Juridique et RGPD - Fiche de révision

1. La gestion de projet

1.1 Acteurs et vie d'un projet

Projet Interne (à l'intérieur d'une équipe) **Projet Transverse** (exemple : recrutement d'un nouveau collaborateur, implémentation ISO, etc ...) **Projet inter-entreprises**, dans le but de s'associer sur un un seul et même projet **Projet Externalisé** : Projet confié à un prestataire qui pilote/exécute le projet

Le chef de projet

C'est la personne en charge de la bonne conduite du projet, de l'atteinte du/des objectif(s).

L'équipe du projet

On distingue quatre catégories :

- "plate" : l'équipe est non hiérarchisée hormis le chef de projet qui possède l'autorité.
- "restreinte" : cette équipe est composée d'un nombre réduit de participants
- "multidisciplinaire" : combinaison de plusieurs profils techniques différents.
- "complémentaire" : équipe dont tous les membres sont complémentaires.

Les autres acteurs

- les acteurs qui payent, utilisent le projet
- Les parties prenantes

Définition de "parties prenantes":

Acteur, individuel ou collectif, activement ou passivement concerné par une décision ou un projet ; ses intérêts peuvent être affectés positivement ou négativement a la suite de son exécution.

La vie d'un projet

- Définition : objectifs, SWOT, fiche projet, template CR, to do list etc.
- Montage : cahier des charges, lots de travail, RACI, planning, budget etc.
- Exécution : suivi/pilotage, modification Cahier Des Charges (CDC), gestion des risques etc.
- Clôture: livraison, transfert, formation etc.

Matrice Swot : synthétise les forces et faiblesses d'une entrepris (Strength - Weakness - Opportunities - Threat)

1.2 Définition du projet

1.2.1 Objectifs : SMART

S.M.A.R.T est un acronyme désignant les attributs qu'un objectif doit posséder

- S pour “**Spécifique**” : précis et défini
- M pour "**Mesurable**” : exemple → réduire l'absentéisme de 15% au lieu de diminuer l'absentéisme.
- A pour "**Accepté**” : un objectif n'est pas imposé, il est proposé, discuté.
- R pour "**Réaliste**” : l'objectif ne doit être ni trop dur, ni trop facile, suffisamment accessible et ambitieux.

- T pour “**Temps**” : l'objectif doit être défini dans le temps, avec une date d' échéance par exemple.

1.2.2 Fiche de définition du projet

1. **Enjeux**: Besoins des clients et partenaires.
2. **Contexte**: Historique, projets précédents, contraintes.
3. **Livrables**: Produits, services, critères mesurables.
4. **Risques**: Principaux risques identifiés.
5. **Budget**: Ressources (temps, argent, expertise).
6. **Acteurs**: Équipe, chef de projet, client, hiérarchie, engagements.

