Chapitre 2
S'assurer de la licéité de vos traitements

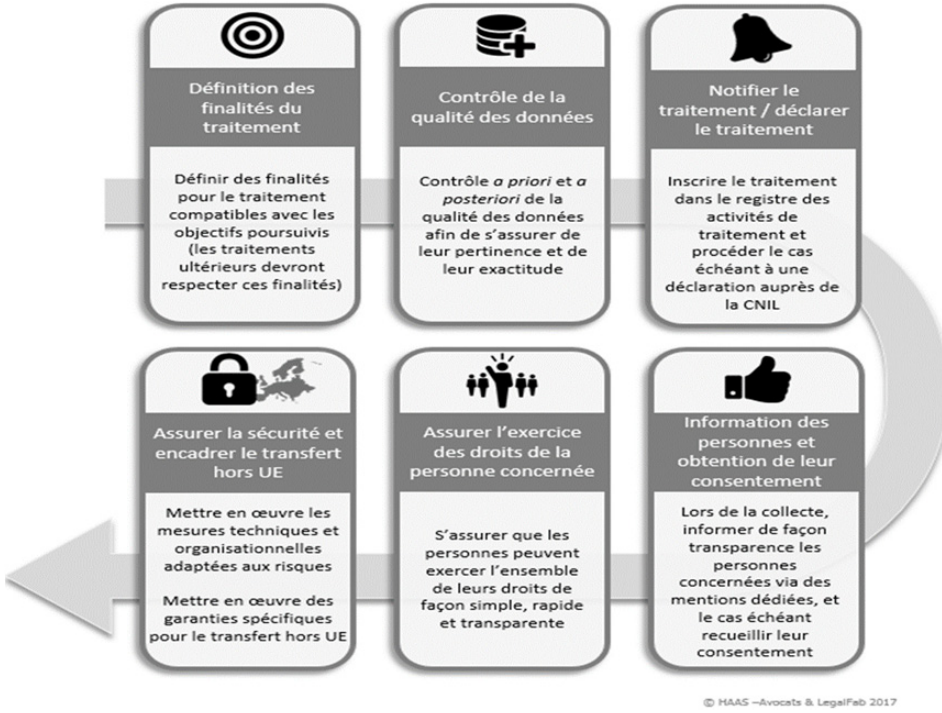
1. Introduction

La licéité constitue le grand principe des grands principes issus du RGPD. Les données personnelles doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée.

Alors que la loyauté et la transparence sont davantage des principes moraux, bien qu'ils aient, comme nous allons le voir, des répercussions importantes sur des notions pratiques, la licéité du traitement conditionne à elle seule le déclenchement de tout le processus juridique venant encadrer spécifiquement le traitement de données à caractère personnel.

Dans ces développements, nous vous proposons de suivre le cycle de licéité du traitement, de sa conception à sa réalisation. Imaginez-vous avoir identifié un besoin métier pour lequel vous devez procéder à un traitement de données à caractère personnel.

Nous allons voir ici étape par étape quelles sont les questions clés que vous devrez vous poser dans la mise en œuvre de ce traitement.



Cycle de licéité du traitement

2. Les étapes clés en amont du traitement

Un traitement de données à caractère personnel obéit à un certain nombre de principes directeurs définis par le RGPD.

Il faudra, dans un premier temps, penser le traitement en amont de sa mise en place. La première étape consiste à définir la finalité du traitement, c'est-à-dire la raison pour laquelle vous avez besoin de procéder à une collecte de données à caractère personnel.

Ensuite, vous devrez définir quelles seront les données collectées et ainsi pré-qualifier la qualité des données qui vous sont nécessaires.

Une fois les métriques du traitement définies, il vous faudra inscrire le traitement dans votre registre des activités de traitement.

