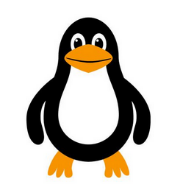
**CEJMA : (B 3.1) : les obligations du responsable de traitement**



Il est important de savoir qui est le responsable de traitement et qui est le sous-traitant dans un contrat passé entre 2 entreprises ou organisations. En effet, en fonction de la qualification qu’elles auront (responsable de traitement ou sous-traitant), elles n’auront pas les mêmes obligations et donc les mêmes responsabilités.

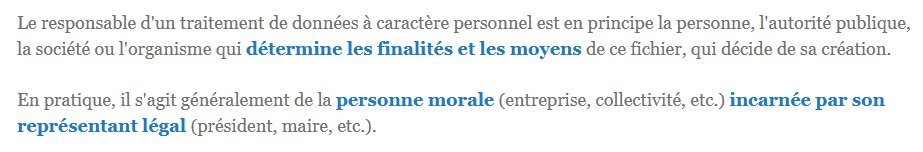
**Compétences : Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel**

**Les obligations du responsable de traitement**

A partir des ressources jointes et de vos recherches, répondez aux questions suivantes :

**Mission 1  : savoir qui est le responsable de traitement ?**

**Document 1 : le responsable de traitement : c’est qui ?**



**Source : CNIL**

**Mission 2: connaitre les obligations du responsable de traitement**

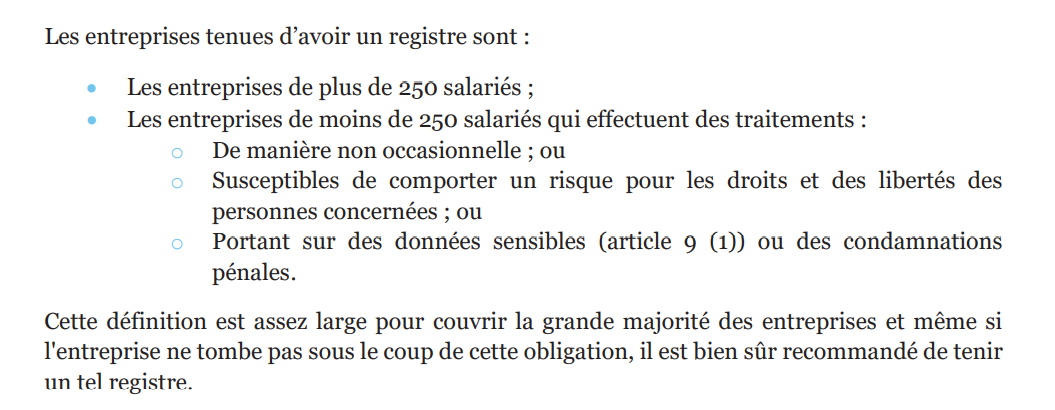
Le RT a plusieurs obligations (elles ne sont pas toutes là) :

* Tenir un **registre des activités** de traitement,
* Désigner un **DPO**,
* Réaliser une **étude d’impact** comprenant privacy by design privacy by default
* Il doit signaler à la CNIL toute violation de DCP dans les 72 heures

**1ere obligation : tenir un registre des activités de traitement**

**Vidéo 1 : La Minute RGPD : Le registre du traitement** [**https://www.youtube.com/watch?v=o9xi39GMylE**](https://www.youtube.com/watch?v=o9xi39GMylE)

**Document 1 : qui doit tenir un registre ?**



**À partir de cette vidéo, répondez aux questions suivantes :**

1. **Qui doit tenir un registre de traitement ?**

Toute entreprise de plus de 250 salariés et celles qui traitent des dcp fréquemment et celles qui traitent des données sensibles.

1. **Identifier les raisons de la tenue d’un registre**

Il permet :

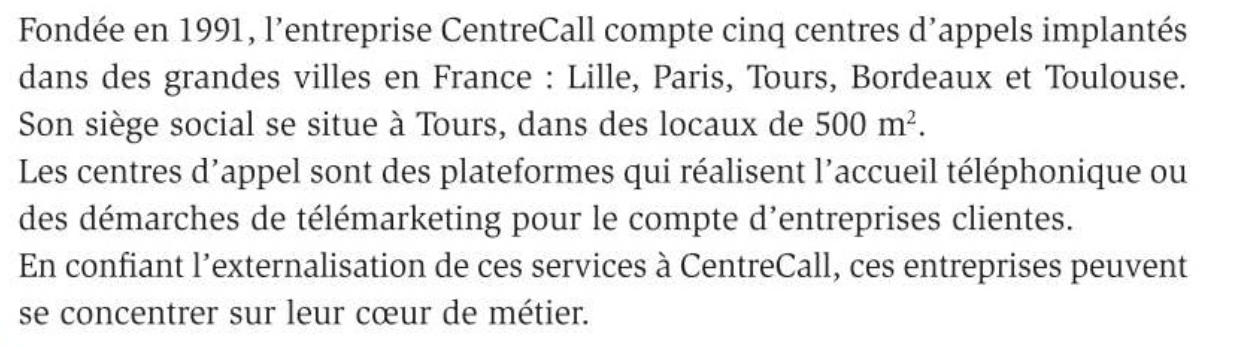
* De recenser les traitements effectués
* D’analyser les traitements
* De prouver sa conformité au RGPD

