborer avec des partenaires et fournisseurs partageant les mêmes exigences en matière de protection des données est également une preuve de confiance.

Par ailleurs, le fait de publier régulièrement des rapports sur la gestion des données personnelles ou intégrer cette thématique dans le rapport RSE de l'organisation, est un moyen efficace de démontrer un engagement constant. Ces rapports peuvent inclure :

- Des indicateurs de performance : délais de traitement des demandes de droits, taux de satisfaction des utilisateurs, etc. ;
- Les mesures clés pour renforcer la sécurité et la confidentialité ;
- Un plan d'amélioration continue, démontrant que l'entreprise ne se limite pas à la conformité minimale, mais cherche à aller plus loin.

Répondre rapidement et efficacement aux demandes des utilisateurs est une autre manière de démontrer cet engagement. Les délais respectés, la qualité des réponses apportées et la simplicité des démarches pour exercer ses droits sont autant d'éléments qui renforcent la perception d'une organisation responsable et la rapprochent du public.

[144] Voir le site web de l'Organisation Internationale de Normalisation concernant la norme ISO 27001:2022, accessible via l'URL suivante : https://www.iso.org/fr/standard/27001

[145] Voir le site web de l'European Privacy Seal, consultable via le l'URL suivante : https://euprivacyseal.com/en/

### 1.2. Renforcer la réputation et le positionnement concurrentiel

Dans un contexte où la sensibilité à la protection des données personnelles ne cesse de croître, la gestion rigoureuse des droits des personnes concernées constitue un levier puissant pour renforcer la réputation d'une organisation et se distinguer sur son marché. Ce positionnement s'opère à deux niveaux : auprès des clients et utilisateurs qui attendent de la transparence, de l'efficacité et de l'éthique ; auprès des partenaires, investisseurs et autres parties prenantes, pour sécuriser et développer des relations d'affaires durables.

*i) Sécuriser et développer les rations avec les clients et utilisateurs*

Les consommateurs accordent de plus en plus d'importance à la protection de la vie privée, à l'éthique et à la transparence. La méfiance envers les pratiques numériques est croissante, les utilisateurs sont plus enclins à choisir des entreprises qui démontrent un engagement clair en faveur de la protection de leurs données personnelles. La gouvernance et la gestion des demandes de droits jouent un rôle clé dans cette dynamique. En répondant rapidement et efficacement aux requêtes des utilisateurs (accès, rectification, effacement, etc…), l'organisation envoie un signal fort : elle respecte leurs droits et place la transparence au cœur de sa relation client. Cette approche améliore directement l'expérience utilisateur, renforçant la fidélité et l'engagement des clients / utilisateurs.

La conformité peut également servir d'outil de différenciation marketing. L'organisation peut mettre en avant ses efforts en matière de conformité et se positionner comme un acteur, (voire un leader) éthique. Elle peut ainsi se distinguer d'autres acteurs, concurrents, perçus comme opaques ou négligents. Cette approche est particulièrement pertinente dans les secteurs sensibles tels que la santé, la finance ou la technologie, où les données personnelles revêtent une importance cruciale pour les individus. L'organisation peut ainsi orienter sa communication et sa stratégie marketing autour de sa responsabilité et de son profil éthique. Ainsi, le responsable du traitement peut communiquer autour de ses pratiques en matière de gestion des demandes de droit et, de manière plus générale, de sa conformité. Il peut expliquer ses pratiques et sensibiliser le public à la valeur ajoutée de sa démarche. Une telle approche participe à la sensibilisation du public tout en démontrant que l'organisation, au-delà des exigences légales, protège les intérêts des personnes concernées.

*ii) Sécuriser et développer les relations avec les parties prenantes*

Une gestion rigoureuse des droits et de la conformité au RGPD constitue également un facteur essentiel de crédibilité vis-à-vis des parties prenantes, notamment les clients professionnels, partenaires et investisseurs. Ces derniers s'attendent à ce qu'une organisation

adopte des pratiques robustes pour réduire les risques juridiques, sécuritaires et réputationnels.

Premièrement, la conformité au RGPD peut être vue comme un levier pour attirer des investisseurs. Ceux-ci sont de plus en plus sensibles aux pratiques éthiques et responsables dans leurs décisions d'investissement, notamment dans le cadre des critères ESG (Environnementaux, Sociaux et de Gouvernance). Une organisation capable de démontrer sa maturité numérique et organisationnelle (via des audits, des certifications ou des rapports réguliers) rassure les investisseurs quant à sa capacité à gérer les risques, à maintenir une réputation solide et à inscrire son activité dans la durée.

Ensuite, dans le cadre des relations B2B, une organisation conforme au RGPD inspire confiance et facilite la conclusion de partenariats. Ainsi, l'intégration de clauses claires sur la protection des données dans les contrats (en particulier en ce qui concerne les rôles des parties dans la gestion des demandes de droits) permet d'harmoniser les pratiques avec les partenaires, facilitant ainsi des collaborations fluides et sécurisées. De plus, avec des prestataires fiables, l'organisation garantit une cohérence dans la chaîne de traitement, limitant ainsi les risques juridiques.

La réciproque est également vraie. Une gestion rigoureuse des données personnelles peut générer des opportunités commerciales, particulièrement dans les secteurs réglementés (comme la santé, la finance) où la conformité est une condition essentielle à l'établissement de partenariats stratégiques. Mais, plus généralement, c'est aussi le cas dans un nombre croissant de secteurs d'activité. En effet, les obligations en matière de responsabilité et de contractualisation s'attachent à l'ensemble de la chaîne de traitement. Les partenaires, organisations privées, organismes publics et autres clients professionnels sont incités à revoir leurs exigences à la hausse en matière de protection des données personnelles. Ainsi, par un effet « boule de neige », l'accession à de nouveaux marchés (ou le maintien des marchés existants) est de plus en plus conditionnée à des standards élevés en termes de protection de la vie privée. Ces exigences de conformité sont désormais intégrées dans les appels d'offre, cahiers des charges, marchés publics, certifications, etc. Or, la gestion et le traitement des demandes de droits sont un indicateur précieux de la maturité d'une organisation. En termes de protection des données.

### 1.3. Approche proactive et collaborative

Afin de s'assurer que les solutions choisies répondent aux exigences des personnes concernées et qu'elles satisfont leurs attentes en matière de traitement des demandes de droits, il est préférable de les consulter, voire de collaborer directement avec elles. Ainsi,

l'organisation ne se contente pas de déployer des solutions techniques ou juridiques : elle engage un dialogue actif avec les parties prenantes et place les attentes des utilisateurs et des collaborateurs au cœur de la gestion des droits.

Le responsable du traitement peut alors travailler avec des panels d'utilisateurs afin de cocréer des solutions transparentes et faciles d'accès pour un public non initié, de s'assurer de l'efficacité des processus déployés. Il peut également engager des dialogues institutionnels, avec notamment des autorités, des associations de défense des intérêts des consommateurs, des syndicats, des représentants du personnel, des groupes d'entreprises d'un même secteur d'activité.

*i) Dialoguer avec les parties prenantes institutionnelles et sectorielles*

Adopter une approche proactive et collaborative de la conformité au RGPD ne se limite pas à répondre à des obligations. Il s'agit d'impliquer activement les parties prenantes dans la construction et l'amélioration des dispositifs, tout en valorisant la transparence pour bâtir une relation de confiance durable. En cocréant des solutions adaptées, en dialoguant avec les institutions et en communiquant de manière proactive, l'organisation renforce sa crédibilité et se distingue comme un acteur éthique et exemplaire. Le responsable du traitement a donc intérêt à engager un dialogue avec d'autres parties prenantes, telles que les autorités de régulation, les associations ou les syndicats. Il pourra ainsi affiner ses pratiques, anticiper les évolutions réglementaires, mutualiser les efforts engagés dans la gestion des demandes de droits et, plus généralement, de la conformité.

Ainsi, des interactions régulières avec des autorités de contrôle, comme la CNIL, permettent à l'organisation de mieux comprendre les attentes des régulateurs et de s'assurer que ses pratiques sont conformes. Ce dialogue peut aussi permettre d'obtenir des recommandations ou des certifications, renforçant ainsi la crédibilité de l'organisation. D'autre part, le fait de collaborer avec des associations de défense des consommateurs ou des syndicats offre un double avantage : identifier des pistes d'amélioration spécifiques, renforcer la légitimité et l'adhésion des collaborateurs, des clients/utilisateurs, etc. aux processus déployés. Enfin, la participation à des initiatives intersectorielles - ou d'un même groupe, ou réseau - à la mutualisation des efforts, au partage des bonnes pratiques, peut s'avérer très intéressant pour le responsable du traitement. De telles interactions permettent non seulement de s'assurer de la conformité réglementaire mais également d'économiser des ressources. A titre d'exemple,

on peut mentionner l'initiative du « Data Portal » initiée par PERNOD RICARD, JC DECAUX et ACCOR.[146]

*ii) Cocréer des solutions adaptées avec les personnes concernées*

Pour garantir que les outils et processus mis en œuvre pour traiter les demandes de droits répondent véritablement aux attentes des personnes concernées, il peut être pertinent d'impliquer ces dernières directement dans la conception. Une telle démarche permettrait de concevoir des parcours clairs, accessibles et adaptés aux besoins réels. Ainsi, constituer et consulter des panels de test composés de clients ou d'utilisateurs finaux offrirait l'opportunité de valider l'efficacité et l'accessibilité des dispositifs mis en place. Par exemple, un formulaire en ligne destiné à exercer un droit d'accès ou d'effacement, pourrait être testé par les personnes concernées afin de vérifier sa clarté et sa facilité d'utilisation.