1.3 Montage du projet

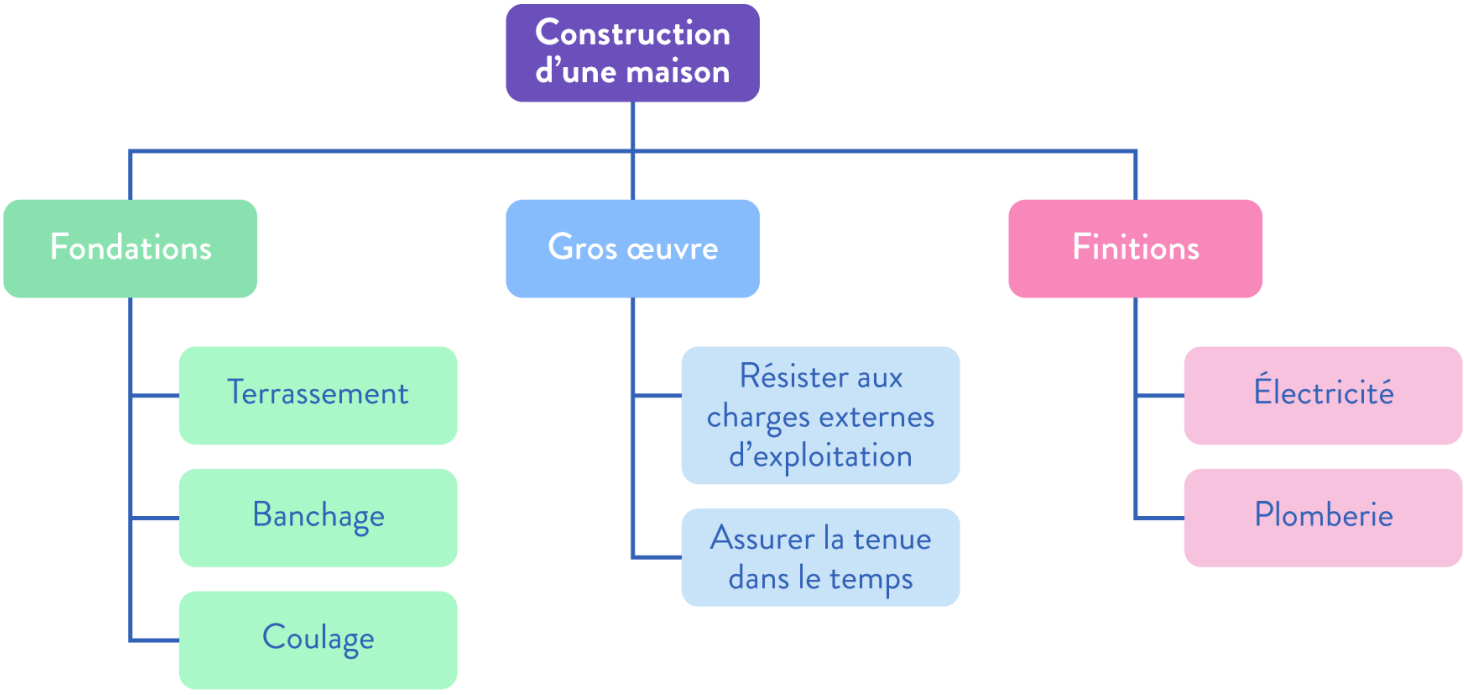
1.3.1 - Budget

Le budget du projet consiste en trois types de ressources : humaines, matérielles et financières. Il détermine la taille du projet.

1.3.2 - OBS et WBS

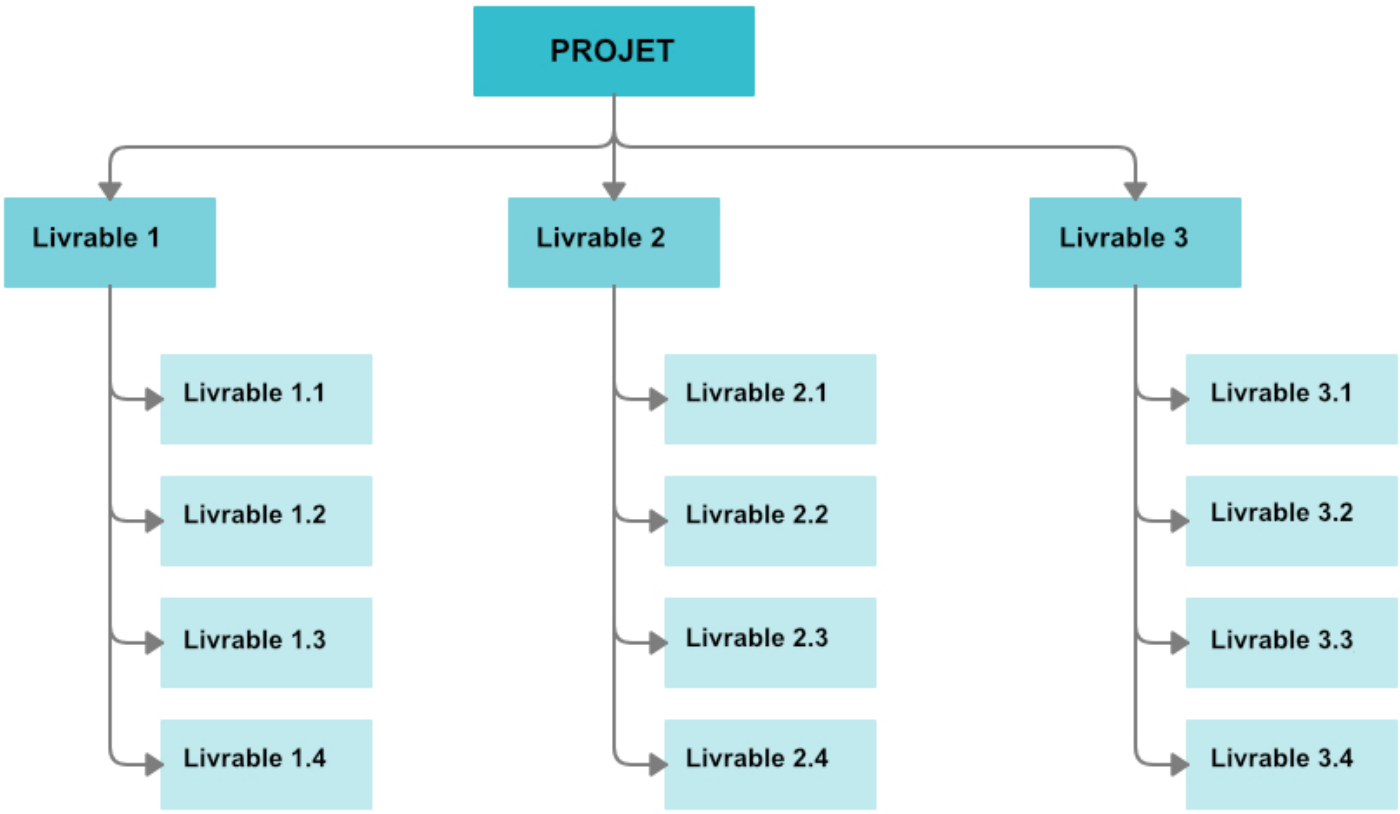
OBS (Organisation Breakdown Structure) :