2.1 Les finalités du traitement

L'analyse de la finalité des traitements repose sur le fait que chaque traitement de données à caractère personnel doit avoir une finalité déterminée, explicite et légitime (RGPD, art. 5, b). Autrement dit, le traitement de données doit répondre à un but ou à un besoin défini. On ne peut pas collecter les données d'autrui sans raison particulière.

Une fois que les données sont collectées pour une finalité, il n'est, par principe, plus possible de les utiliser pour la réalisation d'un traitement ayant une finalité différente. En clair, les données collectées ne peuvent être traitées ultérieurement de manière incompatible avec les finalités initiales, c'est-à-dire pour une finalité différente que celle pour laquelle le consentement initial a été donné. Il s'agit d'une règle essentielle dont le but est bien évidemment d'empêcher les détournements de consentement.

À titre d'exemple, la collecte de l'adresse électronique des adhérents pour la gestion de leur compte ne peut pas être détournée pour de la prospection politique.

Le règlement prévoit toutefois certaines exceptions : les traitements ultérieurs à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ne seront ainsi pas considérés comme incompatibles avec les finalités initiales.

Il existe donc quatre grands principes :

– la finalité doit être déterminée, légitime et explicite ;
– la finalité doit être respectée ;
– la finalité permet de déterminer la pertinence des données recueillies ;
– la finalité permet de fixer la durée de conservation des données.

2.2 La qualité des données (principes de minimisation, d'exactitude et de mise à jour)

La qualité des données à caractère personnel est mesurée par trois grands principes : la minimisation, l'exactitude et la mise à jour des données collectées. La direction marketing, la direction commerciale et les data scientists le savent bien : une base de données n'est économiquement exploitable que lorsqu'elle est régulièrement mise à jour. Dans ce cas, les données personnelles conservent leur valeur et peuvent même en gagner, créant ainsi un outil concurrentiel redoutable pour proposer les produits les plus adaptés aux besoins identifiés. Cette réalité économique de la qualité des données possède son pendant juridique dans le RGPD :

Les trois principes de la qualité des données personnelles

Le principe de « minimisation des données » (RGPD, art. 5) est un des nouveaux principes consacrés par le RGPD. Il fait écho au principe de « nécessité » que l'on retrouve dans la loi Informatique et Libertés (Loi n° 78-17, art. 6). Au nom de ce principe, les données collectées doivent êtres adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Ce principe conduit à éviter de collecter et traiter des données à caractère personnel à moins que l'objectif recherché rende cette collecte indispensable.

Concrètement, les responsables de traitement doivent veiller à limiter la quantité de données traitées dès le départ. Cette exigence de minimisation signifie que le responsable doit limiter les caractéristiques de son traitement uniquement à ce qui est indispensable à la poursuite des finalités de celui-ci (remarquons que ceci est vrai tant pour les données traitées que pour les personnes qui seront amenées à les traiter, c'est-à-dire les destinataires au sens de l'article 4.9 du RGPD.

Les bonnes pratiques autour de la minimisation

Le responsable du traitement doit :

- **Identifier les données strictement nécessaires à la finalité du traitement**. Écarter toute donnée superflue par rapport à la finalité du traitement.
- **Éviter toute collecte supplémentaire** en ne créant que des champs relatifs aux données déterminées et éviter d'insérer des zones de commentaires libres. Il convient de vérifier régulièrement qu'aucune donnée supplémentaire et non prévue initialement n'a été insérée.
- **Limiter l'envoi des documents électroniques contenant des données aux seules personnes habilitées** à les connaître. Il est recommandé d'effacer de manière sécurisée les données personnelles qui ne sont plus utiles ou qu'une personne demande de supprimer, sur le système en opération et sur les sauvegardes le cas échéant.

– **Utiliser un outil d'effacement sécurisé** pour les documents électroniques, un « dégausseur » pour les unités de stockage à technologie magnétique, etc.

  Outillage : logiciels d'effacement sécurisé certifiés par l'ANSSI.