Par cette approche impliquant directement les personnes concernées, l'organisation montre qu'elle prend en considération leurs préoccupations, ce qui contribue à construire une relation de confiance durable. Une telle approche est complémentaire avec une dynamique innovatrice plaçant l'amélioration de la relation client et/ou de l'expérience utilisateur ainsi que le développement de nouveaux services, au centre de l'activité de l'organisation.

En plaçant la gestion des demandes de droits et, plus largement, la conformité au RGPD et la confiance numérique au cœur de sa stratégie, le responsable du traitement peut non seulement répondre aux attentes croissantes de ses clients, mais aussi se positionner comme un acteur de confiance auprès de ses partenaires et investisseurs. Les organisations adoptant une posture proactive et éthique, qui communiquent efficacement sur leurs efforts, se différencient davantage dans un marché concurrentiel. À la croisée de la fidélisation, de la crédibilité et de la sécurisation des relations d'affaires, la conformité au RGPD devient alors un véritable atout compétitif et stratégique.

## 2. Mettre à profit le traitement des demandes d'exercice de droits pour améliorer l'offre et la qualité des services

Parmi les opportunités de différenciation sur un marché compétitif, l'organisation peut mettre à profit la gestion et le traitement des demandes de droits (et plus largement la conformité au RGPD) afin d'élargir et/ou améliorer son offre de services. Notamment grâce à

[146] Voir article sur le site de l'Usine Digitale, A. VITARD, Pernod Ricard, JCDecaux, Accor unissent leurs forces autour d'un portail de données, 4 février 2025, disponible via l'URL suivante : https://www.usine-digitale.fr/editorial/pernod-ricard-jcdecaux-et-accor-unissent-leurs-forces-autour-d-un-portail-de-donnees.N2226933

une approche centrée sur l'utilisateur, le responsable du traitement peut tirer parti de la gestion des demandes de droits pour améliorer et personnaliser ses services (2.1), voire adopter une dynamique d'innovation, afin d'élargir son offre de services (2.2). Le responsable du traitement peut ainsi transformer la mise en conformité réglementaire en vecteur de création de valeur.

### 2.1. L'amélioration et la personnalisation des services autour de la gestion des droits au travers d'une approche centrée sur l'utilisateur

En s'appuyant sur une démarche d'amélioration continue, sur des outils de mesure (satisfaction clients/utilisateurs, engagement/fidélité, etc.), sur l'amélioration de la qualité des données client et sur des équipes pluridisciplinaires (qualité, marketing, commercial, développement, etc.), le responsable du traitement peut adopter une approche centrée sur les utilisateurs. Cela lui permettra d'améliorer ses services, voire de proposer de nouvelles fonctionnalités afin de répondre aux besoins de ces derniers (notamment en termes de personnalisation et de transparence). Une telle approche permettrait à l'organisation de mieux respecter les droits des personnes concernées, de créer une différenciation concurrentielle par la qualité de ses services pour finalement transformer la conformité réglementaire en opportunité.

Le responsable du traitement peut ainsi mobiliser les informations dont il dispose - notamment via le levier de l'intelligence business - pour déterminer et anticiper l'évolution des besoins des personnes concernées. Il peut mettre à profit ces éléments au travers d'une approche centrée sur l'utilisateur afin d'identifier des opportunités de correction, d'amélioration et de personnalisation de ses services.

*i) Intelligence business et approche « smart data » …*

L'intelligence business désigne les processus, outils et solutions visant à collecter, traiter et analyser des données pour accroître la capacité d'une organisation à prendre des décisions éclairées et stratégiques. D'une manière générale, il s'agit de transformer des données (brutes) en informations exploitables pour améliorer les processus internes, anticiper les tendances (et notamment l'évolution des besoins des utilisateurs/clients), optimiser les performances et processus opérationnels. La notion de « smart data » se concentre sur l'extraction de données pertinentes et leur analyse dans un cadre stratégique et/ou éthique. Contrairement au Big Data, visant à traiter d'importants volumes de données, il est ici question d'identifier et de cibler une quantité plus réduite de données, utiles, précises et exploitables (en garantissant le respect des droits des personnes concernées) ; l'idée étant de réduire le nombre de données superflues pour mieux se concentrer sur celles pouvant guider les orientations stratégiques de l'organisation et/ou l'innovation éthique et durable.

La gestion et l'analyse du traitement des demandes de droits par le responsable du traitement, notamment via des métriques (voir supra : Métriques et indicateurs) et dans le cadre d'une logique d'amélioration continue (voir supra : Amélioration continue) peut permettre d'identifier des opportunités stratégiques et/ou opérationnelles, mais également apporter une meilleure vision/anticipation des attentes des utilisateurs/clients. Une approche orientée « smart data » permet d'observer des tendances dans le comportement des personnes concernées : identifier des moments clés, analyser les raisons sous-jacentes à l'exercice de certains droits peut, par exemple, aider à ajuster la stratégie commerciale, affiner les campagnes marketing, adapter l'offre de services, etc.

En effet, l'intelligence économique (combinée à des mécanismes d'écoute anticipative, ou « veille ») permet d'identifier des « signaux faibles » (ANSOFF, 1975). Il s'agit d' « *informations précoces de faible intensité sur l'environnement d'une organisation, sur de nouveaux outils et solutions, ou sur des « insights consommateurs* »,[147] *annonciatrices d'une tendance, d'une menace ou d'une opportunité* ».[148] L'analyse des « signaux faibles » contribue à renforcer la capacité qu'ont les managers à anticiper les besoins futurs des personnes concernées, tout en maximisant le potentiel des équipes pour améliorer, personnaliser les services et stimuler l'innovation. De plus, les données issues des demandes et des interactions avec les personnes concernées (demandes récurrentes, feedbacks qualitatifs, frictions identifiées, etc.) peuvent fournir des indications précises sur leurs attentes et besoins. L'organisation peut alors utilement se livrer à une analyse quantitative et qualitative afin d'identifier et de cartographie les attentes et les besoins de ses utilisateurs/clients.

Le responsable du traitement peut encore mettre à profit les données d'analyse recueillies concernant les demandes de droits traitées pour mieux structurer ses données utilisateurs et identifier des segments spécifiques parmi ses utilisateurs/clients (voir supra : Segmentation des données et utilisation de métadonnées). L'organisation peut ainsi réagir en conséquence pour adapter ses process, certes, mais également pour orienter sa stratégie data et produit, ou encore améliorer les services qu'elle propose.

Par exemple, l'analyse des demandes de portabilité dans le secteur bancaire peut mettre en évidence que certains groupes d'âge ou régions sollicitent plus souvent ce service, indiquant

[147] La « consumer insight » ou la « perception du consommateur » peut se définir comme *la perception par le consommateur d'un problème ou d'un dilemme irrésolu sur la catégorie de produits où la marque opère ».* Définition de la notion d' « insight consommateur » disponible sur Wikipédia via l'URL suivante : https://fr.wikipedia.org/wiki/Insight_consommateur

[148] Article publié sur le site DigiMind : C. ASSELIN, Les signaux faibles : Définition, intérêt en marketing et conseils d'experts, 27 avril 2023, consultable via l'URL suivante **:** https://blog.digimind.com/fr/insight-driven-marketing/signaux-faibles-definition-interet-marketing-analyse-reseaux-sociaux#:~:text=SelonIgorAnsoff%2C

un besoin d'autonomie plus fort. De la même manière, des demandes d'accès récurrentes peuvent traduire des besoins utilisateurs non satisfaits, ouvrant sur des opportunités d'adaptation des services. Autre illustration : si, dans le cadre d'un service de mobilité, un certain nombre d'utilisateurs demande systématiquement des données liées à leur déplacement, le responsable du traitement pourra déployer un service de suivi des trajets. Enfin, si des utilisateurs sollicitent régulièrement des données relatives à leurs interactions, (telles que leurs listes de souhaits, historiques d'achats, etc.), cela peut démontrer un intérêt pour des outils de consultation, de suivi, ou de synthèse de l'information.

*ii) Pour une approche centrée sur les besoins des utilisateurs …*

En complément de l'utilisation d'outils d'intelligence business et d'une approche « smart data », l'organisation peut poursuivre une logique centrée sur les besoins des utilisateurs. En ce sens, il pourra tout d'abord orienter la conception de ses services sur les utilisateurs/clients (« Human-Centered Design »). Une telle approche vise à analyser leur comportement via des données pseudonymisées (voire anonymisées) afin d'identifier les problèmes ou opportunités méritant une amélioration ou une innovation. Dans l'idéal, la conception de ces (nouveaux) services devrait se faire en collaboration directe avec les personnes concernées et/ou utilisateurs finaux (tout du moins en les impliquant dans les tests et la validation des choix opérés).