Structure organisationnelle (du projet), OBS est un schéma qui représente les responsabilités de chaque membre pour chaque tache d'un projet.



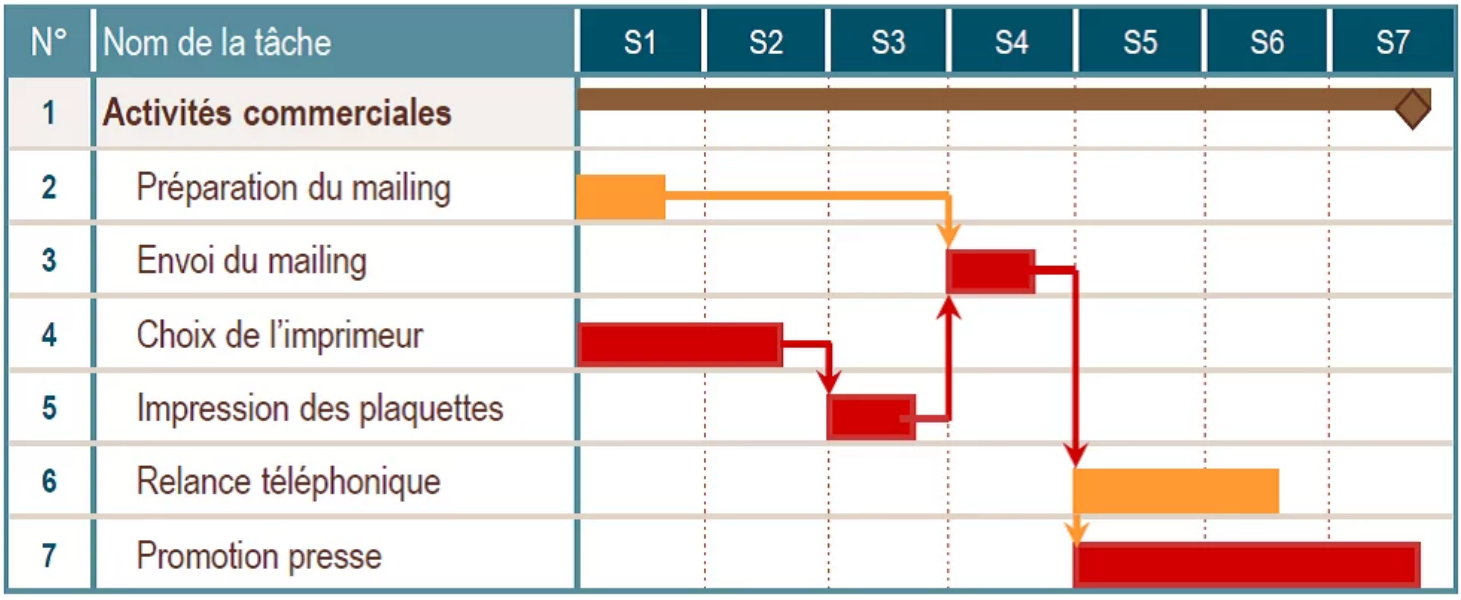
WBS (Work breakdown structure) :

