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.

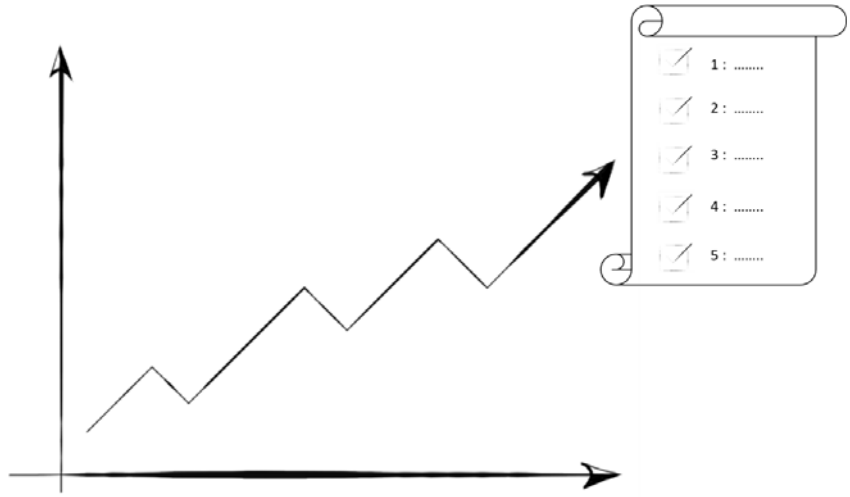
2. Choix de la méthode

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.

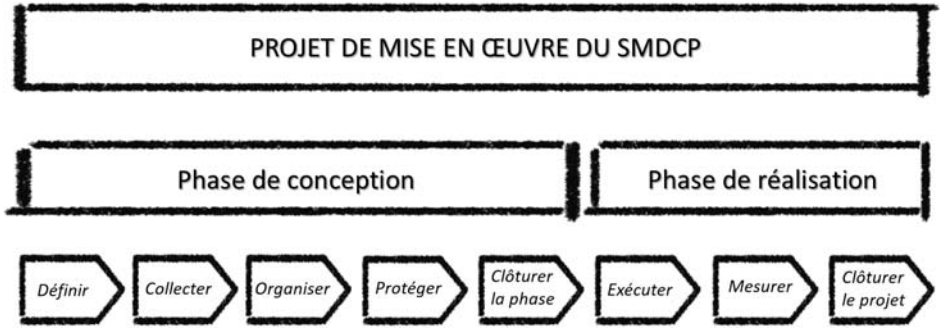
Quelle que soit l'écoute accordée, le projet RGPD est un projet pour lequel les directions ne souhaitent pas investir beaucoup de temps ni de ressources. La méthode de mise en œuvre s'appuie sur deux principes :

– 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 :

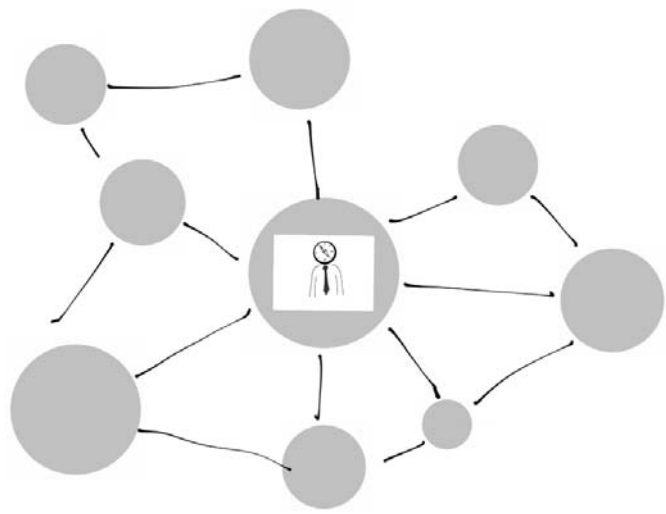
– Nommer le chef de projet
– Définir le périmètre du SMDCP
– Identifier les acteurs de la gouvernance
– Définir les critères du registre des activités de traitement
– Définir un support de sensibilisation
– Impliquer la direction

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.