De plus, une conception centrée sur l'humain s'accompagne d'une dimension comportementale et emphatique : il s'agit de comprendre les besoins, frustrations et attentes des parties prenantes, tout en prenant en compte différents leviers psychologiques. Par exemple, le responsable du traitement peut réfléchir à des parcours utilisateurs simples et intuitifs et prendre en compte des mécanismes comme l'aversion à la complexité ou la peur de l'inconnu. Ces parcours peuvent également renforcer le sentiment de contrôle chez les personnes concernées. Ainsi, des solutions favorisant la simplicité, l'accessibilité et la transparence des informations peuvent permettre de passer outre de tels mécanismes et accroître la capacité des personnes concernées à gérer leurs données de manière plus autonome.

Enfin, les demandes de droits représentent l'opportunité pour le responsable du traitement d'obtenir une meilleure visibilité sur les données que les utilisateurs jugent importantes ou sensibles et, par-là, de mieux comprendre leurs préoccupations et leurs attentes globales, au-delà de la seule protection de leurs données personnelles.

*iii) Afin d'accroître la qualité et la personnalisation des services*

Après avoir pris la mesure des besoins et attentes de ses utilisateurs/clients, le responsable du traitement a la capacité d'engager des actions visant à transformer les besoins des utilisateurs en services améliorés et/ou personnalisés. L'enjeu est ici double : d'une part, améliorer directement l'expérience utilisateur et se différencier par la qualité des services proposés ; d'autre part, améliorer et personnaliser les services proposés en intégrant les retours des personnes concernées.

Suivant cette logique, l'organisation peut donc chercher à simplifier les démarches pour les personnes concernées en leur proposant des interfaces intuitives et universellement accessibles (notamment pour les adapter à des publics « vulnérables »), ainsi que des parcours simplifiés. Des mécanismes intuitifs pour exercer ses droits (tels que des outils permettant de les exercer en quelques clics) peuvent améliorer l'expérience de la personne concernée et favoriser la confiance et l'engagement. Il en va de même en ce qui concerne l'accompagnement (chat, courriel, ligne téléphonique, etc.) pour répondre aux questions et informer sur l'avancement des demandes. Par ailleurs, il est nécessaire de pouvoir conserver en toutes circonstances une intervention humaine afin d'être en mesure de gérer les cas ou de répondre aux demandes complexes.

L'organisation peut également prévoir un parcours utilisateur guidé pour les personnes concernées. Un tel parcours peut, par exemple, comprendre un onboarding personnalisé sur la protection des données, des étapes progressives d'information de la personne concernée, des tests interactifs et réguliers du respect des droits, ainsi que la mesure de sa satisfaction. De plus, il est envisageable d'introduire au sein du parcours un système de récompense de la personne concernée (par exemple, un bon d'achat lorsqu'elle paramètre ses préférences en termes de protection des données personnelles) afin d'augmenter son adhésion et de chercher à la fidéliser davantage.

Par ailleurs, l'ergonomie et la convivialité des services améliorés ou personnalisés peuvent inspirer la refonte d'autres services / fonctionnalités. En ce sens, la gestion des demandes de droits peut bénéficier à d'autres secteurs opérationnels que celui de la simple conformité. Simplifier les démarches et optimiser les parcours utilisateurs dans le cadre des demandes de droits RGPD peut donc inspirer des améliorations similaires dans le cadre d'autres parcours, ne relevant pas de la conformité (tels que le support client, la gestion des réclamations, etc.).

Dans une même logique, le responsable du traitement peut faire le choix de mettre à la disposition de la personne concernée, un tableau de bord numérique (ou un portail self-

service) pour faciliter l'exercice des droits et, finalement, améliorer la qualité de son/ses service(s) en plus d'améliorer la gouvernance des données et la gestion et de traitement des demandes de droits (Voir : Automatisation : vers l'industrialisation du traitement des demandes de droits). En effet, ce tableau de bord numérique peut rassembler les éléments pertinents concernant les données personnelles (communication, exercice des droits, contact, gestion des préférences, consentement, accès aux données, etc.). Connecté au système d'information de l'organisation, il renverra alors un certain nombre d'informations et d'instructions relatives aux données de la personne concernée. Par ailleurs, un tel outil peut être personnalisé afin de permettre aux utilisateurs non seulement de consulter leurs données, mais aussi d'accéder à des analyses et/ou recommandations issues de ces informations, et notamment des :

- Analyses de consommation (historique des interactions, conseils personnalisés, etc.) ;
- Suggestions d'amélioration basées sur les préférences utilisateurs (optimiser des abonnements ou contrats, par exemple) ;
- Mesures d'empreinte numérique (visualisation des données partagées, services liés à leur suppression) ;
- Outils pour la gestion, en temps réel, des préférences relatives au partage de données avec des tiers.

En définitive, une démarche centrée sur les besoins et attentes des utilisateurs est un levier puissant pour transformer la gestion des demandes de droits (et plus largement la conformité au RGPD) en une ressource stratégique permettant d'anticiper, personnaliser et optimiser les services tout en ouvrant la voie à de nouvelles perspectives d'innovation. Une telle approche repose sur une écoute active, des méthodologies de conception - centrées sur l'humain - et une volonté affirmée de placer l'utilisateur au cœur des priorités stratégiques. De cette manière, l'organisation ne se contente pas de répondre aux exigences réglementaires mais s'inscrit également dans une démarche proactive et éthique, renforçant sa compétitivité et son positionnement sur le marché.

### 2.2. Créer une dynamique d'innovation au travers de la gestion des droits RGPD

Outre l'amélioration de l'expérience utilisateur et la personnalisation de ses services, l'organisation peut tirer parti de la gestion des demandes de droits des personnes concernées pour innover et développer de nouveaux services et fonctionnalités exploitant la transparence, la sécurité et la personnalisation des données. Cela, notamment, via des leviers tels que la Privacy by Design / by Default et la portabilité des données.

*i) Privacy by Design / by Default, leviers d'innovation*

Le Privacy by Design (protection des données intégrée dès la conception d'un service, d'un produit ou d'un processus) / Privacy by Default (protection des données mise en œuvre sans qu'aucune intervention de la personne concernée ne soit nécessaire) est une obligation imposée au responsable du traitement par le RGPD.[149] Ces notions s'inscrivent dans le cadre de la conformité, mais leur intégration peut également devenir une source d'innovation et d'amélioration des services.

Dans le cadre des demandes de droits, l'anticipation des besoins des personnes concernées en termes de confidentialité peut conduire le responsable du traitement à proposer des fonctionnalités automatisées afin de respecter les droits des personnes concernées (purges automatiques à l'expiration d'un certain délai, service d'anonymisation - en temps réel - par exemple).

Il peut également s'agir de limiter l'intérêt pour les personnes concernées à exercer leurs droits grâce à l'implémentation de fonctionnalités visant à simplifier le paramétrage de leurs préférences en matière de confidentialité ou à accroître la transparence et l'accessibilité des informations qui leur sont fournies (par exemple via la visualisation interactive, la traçabilité des choix, etc.). Ainsi, le responsable du traitement peut potentiellement réduire le nombre de demandes de droits (accès, opposition, effacement, notamment) en même temps que d'éventuelles frictions et insatisfactions de ses clients/utilisateurs.

Par ailleurs, l'organisation a la possibilité de capitaliser sur l'application des principes de Privacy by Design / by Default en les intégrants dans son argumentation commerciale. Il peut donc également s'agir d'un levier de communication et de différenciation sur le marché. Une telle argumentation pourrait par exemple s'orienter autour de la sécurité et du contrôle octroyés aux personnes concernées.

Une piste intéressante de prospective peut alors être abordée : celle de l'automatisation intelligente des préférences des personnes concernées. Il est facilement envisageable que des acteurs cherchent à déployer des algorithmes pour prédire les besoins de confidentialité des utilisateurs en fonction de leurs interactions précédentes. Une telle démarche pourrait s'inscrire dans la logique du principe de Privacy by Default : la personne concernée n'a rien à faire, ses paramètres de confidentialité sont appliqués selon son comportement habituel dans des situations similaires. Cependant, un certain nombre de questions peuvent alors se poser, dans la mesure où ses préférences sont plus déduites qu'exprimées. Une telle pratique ne

[149] Article 25 RGPD

représenterait-t-elle pas un risque de privation d'autonomie ? N'introduirait-elle pas un certain arbitraire dans la protection de ses données personnelles ? Quid des traitements envisagés mobilisant le consentement ?