-Organigramme des taches du projet (OTP), est une décomposition hiérarchique des travaux nécessaires pour réaliser les objectifs d'un projet.



1.3.3 - Planification du projet et diagramme de Gantt

Calendrier de réalisation d'un projet



1.3.4 - Roles et responsabilités

Matrice R.A.C.I R = Responsible → Celui qui fait A = Accountable → Celui qui valide C = Consulted I = Informed

R : Réalisateur
A : Approbateur
C : Consultant
I : Informé

ID	Livrable ou tâche	Sponsor	Changement	Informatique	Chef de Projet	Intégration	Coordination Finances	Coordination Ventes	Coordination Achats	Coordination Logistique	Coordination Production	Team Finances
		Equipe Management			Équipe Projet							
	INITIATION											
1	Etude d'opportunité	A	I	I	R	C	C	C	C	C	C	
2	Charte Projet	A	C	C	R	C	C	C	C	C	C	
	PLANIFICATION											
3	Cahier des Charges	A	C	C	R	C	C	C	C	C	C	C
4	Plan détaillé	A	C	C	R	C	C	C	C	C	C	I
	REALISATION											
5	Registre des risques et problèmes	A	C	C	R	C	C	C	C	C	C	C
6	Plan de Communication	A	R	C	C	C	C	C	C	C	C	I
7	Mise en place Finances	I	I	I	A	C	R	I	I	I	I	C
8	Mise en place Ventes	I	I	I	A	C	I	R	I	I	I	I
9	Mise en place Achats	I	I	I	A	C	I	I	R	I	I	I
10	Mise en place Production	I	I	I	A	C	I	I	I	R	I	I
11	Mise en place Logistique	I	I	I	A	C	I	I	I	I	R	I

1.4 Exécution du projet

1.4.1 - Indicateurs et état d'avancement

Jalons, réunions.

Etat d'avancement :

Suivi de projet : Prérequis (livrables et jalons), outils (cahier des charges, lots de travail, Gantt, budget) pour surveiller l'avancement et être proactif face aux difficultés.

1.4.2 - Analyse d'écarts

Méthode de suivi et d'analyse des écarts :

- Analyser les écarts prévus/réalisés et leurs causes.
- Identifier les causes possibles
- Re-planifier de manière réaliste si nécessaire
- Les objectifs non atteints sans analyse des causes peuvent entraîner l'échec du projet. Outils :
- Diagramme d'Ishikawa (5M) : classe les causes en 5 familles : Matière, Milieu, Méthodes, Matériel, Main d'œuvre.

1.5 Réunions et instances de pilotage

Réunion efficace : Deux rôles principaux

- animateur (gestion du temps)
- secrétaire (rédaction du compte rendu). Le Chef de Projet envoie le CR et décide des actions concrètes pour le PDCA. Types de réunions :
- Réunion technique : approfondir, résoudre des points précis.
- Réunion de chantier : présenter l'avancement et les résultats.
- Réunion d'avancement : suivre l'avancement, traiter les problèmes.
- Réunion "debout" (stand-up) : point rapide. Toutes les réunions doivent être suivies d'un compte rendu.

1.6 Comptes rendus

Un bon compte rendu est cohérent, détaille les objectifs avec les responsables, assure le suivi, est simple, partagé sur le même document, envoyé sous 48h et demande l'approbation par défaut.