En plus du respect du principe de minimisation, le responsable de traitement devra apprécier l'exactitude des données collectées (RGPD, art. 5). Bien entendu, il n'est pas envisageable de procéder à une enquête individuelle sur chacune des personnes concernées par le traitement, ce qui s'avérerait impossible en pratique (de telles obligations existent cependant dans le domaine bancaire avec le KYC ou dans le domaine des RH afin de pouvoir procéder à la paie de salariés).

Il conviendra de distinguer deux situations : lorsque la collecte est effectuée en interne et lorsqu'elle est effectuée par un tiers.

Dans le cas où la collecte est effectuée par l'entreprise elle-même, le principe de l'exactitude des données se traduit par la formation du personnel sur les modalités de la collecte.

Lorsque la collecte est effectuée par un tiers, les implications sont toutes autres. Cela peut recouper plusieurs situations, comme par exemple l'achat d'une base de données client ou encore la collecte de données via des sondages effectués par un sous-traitant. Dans ces cas d'espèce, le responsable de traitement devra s'assurer que les données collectées sont exactes et correspondent à la réalité. Cette mesure de l'exactitude se traduit contractuellement par des garanties spécifiques qui seront insérées dans le contrat passé entre l'entreprise et l'organisme tiers.

Maillon complémentaire du principe d'exactitude, la mise à jour des données revêt une praticité beaucoup plus concrète. Ce principe s'articule avec l'exercice des droits des personnes que nous détaillerons dans les développements suivants. Dès lors qu'une opportunité de mise à jour se présente au responsable de traitement, ce dernier devra la saisir. Le but est ici de lutter contre les données obsolètes dont l'usage qui en est fait peut apparaître non pertinent, voire même préjudiciable pour la personne concernée.

Chapitre 4
Mise en œuvre du système de management

1. Introduction

La méthode exposée dans ce chapitre permet de disposer au bout de quelques jours pour les petites entreprises et quelques semaines pour les plus grandes :

– d'un système de management opérationnel

– de preuves opposables en cas de sollicitations ou de poursuite

Le chef de projet devra faire preuve de tactique en combinant de manière optimale les modes opératoires et les moyens dont il dispose. Un tel projet vient nourrir la transition numérique de l'entreprise et fait bouger les lignes de l'organisation.

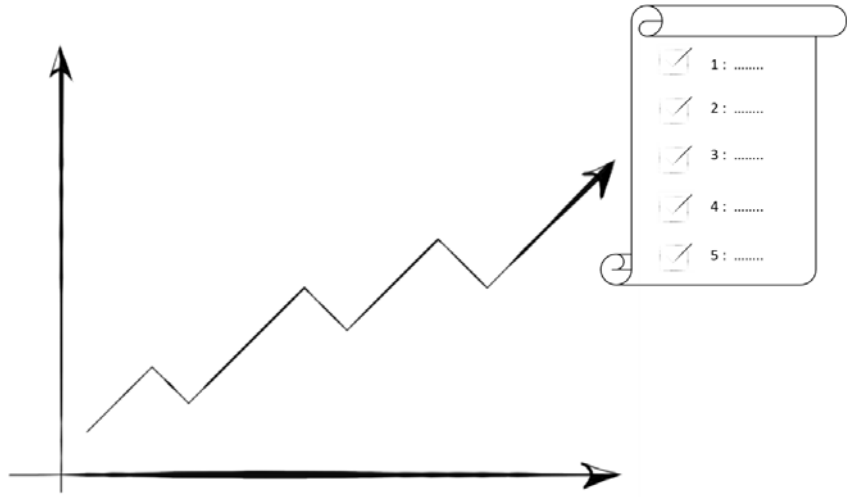
2. Choix de la méthode

Le chapitre Un système de management conclut qu'il faut mettre en œuvre un SMDCP composé de processus, d'outils, qui nécessitent des compétences (internes ou externes) ainsi qu'une structure de gouvernance pour atteindre le but. De plus, en présence de systèmes déjà existants, il doit en être tenu compte dans la phase de conception.