*ii) Portabilité des données, opportunité de création de nouveaux services*

Dans ses efforts de positionnement en tant que leader d'un numérique éthique, concurrentiel et innovant, l'Union européenne a entamé un effort de régulation pour favoriser, notamment, la souveraineté numérique, la circulation contrôlée et sécurisée des données et l'émergence de champions européens innovants et disruptifs. L'initiative, portée par le RGPD, s'amplifie avec l'émergence de nouveaux règlements constituant le « Paquet numérique » (entre autres DGA, Data Act, IA Act, etc.). Ces initiatives législatives ouvrent la voie à une économie de la donnée fluide, dynamique mais également éthique. Elles visent à intensifier le partage, la collaboration et l'interopérabilité des données. A ce titre, la portabilité des données est un élément capital puisqu'elle incite les acteurs économiques à développer des outils et solutions interopérables ainsi que des services innovants pour capter et fidéliser les utilisateurs.

Initialement, la portabilité des données personnelles a été poussée par le RGPD, aussi bien en tant que droit reconnu aux personnes concernées qu'en tant qu'outil de structuration d'un secteur économique dynamique et interconnecté. Elle fait actuellement l'objet d'une discussion au sein des instances européennes pour un futur règlement dont l'ambition est de rendre la portabilité plus opérationnelle et universelle sur le territoire européen.

En effet, la portabilité permet non seulement de réduire les barrières d'entrée sur les marchés et de favoriser l'innovation (en permettant l'exploitation de données qui, autrement, resteraient cloisonnées), mais elle représente également des opportunités pour la création de nouveaux services et le développement d'écosystèmes numériques interopérables. Dans cette perspective, la standardisation des formats de données favorise leur transfert entre différents acteurs, pour une (ré)utilisation d'un service à un autre. D'un point de vue économique et concurrentiel, un tel partage (sécurisé) des données soutiendrait l'émergence d'une multitude d'acteurs tout en permettant l'essor de nouveaux modèles économique et l'enrichissement des services existants.

Par ailleurs, ces efforts normatifs pourraient également conduire à la création de plateformes de partage de données et à l'essor de services personnalisés, bénéficiant tant aux opérateurs économiques qu'aux consommateurs. Par exemple, dans le secteur de l'énergie, un utilisateur pourrait porter ses données de consommation pour accéder à des simulations ou des recommandations d'efficacité énergétique auprès de différents fournisseurs. De la même

manière, dans le domaine des transports, des données de mobilité partagées entre prestataires de transport, collectivités et usagers pourraient donner naissance à des applications offrant des solutions de transports multimodaux et des outils de suivi des émissions carbone.

Au-delà de la perception d'une menace pesant sur leurs avantages concurrentiels (en facilitant la migration des utilisateurs/clients et de leurs données vers des concurrents), les organisations peuvent envisager la portabilité comme une opportunité d'accéder à de nouveaux marchés, de déployer de nouveaux services attractifs et/ou de capter de nouveaux publics. Ainsi, de tels transferts de données peuvent aboutir à la création de services/fonctionnalités enrichi(e)s et interopérables. D'autre part, des données portées entre différents secteurs peuvent générer des opportunités de services sur des marchés intersectoriels.

En revanche, les organisations qui ne saisissent pas l'opportunité de transformer la gestion des données en levier d'innovation et de création de services nouveaux s'exposent au risque de manquer des opportunités, voire de laisser d'autres acteurs développer ces services innovants à leur place. Un tel constat pourrait, par exemple, être tiré d'une société agissant en tant que mandataire pour exercer des demandes de demandes de portabilité pour le compte de clients membres des programmes fidélité d'enseignes de la grande distribution. C'est par exemple le cas de la plateforme UNNIDATA, qui adresse à ses utilisateurs les promesses suivantes : « reprenez le contrôle de vos données personnelles » ; « surveillez les cagnottes de vos cartes fidélités [qui sont réinitialisées à chaque fin d'année] et ne perdez plus un seul euro ».[150] Face aux pratiques d'un tel acteur (et aux potentiels risques commerciaux qu'elles impliquent), il semble plausible de penser que les distributeurs eux-mêmes ont laissé une porte ouverte, permettant à cette plateforme de développer son activité. En effet, si les enseignes de la grande distribution avaient développé des services attractifs permettant à leurs clients de gérer eux-mêmes leurs cagnottes, les promesses d'une telle plateforme n'auraient probablement pas été aussi attractives et les clients n'auraient peut-être pas été tentés d'exercer leur droit à la portabilité par l'intermédiaire d'un organisme tiers.

En définitive, la portabilité des données peut donc pleinement rejoindre une vision d'avenir portée sur des services centrés sur la donnée. Elle peut à ce titre intégrer la stratégie d'innovation de l'organisation.

[150] Voir en ce sens le site web de la société Unnidata, consutable via l'URL suivante : https://www.unnidata.com

Pour le responsable du traitement, la gestion des demandes de droits ne doit donc pas être vue comme une simple contrainte réglementaire, mais bien comme un levier de transformation des services proposés. En s'appuyant sur des outils d'analyse, une démarche d'amélioration continue, il peut déployer des fonctionnalités de personnalisation avancées et des principes de gouvernance des données éthiques. Le responsable du traitement peut alors développer des services plus performants et respectueux des utilisateurs.

En plaçant la gestion des demandes de droits et, plus largement, la conformité au RGPD et la confiance numérique au cœur de sa stratégie, l'organisation peut non seulement répondre aux attentes croissantes de ses clients, mais aussi se positionner comme un acteur de confiance auprès de ses partenaires et investisseurs. Les organisations adoptant une posture proactive et éthique, tout en communicant efficacement sur leurs efforts, peuvent davantage se différencier dans un marché concurrentiel. À la croisée de la fidélisation, de la crédibilité et de la sécurisation des relations d'affaires, la conformité au RGPD devient alors un véritable atout compétitif et stratégique.

# CONCLUSION

Il apparaît clairement que la gestion et le traitement des demandes de droits incarnent bien plus qu'une obligation légale imposée par la réglementation applicable en matière de protection des données personnelle. Elles représentent également une opportunité stratégique permettant au responsable du traitement d'aller au-delà de la simple conformité pour créer de la valeur.

A ce titre, intégrer la gestion des droits dans une stratégie globale peut s'aligner pleinement avec des objectifs clés de l'organisation et l'optimisation opérationnelle. Cette démarche renforce la cohérence des actions menées à travers tous les services et contribue à faire du RGPD un levier pour consolider la compétitivité à long terme. En effet, au-delà de la gestion des risques juridiques, financiers et réglementaires, le responsable du traitement peut exploiter la gestion des demandes de droits – et plus largement la conformité au RGPD – pour initier (ou renforcer) sa transition numérique, améliorer sa gouvernance et ses capacités organisationnelles, sécuriser et développer ses activités, optimiser ses performances, etc. Ainsi, une logique de mise en conformité pertinente peut avoir des impacts positifs sur l'ensemble des équipes métiers et fonctions supports.

Du côté des personnels, un effort doit être mené par le responsable du traitement. En effet, dès lors qu'une personne est impliquée dans le traitement d'une demande de droit, elle doit savoir ce qu'elle doit dire (ou ne pas dire) et ce qu'elle doit faire. Il est donc essentiel d'investir dans la formation et la sensibilisation des collaborateurs, mais également de mettre en place des procédures claires et précises.

Pour ce qui concerne l'accroissement de ses capacités organisationnelles, l'organisation peut saisir l'occasion d'optimiser la circulation de l'information et des bonnes pratiques (entre services, entre filiales, etc.). Cela permet également de créer de l'efficacité, de générer des processus opérationnels bénéfiques pour l'ensemble des équipes et d'intégrer la conformité au RGPD dans tous les secteurs d'activité.

Lorsqu'elles s'inscrivent dans une dimension transversale, la gouvernance, la gestion des demandes de droits - et d'une façon plus générale, la mise en conformité - permettent non seulement d'améliorer les pratiques de l'organisation, mais également de moderniser et de fluidifier les interactions entre les différentes fonctions de l'organisation : marketing, communication, logistique, Ressources Humaines, finances, juridique, etc. Ces bénéfices se

traduisent, notamment, par une prise de décision plus éclairée, une efficacité accrue et une agilité renforcée dans un secteur du numérique en perpétuelle évolution.

Au travers d'une logique de transition numérique, de digitalisation - voire d'automatisation, ou même d'industrialisation - du traitement des demandes de droits, l'organisation peut utilement chercher à faciliter le déploiement et la gestion de sa mise en conformité. Toutefois, cela nécessite que les parcours de traitement des demandes de droits aient été bien planifiés en amont et ce, pour chacune des différentes étapes du traitement des demandes.

Le responsable du traitement doit également envisager des processus pertinents en fonction du contexte de son activité, ainsi que des moyens et des capacités dont il dispose. Afin d'anticiper les cas complexes, l'organisation doit aménager des marges d'adaptation et d'intervention. La digitalisation ne doit pas la conduire à se détacher des personnes concernées : il est essentiel de pouvoir maintenir un rapport humain afin de ne pas créer de frictions avec les personnes concernées. Le cas échéant, l'organisation devra être en mesure d'expliquer le contexte propre à leur situation et de leur faire comprendre qu'elle agit selon leurs intérêts. Il s'agit ici de trouver un équilibre entre une dynamique d'automatisation et le maintien d'interactions humaines.