1.7 Conseils en gestion de projet

Pour un bon projet : bon management, gestion des conflits, communication transparente, vision globale, anticipation des changements. ISO 21500 fournit un cadre de référence.

2. Gestion des risques au sein d'un projet

2.1. Identification des risques

- Humains : compétences indisponibles, démission, risques politiques, facteurs humains
- Économiques : marché, budget sous-estimé, recettes tardives, satisfaction des financeurs
- Temporels : facteurs exogènes, achats/sous-traitance, délais, mise au point
- Autres : évolutions techniques, sécurité, environnement, juridique.

2.2. Priorisation des risques

Risques prioritaires

Il est impossible de traiter la totalité des risques d'un projet, il faut donc les prioriser. Risque = Gravité x Vraisemblance

Loi de Pareto

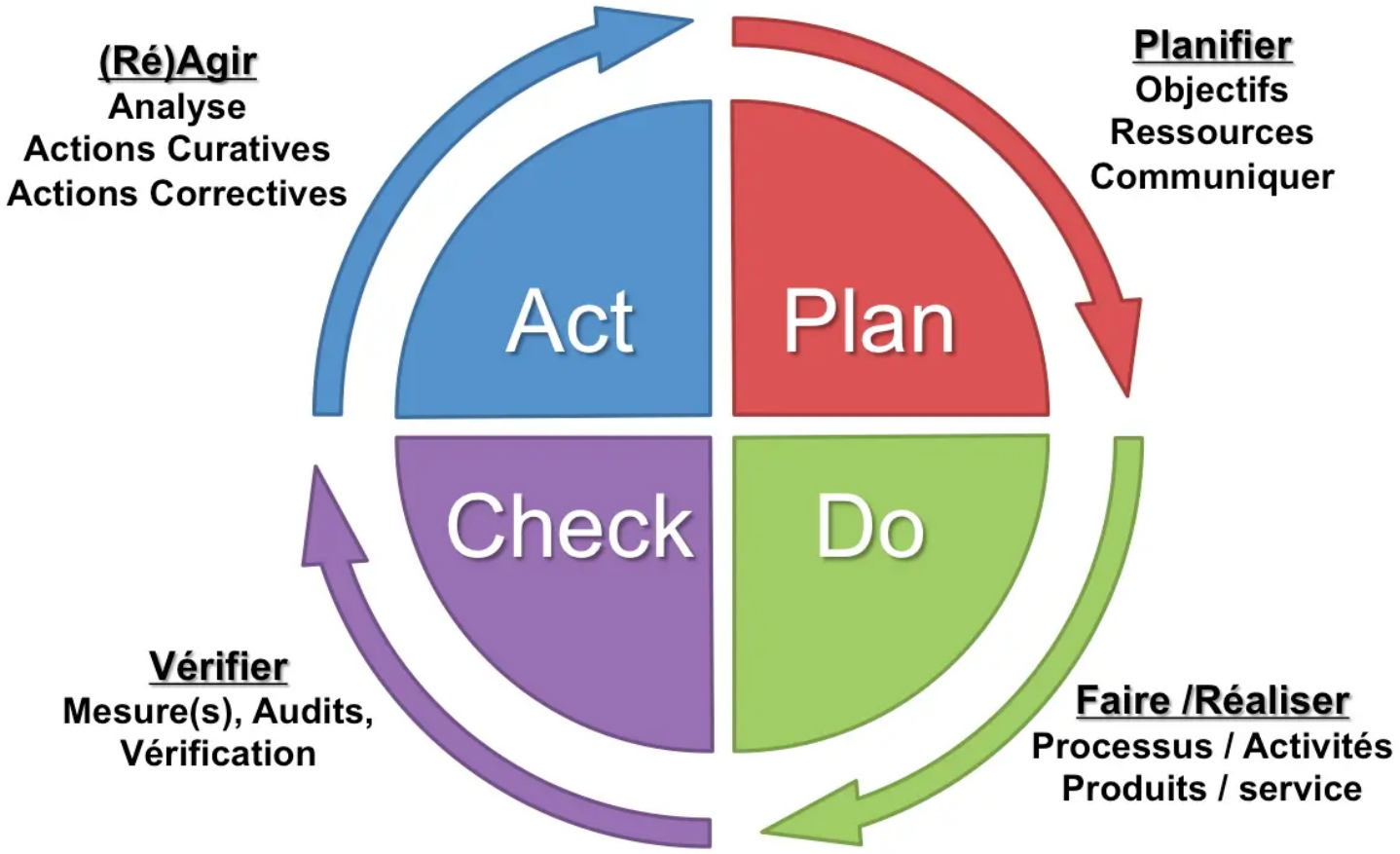
La loi de Pareto suggère que 80% des résultats proviennent de 20% des causes, ce qui permet de prioriser les actions sur les risques les plus importants.