Dans 80 % des cas, c'est le service informatique qui initialise la réflexion auprès de la direction. Le responsable informatique ou la personne qui en prend l'initiative va profiter d'une réunion de direction pour expliquer les enjeux du RGPD et les obligations de l'entreprise.

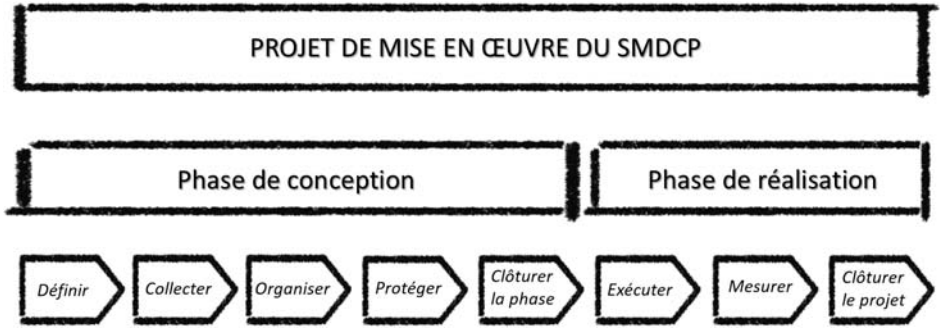
Quelle que soit l'écoute accordée, le projet RGPD est un projet pour lequel les directions ne souhaitent pas investir beaucoup de temps ni de ressources. La méthode de mise en œuvre s'appuie sur deux principes :

– Utiliser des cycles courts pour obtenir rapidement des résultats.
– Capitaliser sur des ressources déjà existantes pour limiter les coûts.



Peu de moyens et beaucoup de résultats

Inspirée du lean startup, la méthode pragmatique du build & run est celle que nous avons retenue. Elle comprend deux phases, conception et réalisation, que nous découpons en cinq étapes pour la conception et trois pour la réalisation.



Dès la phase de conception, des preuves opposables sont produites, la phase de réalisation vient les compléter et les enrichir. Au terme de cette seconde phase, le SMDCP passe en mode PDCA, nous parlerons alors du cycle de vie du SMDCP.

3. Phase de conception

La phase de conception comprend cinq étapes :

1. Initialiser le projet et définir le périmètre.
2. Collecter les activités de traitement.
3. Évaluer les éléments du système et projeter une organisation.
4. Apprécier le dispositif de sécurité, traiter les analyses d'impacts relatives à la protection des données et rédiger les politiques.
5. Valider le plan de progrès, enregistrer les documents à valeur de preuves et clôturer la phase.

Nous ne rappelons pas les bonnes pratiques de la gestion de projet, elles sont considérées comme connues.

3.1 Étape 1 : Définir

3.1.1 Objectifs

C'est le lancement du projet. Cette étape vise six objectifs :

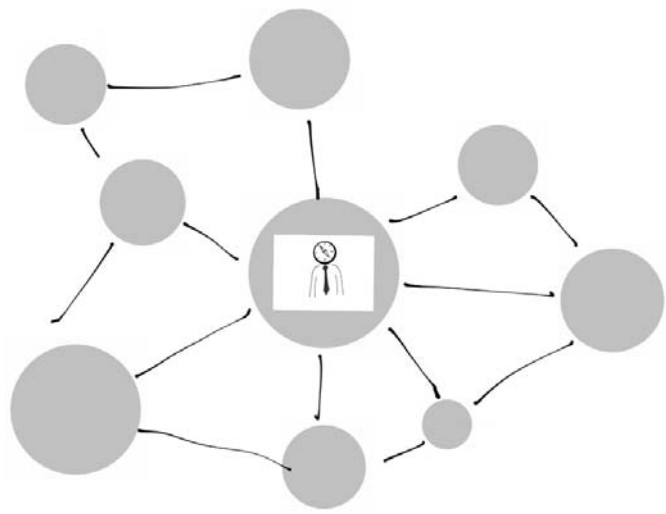
– Nommer le chef de projet
– Définir le périmètre du SMDCP
– Identifier les acteurs de la gouvernance
– Définir les critères du registre des activités de traitement
– Définir un support de sensibilisation
– Impliquer la direction