Par ailleurs, les indicateurs (de mesure et d'analyse) constituent des outils majeurs dans le cadre de la valorisation de la conformité. D'un côté, le DPO peut s'en servir pour objectiver les mesures entreprises et démontrer le bien-fondé de la mise en conformité et la valeur qu'elle génère. D'un autre, les sphères managériales peuvent s'en servir pour prendre des décisions (stratégiques et/ou structurelles) éclairées, aussi bien dans des domaines opérationnels qu'organisationnels. En effet, la qualité des données demeure un élément crucial dans le cadre de l'intelligence business et de l'optimisation des opérations (notamment, mais sans s'y limiter, dans le domaine du marketing). De plus, l'organisation peut s'appuyer sur des métriques pour s'ancrer dans une démarche d'amélioration continue, renforçant par-là les efforts entrepris en termes de protection des données personnelles.

Mais au-delà de l'optimisation des pratiques et capacités du responsable du traitement, ses efforts en termes de conformité au RGPD ouvrent la voie à la sécurisation des affaires et au développement commercial, que ce soit par la confiance ou par la qualité des services. La capacité de l'organisation à intégrer ces dynamiques au sein d'une stratégie globale constitue un facteur clé de succès. En mobilisant les ressources adaptées à ses besoins et en plaçant les utilisateurs au cœur de ses démarches d'amélioration et d'innovation, l'organisation peut transformer la contrainte réglementaire en moteur d'innovation et de croissance durable.

En capitalisant sur la transparence et en conférant aux personnes concernées la maîtrise effective de leurs données personnelles, le responsable du traitement peut générer confiance, adhésion et fidélisation. Toutefois, une transparence réelle (et non fictive) requiert de sa part un véritable travail de fond concernant aussi bien le contenu de l'information que la manière dont elle est communiquée au(x) public(s). De tels efforts sont amplement justifiés par la perspective d'améliorer le positionnement du responsable du traitement sur le marché.

Par ailleurs, la gestion des demandes de droits – et plus généralement, la conformité au RGPD - constituent un levier concurrentiel pour l'organisation. Il s'agit pour elle d'un moyen de se différencier par l'éthique, la qualité et l'amélioration des services, notamment au travers d'une approche centrée sur les attentes clients/utilisateurs, sur l'écoute de leurs exigences et l'intelligence business. La différenciation peut également provenir de la création de services innovants autour de la protection des données personnelles, notamment par l'application du Privacy by Default / by Design ou par le biais de mécanismes tels que la portabilité des données.

Toutes ces dynamiques génèrent des synergies en interne tout comme elles encouragent les collaborations externes, avec des partenaires ou des acteurs tiers. Elles renforcent ainsi la capacité d'innovation des organisations et facilitant l'exploration de nouveaux marchés ou segments.

Enfin, la mise en conformité régule, de manière de plus en plus constante et dans un nombre croissant de secteurs d'activité, l'accès à de nouveaux marchés et la conservation des marchés acquis par le responsable du traitement. En effet, le RGPD oblige les organisations à s'assurer de la conformité de l'ensemble de la chaîne de traitement. Ainsi, les acteurs ayant d'ores et déjà avancé dans leur mise en conformité exigent de plus en plus que leurs prestataires et partenaires aient également évolué en ce sens. Dans le cas contraire, ils prendraient le risque de mettre en péril les efforts entrepris et de voir leur responsabilité engagée. Par un « effet boule de neige », la protection des données personnelles est donc de plus en plus intégrée au sein d'appels d'offre, de cahiers des charges, d'évaluations, etc.

**En définitive, l'instauration d'un climat de confiance - grâce à une gestion éthique et proactive des droits - devient un atout de différenciation sur le marché, favorisant l'adhésion et l'engagement des utilisateurs tout en créant de nouvelles opportunités d'affaires et en sécurisant celles en cours. La conformité au RGPD se révèle ainsi être un véritable levier de création de valeur, profitable à toute organisation, quelle que soit sa taille ou son secteur d'activité.**

**La protection des données personnelles, partie intégrante du dispositif « Cyber-score » ?**

La « confiance numérique » est bien plus qu'une notion abstraite : elle constitue un véritable levier stratégique pour les organisations. En investissant dans la sécurité, la transparence et une éthique numérique exemplaire, les organisations peuvent bâtir des relations solides avec l'ensemble des parties prenantes. Elles peuvent également se protéger des crises et s'affirmer comme des leaders responsables sur leur marché. La mise en avant de preuves tangibles de confiance renforce la crédibilité et la résilience des organisations, tout en participant à leur attractivité et à leur compétitivité. Un dispositif apparaît alors particulièrement intéressant : celui du « Cyber-score », basé sur une approche collective de la confiance numérique. Il s'agit d'une création législative relativement récente,[151] visant à créer un outil similaire au « Nutri-score » et permettant - via une échelle de notation (A+ à F) et un système de couleurs - de véhiculer une information lisible, claire et facilement compréhensible sur le niveau de sécurité que présentent certaines solutions numériques.

Le « Cyber-score » part d'un constat simple : les utilisateurs numériques (particuliers, collectivités, PME, etc.) manquent d'informations claires quant à la sécurité des services numériques qu'ils utilisent. Cela peut exposer leurs systèmes d'information à des failles exploitables par des acteurs malveillants. Ce dispositif a pour vocation d'aider les utilisateurs à réaliser des choix éclairés lorsqu'ils sont amenés à comparer les services de plateformes numériques (plateforme, solution logicielle ou applicative, messagerie, etc.). Ainsi, le « Cyber-score » obéit à un double objectif : sensibiliser et informer sur la sécurité des services numériques tout en incitant les opérateurs économiques à améliorer leurs pratiques.[152]

Il s'agit également d'un moyen efficace pour « *permettre aux managers de prendre leurs responsabilités* » en matière de sécurité des systèmes d'information,[153] dans des environnements parfois cloisonnés entre les différentes parties prenantes en matière de cybersécurité et de gouvernance (IT, juridique, responsables de la gouvernance, etc.).[154]

---

[151] Cyberscore : Loi n° 2022-309 du 3 mars 2022 pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, consultable via l'URL suivante : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275

[152] Sénat, Rapport législatif n° 503 (2021-2022) concernant la proposition de loi pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, déposé le 16 février 2022, consultable via l'URL suivante : https://www.senat.fr/rap/l21-503/l21-5032.html

[153] Citation de B. Fuzeau, Président du Clusif, dans un article de F. JEANNE, "Le cyber score des applications métiers vaut bien une thèse !", 2023, consultable via l'URL suivante : https://www.itforbusiness.fr/le-cyberscore-des-applications-metiers-vaut-bien-une-these-64624v

[154] E. PENELOUX, P. LEPINARD, C. GODE, "La perception du risque cyber en entreprise : conception d'un cyberscore professionnel à destination des dirigeants", 28ème conférence de l'AIM, Association

Cependant, un tel dispositif peut créer des barrières d'entrée sur le marché (notamment en raison des investissements nécessaires à la réalisation d'un audit, ou des coûts de déploiement de mesures de sécurité trop ambitieuses). Cela est particulièrement vrai pour des petites structures innovantes. Il faut donc veiller, en cherchant à répondre à un objectif de transparence, à ne pas venir créer des distorsions de la concurrence pénalisantes pour certains acteurs économiques

D'une manière plus concrète, le cadre législatif créée une nouvelle obligation : celle de se livrer à un audit de cyber sécurité réalisé par des prestataires agrées par l'ANSSI. Toutefois, il convient de noter que les éléments devant intégrer le « Cyber-score » n'ont pas encore été déterminés. En effet, le contenu précis de l'audit doit être précisé par la voie réglementaire (seuil d'activité, critères de l'audit, modalités de calcul du score, etc.). Mais, à ce jour, aucun texte n'est venu indiquer les modalités d'application du dispositif, bien qu'une consultation publique ait été menée. Les critères envisagés sont d'ordre technique (mesures de sécurité déployées), juridique (extraterritorialité de certaines dispositions de droit étranger), statistique (nombres de failles détectées, de condamnations par des autorités de contrôle, etc.), et géographique (hébergement des données). Selon le Cabinet ADVENS,[155] l'évaluation s'appuierait sur une grille d'audit regroupant les neuf thématiques suivantes :

- Organisation et gouvernance
- Protection des données (mesures de sécurité techniques)
- Connaissance et maîtrise du service numérique (via une cartographie des partenaires et sous-traitants continuant au service)
- Niveau d'externalisation (localisation des infrastructures d'hébergement)
- Niveau d'exposition sur Internet (identification et authentification des administrateurs techniques et fonctionnels du service)
- Dispositif de traitement des incidents de sécurité
- Audit du service numérique étudié
- Sensibilisation aux risques Cyber et lutte anti-fraude
- Développement sécurisé

Information et Management, 2023, p.4, consultable via l'URL suivante : https://hal.science/hal-04114882v1/file/AIM

[155] Voir la page dédiée au cyber score sur le site web du Cabinet ADVENTIS, consultable via l'URL suivante : https://media.advens.com/cyber-news/cyberscore-comprendre-definition/

Toutefois et au vu de l'importance croissante de la protection des données personnelles, il serait intéressant d'envisager la possibilité d'intégrer des critères tenant à la conformité au RGPD et à la gouvernance des données. Ainsi, le respect des droits des personnes concernées pourrait être évalué. Des métriques démontrant l'efficacité des processus déployés dans le cadre du traitement des demandes de droits pourraient alors être intégrés à l'audit « Cyber-score » (par exemple : taux de respect des délais légaux dans les réponses, taux de satisfaction des demandes, etc.).