2.3. Réflexion et traitements des risques

Pour traiter les risques, on peut utiliser différentes mesures techniques, juridiques, organisationnelles, financières ou de transfert de risque (assurance). La proactivité est essentielle, et un bon plan d'action doit inclure les acteurs, l'évaluation du risque, les responsables, et le type d'action à entreprendre.

2.4. Suivi des risques

Amélioration continue : PDCA!



Gestion des problèmes

Loi de Brooks: Ajouter des participants à une tâche en retard la retarde encore plus. Privilégier des experts pour les tâches importantes et des débutants pour les tâches moins critiques.

Lois du temps

- **Loi de Murphy**: Tout ce qui peut mal tourner va mal tourner
- **Loi de Ilich**: Au-delà d'un certain seuil, l'efficacité humaine décroit, voire devient négative
- **Loi de Carlson**: Un travail réalisé en continu prend moins de temps et d'énergie que lorsqu'il est réalisé en plusieurs fois

3. Réglementation RGPD

3.1. RGPD : définitions et historique

Règlement Général sur la Protection des Données

L'acronyme RGPD signifie « Règlement Général sur la Protection des Données » Il harmonise les règles en Europe en offrant un cadre juridique unique aux professionnels.

Donnée à caractère personnel

Les données à caractère personnel identifient une personne, soit directement, soit en les associant à d'autres informations. Pour être anonymisées, elles ne doivent plus permettre l'identification. Les traitements doivent respecter

les réglementations en vigueur.

Données sensibles

Les données sensibles sont des informations sur l'origine raciale, les opinions politiques, les convictions religieuses, etc. Leur utilisation est généralement interdite, sauf sous certaines conditions spécifiques

Personne identifiee ou identifiable

L'identification d'une personne peut être réalisée à partir d'une seule ou de plusieurs données

Traitement de données personnelles

Le traitement de données personnelles doit avoir une finalité définie.

Historique du RGPD

En 1973, le projet SAFARI visait à centraliser les informations des citoyens français En 1978, la loi française "Informatique et Libertés" est promulguée Le 25 mai 2018, le Règlement Général sur la Protection des Données (RGPD) entre en vigueur dans l'ensemble de l'Union Européenne

3.2. Nouvelles obligations

Les nouvelles obligations liées au Règlement Général sur la Protection des Données (RGPD) comprennent l'engagement d'un délégué à la protection des données (DPO), le respect des droits des personnes, l'identification et l'information des personnes sur les traitements de données personnelles, ainsi que la prévention et la notification à la CNIL en cas de violation de la vie privée ou de perte de données présentant un risque élevé. Les sanctions en cas de non-conformité doivent également être prises en compte.

3.3. Organismes concernés

Le RGPD s'applique à toutes les organisations qui traitent des données personnelles pour leur propre compte ou pour le compte d'autres organismes, dès lors qu'elles sont établies dans l'Union Européenne ou ciblent directement des résidents européens.

3.4. Acteurs et intervenants

Aperçu des différents acteurs et intervenants

- Personne protégée: Personne physique dont les libertés et droits fondamentaux sont protégés par le RGPD.
- Responsable de traitement: Entité qui détermine les finalités et moyens du traitement des données.
- Sous-traitant: Entité qui traite les données pour le compte du responsable de traitement.
- Destinataire: Entité qui reçoit la communication des données, qu'il s'agisse d'un tiers ou non.
- Tiers: Personne physique ou morale, qui n'est pas autorisée à traiter les données.
- Autorité de contrôle: Autorité publique indépendante chargée de superviser le traitement des données personnelles (ex: CNIL en France).