3.1.2 Activités

Nommer le chef de projet

Le chef de projet porte la responsabilité de conduire le projet jusqu'à l'étape Clôturer le projet. Sa compétence est décrite dans le chapitre Un système de management. Dans un cas sur deux, il s'agit du DPO ou du référent DPO pressenti.

Il est important qu'il dispose de relais internes dans l'entreprise. Il est nécessaire qu'il ait acquis des connaissances minimales sur le RGPD, au travers de lectures, de séminaires thématiques ou encore d'une formation. Dans tous les cas, il doit être averti sur ce qu'est une donnée à caractère personnel et une activité de traitement.



Il est vivement recommandé que le chef de projet dispose d'un réseau interne

Définir le périmètre

La note de cadrage doit reprendre l'objectif du projet, préciser le périmètre, rappeler les phases, les étapes et les livrables attendus, les ressources demandées et un premier de plan de communication qui sera mis à jour au fil du projet.

Il est fondamental que cette note de cadrage soit signée par la direction pour s'assurer de son support.

Remarque

La première source d'échec du projet est l'absence d'implication de la direction.

Identifier les acteurs de la gouvernance

Le chef de projet projette une première structure de gouvernance. En présence de systèmes déjà existants, il se rapproche de leurs responsables auprès desquels il affine cette structure. Sinon, la gouvernance va naturellement être composée comme suit :

– La direction générale en tant que représentant du responsable des activités de traitement.
– Le DPO ou le référent DPO.
– Le responsable du système d'information.
– Les directions fonctionnelles : ressources humaines, production, logistique, commerce, marketing, communication, etc.

Cette liste peut être complétée dans certaines entreprises par :

– Le responsable de la sécurité du système d'information.
– Le responsable de la qualité.
– Le responsable e-business ou open data.

Définir les critères du registre des activités de traitement

Pour préparer la collecte, le chef de projet définit les critères du registre. L'utilisation d'un tableur est recommandée, il facilite la collecte et permet de produire des indicateurs mesurables. À partir des critères retenus, le chef de projet conçoit un modèle de fiche sur la base duquel sont générées autant de fiches qu'il y a de traitements. Pour faciliter les séances de travail collectif qui suivront, cette fiche est à imprimer au format A4. La CNIL propose un modèle téléchargeable.

Voici une liste de critères qu'il nous semble pertinent de retenir au regard des exigences du RGPD, des modèles qui peuvent être proposés par les autorités et de nos retours d'expérience :

– L'intitulé de l'activité de traitement.
– Le nom et les coordonnées des différents rôles : responsable du traitement, responsable conjoint, représentant du responsable du traitement, délégué à la protection des données ou référent DPO.

– Le nom du gestionnaire de l'activité de traitement.

Remarque

Ne pas être capable d'identifier la personne qui gère les droits d'accès aux traitements est une source de vulnérabilité.

– Si le traitement est sous-traité :
  – Le nom du sous-traitant et son responsable.
  – Le nom du collaborateur qui gère ce contrat de sous-traitance.

Remarque

Le travail de mise à jour des contrats est souvent considérable. L'identification du gestionnaire des contrats durant la collecte est très utile pour construire le plan de progrès.

– La finalité du traitement.
– Les catégories de personnes concernées, de données à caractère personnel, et les destinataires.
– Le cas échéant, les transferts vers un pays tiers ou à une organisation internationale.
– Les délais prévus pour l'effacement.
– L'exercice des droits des personnes concernées.