D'une manière plus globale, d'autres critères pourraient être pris en compte, tenant par exemple aux modalités de collecte des données personnelles, à la gestion des consentements, à l'absence de pratiques trompeuses (« Dark patterns »), au niveau de transparence de l'information communiquée aux personnes concernées, à la maîtrise des relations contractuelles avec les partenaires et sous-traitants (européens ou non), à la maîtrise des risques en termes de sécurité des données personnelles (mesures techniques et organisationnelles), à la réalisation d'Analyses d'Impact sur la Protection des Données (AIPD), etc.

Une telle approche contribuerait d'autant plus à mettre en avant les efforts entrepris par le responsable du traitement en matière de protection des données personnelles et à les transformer en levier de différenciation et de création de valeur …

# LISTE DES REFERENCES

SITES WEB :

- www.legifrance.gouv.fr
- www.journals.openedition.org
- www.lemonde.fr
- www.eur-lex.europa.eu
- www.cnil.fr
- www.dictionnaire.lerobert.com
- www.edps.europa.eu
- www.jenesuispasunedata.fr
- www.respectemesdatas.fr
- www.mydatadoneright.eu
- www.blog.withjumbo.com
- www.saymine.com
- www.incogni.com
- www.privacybee.com
- www.joindeleteme.com
- www.hestialabs.org
- www.globalsecuritymag.fr
- www.linc.cnil.fr
- www.api.gouv.fr
- www.leblogdudirigeant.com
- www.euprivacyseal.com
- www.lawsofux.com

BIBLIOGRAPHIE :


- **RGPD :** *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*
- **Loi informatique et libertés :** *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée*
- **Code civil**
- **Code pénal**
- G29, Lignes directrices relatives aux droits des personnes concernées du 25 février 2014, consultables via le lien suivant : https://www.edps.europa.eu/sites/default/files/publication/14-02-25_gl_ds_rights_fr.pdf
- CEPD, Lignes directrices relatives à la prise de décision individuelle automatisée et au profilage (WP251) du 3 octobre 2017 (version révisée du 6 février 2018), consultables via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp251_profilage-fr.pdf

- CEPD, Lignes directrices relatives au droit à la portabilité des données (WP242) du 13 décembre 2016 (version révisée du 5 avril 2017), consultable via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp242rev01_fr.pdf

- CEPD, Lignes directrices relatives à la transparence (WP260) du 29 novembre 2017 (version révisée du 11 avril 2018), consultables via le lien suivant : https://www.cnil.fr/sites/cnil/files/atoms/files/wp260_guidelines-transparence-fr.pdf

- CEPD, Lignes directrices relatives au droit d'accès n°01/2022 du 28 mars 2023, disponibles via le lien suivant : https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-012022-data-subject-rights-right-access_fr

- Référentiel Général d'Amélioration de l'Accessibilité (RGAA)

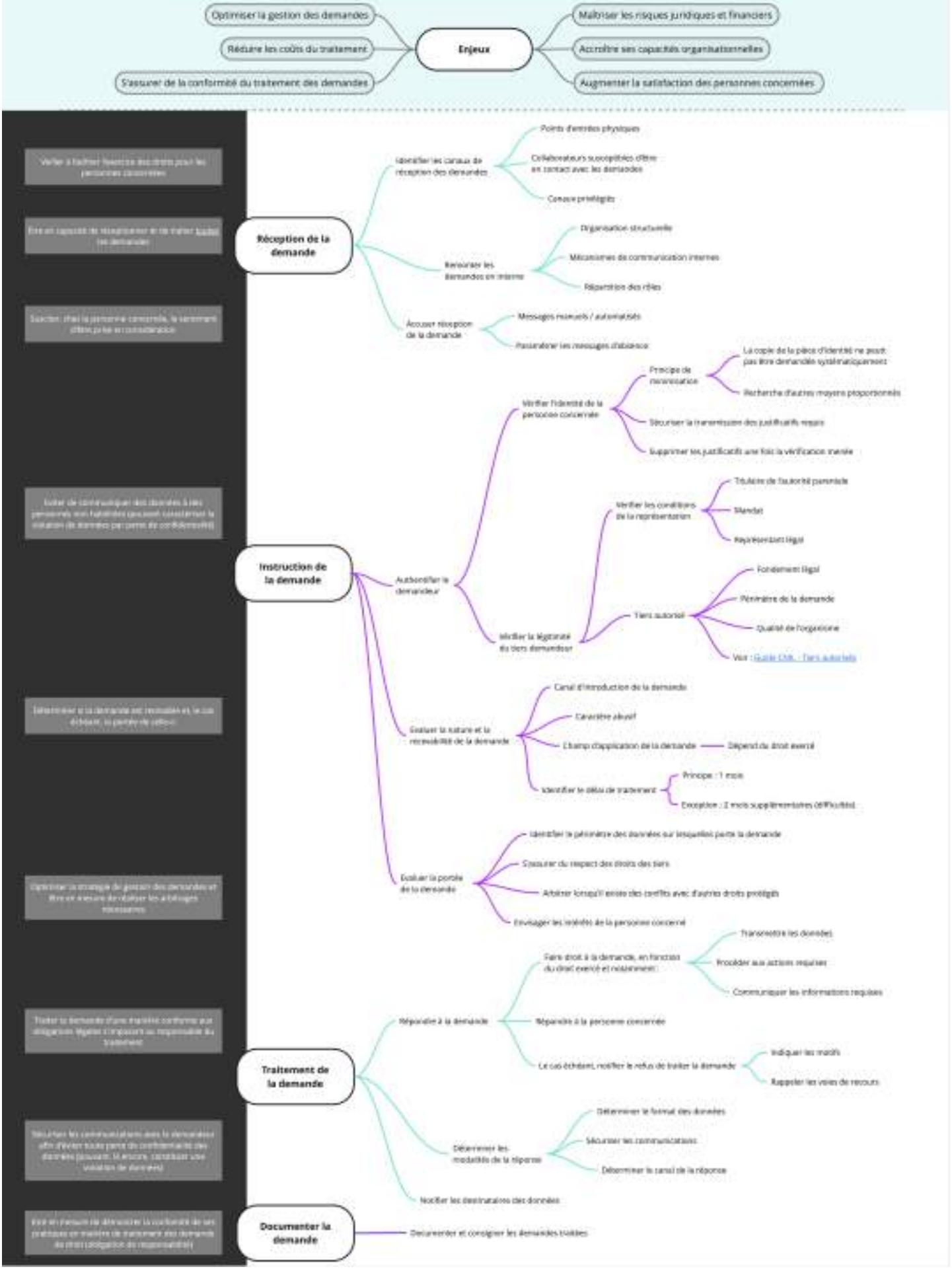
- Déclaration préliminaire des droits de l'homme numérique, présentée au Forum d'Avignon (édition 2014)