3.5. Etapes clés d'une mise en conformité

1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

Désigner un pilote

Le délégué à la protection des données (DPO) est obligatoire pour les organismes publics et certaines entreprises réalisant un suivi régulier et systématique des personnes à grande échelle ou traitant des données sensibles. Le DPO doit :

- **s'informer** sur le contenu des nouvelles obligations
- **sensibiliser** les décideurs sur l'impact de ces nouvelles règles
- **réaliser** l'inventaire des traitements de données de votre organisme
- **concevoir** des actions de sensibilisation
- **piloter** la conformité en continu

Cartographier les traitements de données personnelles

Le Registre des traitements est une documentation interne essentielle pour les organismes se conformant au RGPD. Il recense les différents traitements de données personnelles, leurs objectifs, les acteurs impliqués, et les mesures de sécurité mises en place. Cette mesure permet de mesurer l'impact du RGPD sur l'activité et de répondre aux exigences légales.

Les étapes clés pour la mise en conformité au RGPD sont les suivantes :

1. Lister les applications et bases de données contenant des données personnelles, ainsi que les mesures de sécurité associées.
2. Identifier les processus internes impliquant un traitement de données personnelles en interviewant les responsables métier.
3. Compléter le registre des traitements en fournissant les informations requises par l'article 30 du RGPD, telles que la finalité du traitement, les catégories de personnes concernées, les destinataires et les mesures de sécurité mises en place.

Prioriser les actions a mener

Après avoir identifié les traitements de données personnelles, le DPO doit prioriser les actions à mener pour se conformer aux obligations du RGPD, en tenant compte des risques pour les libertés des personnes concernées.

- Des points d'attention importants s'appliquent à tous les traitements, tels que la minimisation des données collectées, la base juridique du traitement, les mentions d'information, les sous-traitants et les droits des personnes.
- Certains traitements nécessitent une vigilance particulière, notamment les données sensibles (origine raciale, santé, etc.) et les traitements de surveillance systématique ou d'évaluation approfondie.
- Pour les transferts de données hors de l'UE, il faut vérifier l'adéquation du pays de destination ou encadrer ces transferts de manière appropriée avec des mesures spécifiques.

Gérer les risques : AIPD

L'Analyse d'Impact sur la Protection des Données (AIPD) est un outil d'évaluation d'impact sur la vie privée permettant de démontrer la conformité d'un traitement au RGPD. Elle se divise en trois parties :

- description du traitement,
- évaluation juridique de la nécessité et proportionnalité
- étude technique des risques sur la sécurité des données et leur impact sur la vie privée. Un risque sur la vie privée est évalué en termes de gravité et de vraisemblance pour les personnes concernées. L'AIPD doit idéalement être réalisée avant la mise en œuvre du traitement et doit être révisée régulièrement.

Démarche de l'AIPD

La démarche de l'AIPD consiste en trois questions :

1. Le traitement est-il susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques? Si oui, passer à la question 2.
2. Le traitement est-il couvert par une exception incluant l'analyse d'impact? Si non, réaliser une AIPD en impliquant le DPO, les personnes concernées, et respecter le code de conduite.
3. Les risques résiduels sont-ils élevés? Si oui, consulter la CNIL (autorité de contrôle). Sinon, aucune consultation n'est nécessaire.

Une AIPD est obligatoire pour les traitements à risques élevés. Elle implique divers acteurs tels que le responsable de traitement, le DPO, les sous-traitants, les métiers et les personnes concernées.

Organiser les processus internes

Pour se conformer au RGPD, l'organisation doit :

- Prendre en compte la protection des données dès la conception des traitements.
- Sensibiliser et former les collaborateurs.
- Traiter les réclamations et demandes des personnes concernées.
- Documenter les traitements, analyses d'impact, contrats, et preuves de consentement.