- The Oxford Guide to Plain English, Martin CUTTS, Oxford University Press, 2020

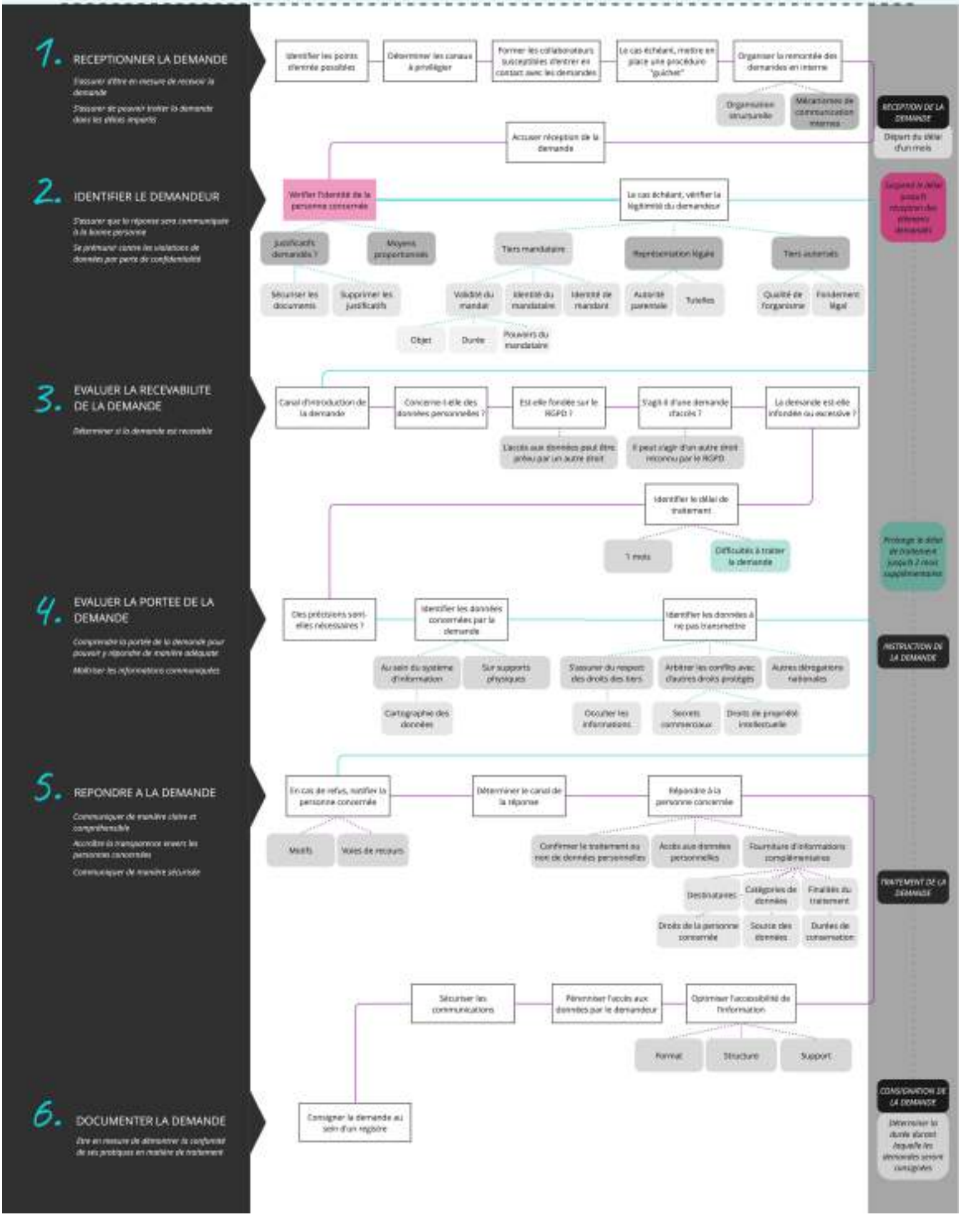
- Écrire pour Être Lu, ministère de la Communauté française de Belgique, 2009

- Rédiger clairement, Publication de l'Union européenne, 2011

# ANNEXE 1 - PARCOURS DU TRAITEMENT DES DEMANDES DE DROITS



# ANNEXE 2 - PARCOURS DU TRAITEMENT D'UNE DEMANDE D'ACCES



# ANNEXE 3 - PARCOURS DU TRAITEMENT D'UNE DEMANDE DE RECTIFICATION

## 1. RECEPTIONNER LA DEMANDE

*S'assurer d'être en mesure de recevoir la demande*

*S'assurer de pouvoir traiter la demande dans les délais impartis*

*S'assurer de la qualité des données*

Identifier les points d'entrée possibles

Déterminer les canaux à privilégier

Former les collaborateurs susceptibles d'entrer en contact avec les demandes

Le cas échéant, mettre en place une procédure "guichet"

Organiser la remontée des demandes en interne

Organisation structurelle

Mécanismes de communication internes

Accusé réception de la demande

**RECEPTION DE LA DEMANDE**

Départ du délai d'un mois

## 2. IDENTIFIER LE DEMANDEUR

*S'assurer que la demande est légitime et ne provient pas d'une personne non habilitée à demander la modification des données / souhaitant nuire à la personne concernée*

*Se prémunir contre les violations de données par perte d'intégrité*

Vérifier l'identité de la personne concernée

Le cas échéant, vérifier la légitimité du demandeur

Justificatifs demandés ?

Moyens proportionnés

Sécuriser les documents

Supprimer les justificatifs

Tiers mandataire

Validité du mandat

Identité du mandataire

Identité de mandant

Objet

Durée

Pouvoirs du mandataire

Représentation légale

Autorité parentale

Tutelles

Tiers autorisés

Qualité de l'organisme

Fondement légal

Suspend le délai jusqu'à réception des éléments demandés

## 3. EVALUER LA RECEVABILITE DE LA DEMANDE

*Déterminer si la demande est recevable*

Canal d'introduction de la demande

La demande est-elle infondée ou excessive ?

La rectification s'oppose-t-elle à une obligation légale ?

Identifier le délai de traitement

1 mois

Difficultés à traiter la demande

*Prolonge le délai de traitement jusqu'à 2 mois supplémentaires*

## 4. EVALUER LA PORTEE DE LA DEMANDE

*Comprendre la portée de la demande pour pouvoir y répondre de manière adéquate*

Sur quoi porte la demande ?

Données incomplètes

Données inexactes

Localiser les données concernées par la demande

Au sein du système d'information

Sur supports physiques

Cartographie des données

Vérifier l'exactitude des données concernées par la demande

Des justificatifs sont-ils nécessaires ?

**INSTRUCTION DE LA DEMANDE**

## 5. REPONDRE A LA DEMANDE

*Déterminer comment les modalités selon lesquelles les données peuvent être modifiées*

*Communiquer de manière sécurisée*

En cas de refus, notifier la personne concernée

Motifs

Voies de recours

Rectifier les données

Notifier la personne concernée

Sécuriser les communications

**TRAITEMENT DE LA DEMANDE**

## 6. NOTIFIER LES DESTINATAIRES DES DONNEES

*Répercuter la rectification des données sur l'ensemble de la chaîne de traitement*

Notifier ses destinataires

Identifier les destinataires des données

Partenaires

Prestataires

Entités du groupe

Organismes publics

Autorités

## 7. DOCUMENTER LA DEMANDE

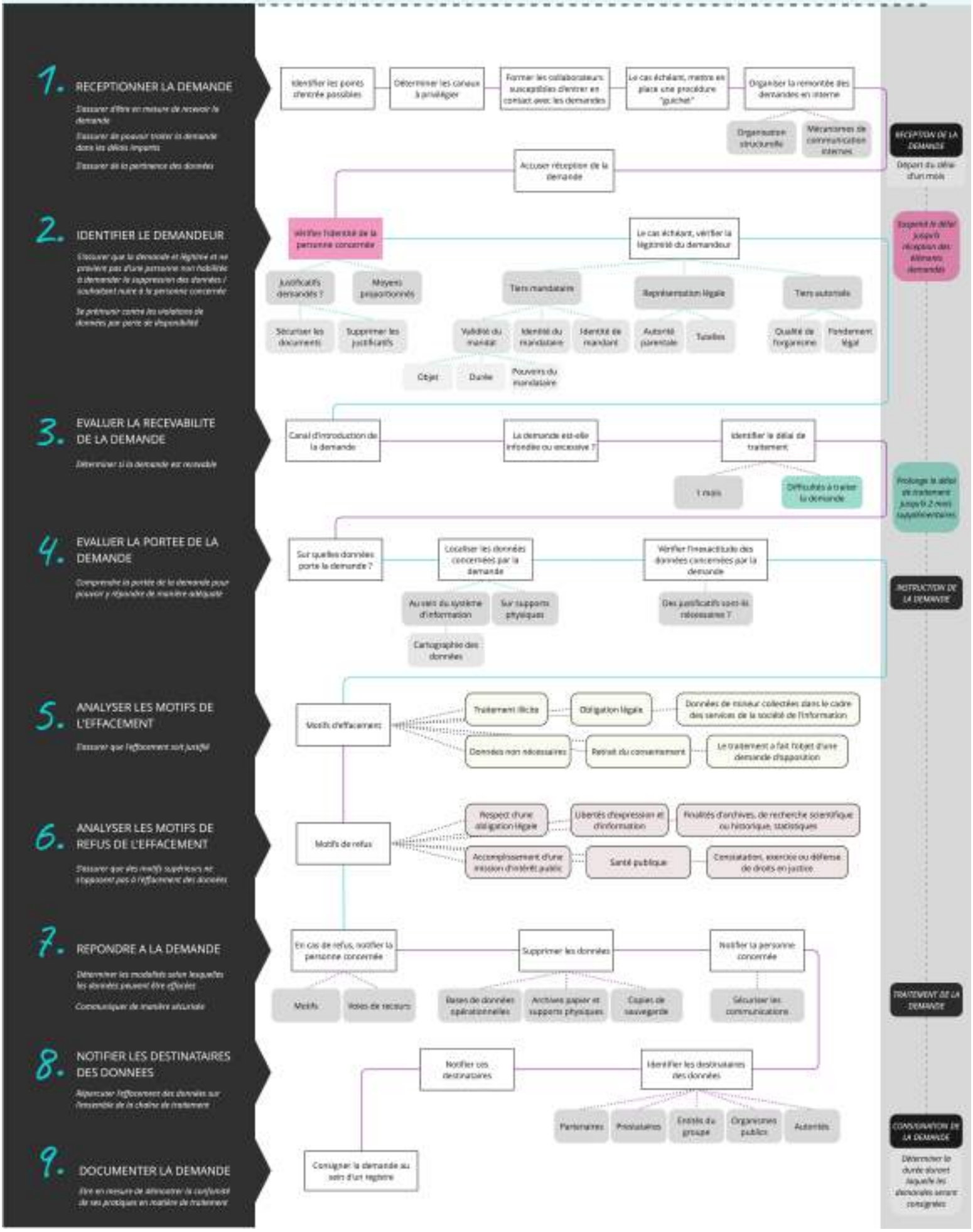
*Être en mesure de démontrer la conformité de ses pratiques en matière de traitement*

Consigner la demande au sein d'un registre

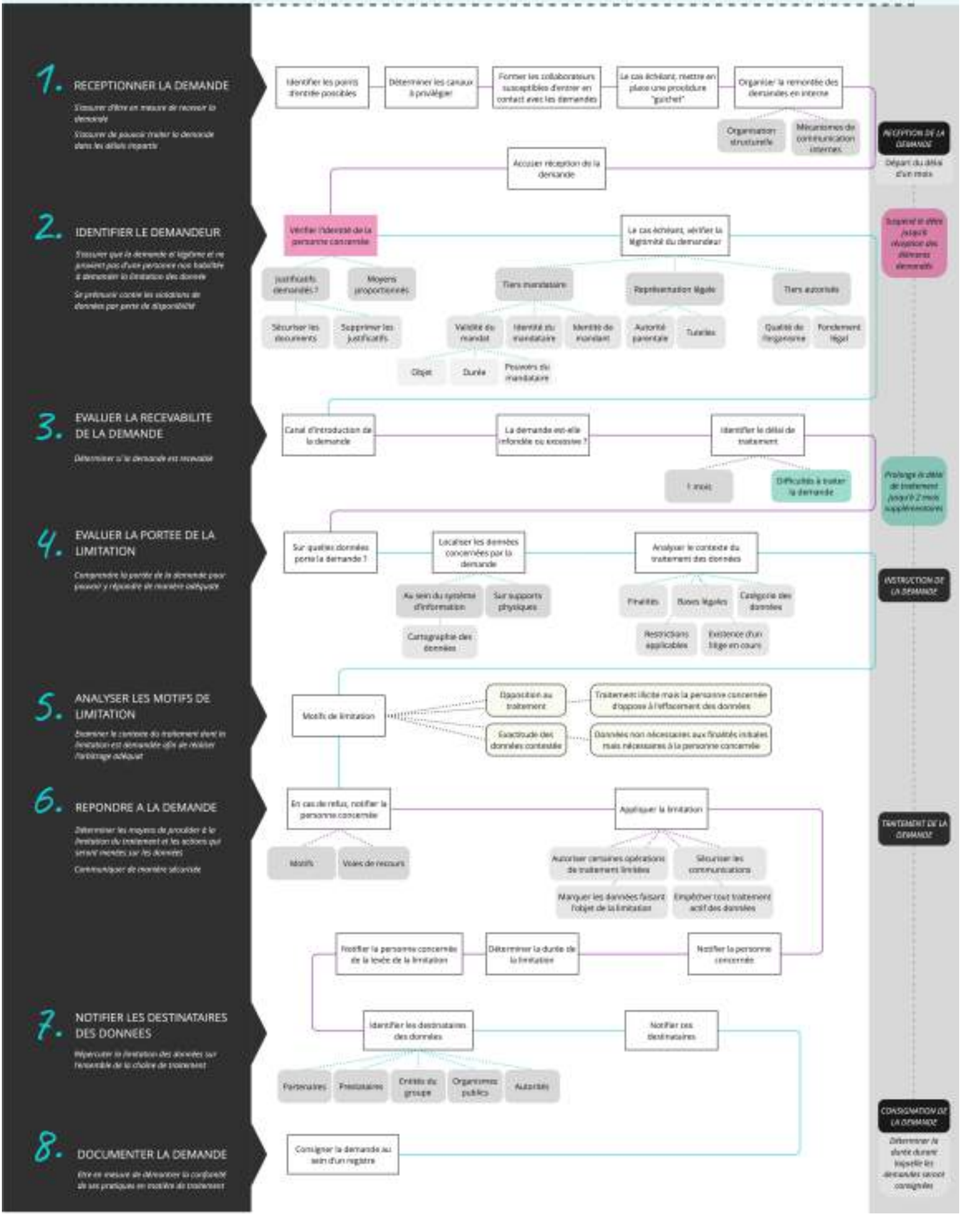
**CONSERVATION DE LA DEMANDE**

*Déterminer la durée durant laquelle les demandes seront consignées*

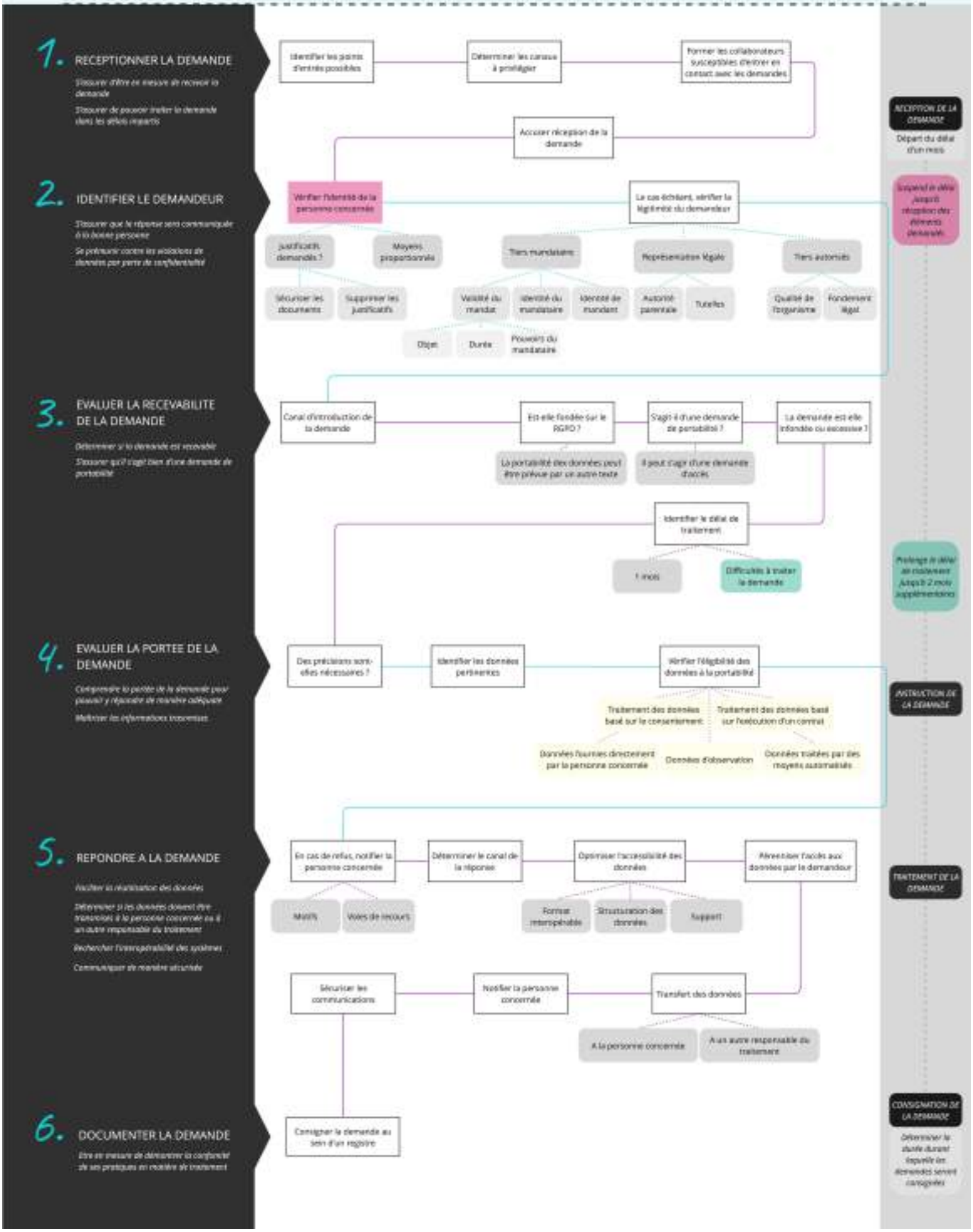
# ANNEXE 4 - PARCOURS DU TRAITEMENT D'UNE DEMANDE D'EFFACEMENT



# ANNEXE 5 - PARCOURS DU TRAITEMENT D'UNE DEMANDE DE LIMITATION



# ANNEXE 6 - PARCOURS DU TRAITEMENT D'UNE DEMANDE DE PORTABILITE



# ANNEXE 7 - PARCOURS DU TRAITEMENT D'UNE DEMANDE D'OPPOSITION