3.6. Utilisation du SI pour une mise en conformité

Cartographie du SI : définition

La cartographie du SI consiste à représenter de manière schématique le système d'information d'une organisation ainsi que ses connexions avec l'extérieur. Elle permet de réaliser l'inventaire patrimonial du SI et de présenter différentes vues allant du métier vers la technique. Ces vues rendent lisibles et compréhensibles divers aspects du système d'information.

Cartographie du SI : les visions

La cartographie du SI comprend trois visions :

1. Vision métier : représentant l'écosystème du SI et ses processus métier principaux.
2. Vision applicative : décrivant les applications et leurs interactions.
3. Vision infrastructure : illustrant l'infrastructure logique et physique du SI.

3.7. Erreurs courantes

- La non-implication de la Direction.

- La non-compréhension de possession de DCP
- L'oubli de traitements de données.
- Le défaut de gestion des données sortantes
- Le manque de formation/sensibilisation, des personnes concernées

4. Sécurité de l'information & juridiques

4.1. Responsabilité légale du RSSI

La responsabilité légale du RSSI (Responsable de la Sécurité des Systèmes d'Information) peut être de nature pénale ou civile. La responsabilité pénale résulte d'une infraction intentionnelle ou non, tandis que la responsabilité civile découle d'un dommage causé par le RSSI ou ses salariés dans l'exercice de leurs fonctions. Le RSSI doit être conscient de ses responsabilités et des risques associés à ses fonctions, notamment en cas d'infraction intentionnelle. En cas de conflit entre un ordre hiérarchique et la loi, le RSSI reste pénalement responsable de ses actes.

4.2. Forensic: limites légales

Après une attaque, les organisations doivent réagir rapidement. Faire appel à des professionnels qualifiés, accompagnés d'un huissier si nécessaire, garantit la valeur des preuves recueillies en vue de poursuites éventuelles. L'ANSSI propose une liste de prestataires qualifiés pour l'investigation numérique.

4.3. Charte informatique

La charte informatique définit les règles d'utilisation des biens informatiques dans l'entreprise. Sa rédaction doit prendre en compte la protection des données personnelles et inclure les responsabilités et sanctions en cas de non-respect. Elle couvre les modalités d'utilisation des moyens informatiques ainsi que les conditions d'administration du SI. La charte informatique doit être maintenue à jour et alignée sur la vision de l'entreprise, elle a une valeur juridique liée au contrat de travail ou au règlement intérieur de l'entreprise.

4.4. BYOD au sein des organisations

Le BYOD (Bring Your Own Device) est une pratique courante dans de nombreuses organisations, mais sa gestion peut poser des problèmes de sécurité. Des solutions techniques et une charte d'utilisation des biens sont nécessaires pour garantir la sécurité des informations si l'entreprise accepte le BYOD.

4.5. Sécurité de l'information vs utilisation personnelle du SI

Dans de nombreuses organisations, la charte informatique tolère l'utilisation du matériel professionnel à des fins personnelles, ce qui peut poser des problèmes de sécurité avec l'entrée en vigueur du RGPD. L'organisation doit garantir la sécurisation des données personnelles transitant par son système d'information.

5. Prise de poste : bonnes pratiques

5.1. Analyse de l'existant

Lors de votre prise de poste, analysez l'existant en identifiant les acteurs, évaluez la maturité du SI et comprenez le schéma directeur de l'entreprise. Réunissez les documents impactant la sécurité de l'information et identifiez les obligations légales et contractuelles. Consultez le manuel qualité s'il existe pour comprendre les processus et responsables associés.

5.2. Etude des processus

Lorsque vous prenez de nouvelles fonctions, étudiez attentivement les processus sous votre responsabilité. Identifiez et cartographiez ces processus, puis croisez-les avec vos ressources internes et externes. Utilisez le RACI pour visualiser les acteurs critiques pour l'organisation. Cette analyse permettra de mieux comprendre les problématiques opérationnelles et d'effectuer des ajustements préventifs. En cas de projet PCA/PRA, cette étape sera une base importante.

5.3. Schéma directeur SSI

Le schéma directeur SSI aligne les projets sur la stratégie de l'organisation, avec des objectifs quantifiables dans un calendrier défini.