1. **Repérez les informations que doit contenir le registre**

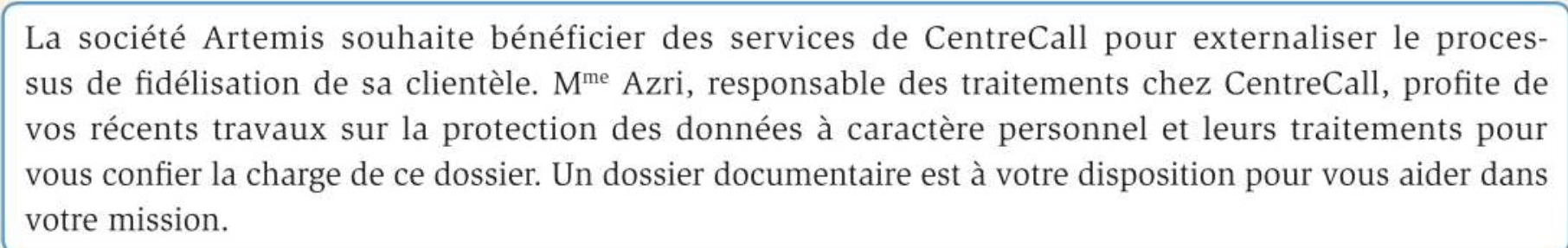
* Le nom et les coordonnées du responsable de traitement, sinon du responsable conjoint, et ceux du délégué à la protection des données
* La finalité du traitement
* Une description des catégories des personnes concernées
* Une description des catégories des dcp
* Les catégories de destinataires auxquels seront communiquées les données :
  + Destinataires internes (dpo, direction informatique,...)
  + Destinataires externes (sous-traitants, partenaires,...)
  + Si les données sont stockées en dehors de l’Union Européenne, préciser le pays
* La durée de conservation des différentes catégories de données
* Une description générale des mesures organisationnelles et de sécurité selon les risques engendrés par le traitement

**Application : la société CentreCall et Artémis**

**Présentation de la société CentreCall**



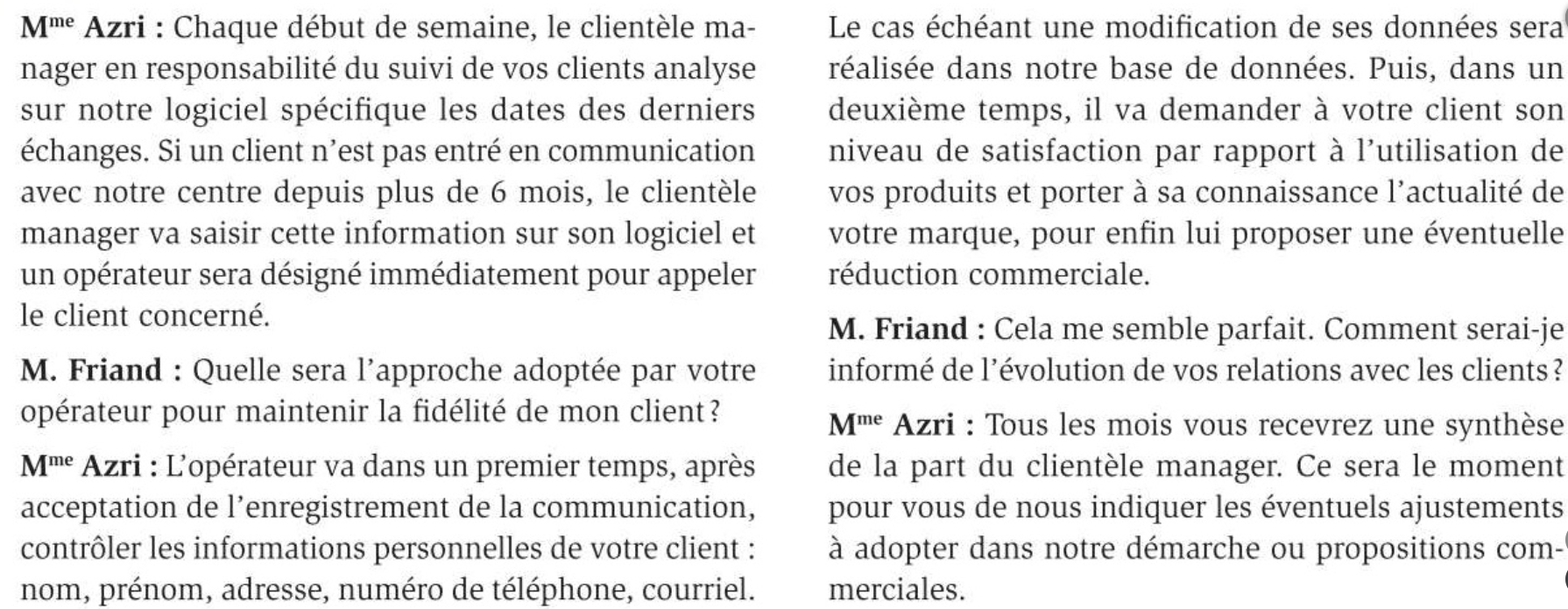
**Présentation de la société Artémis**



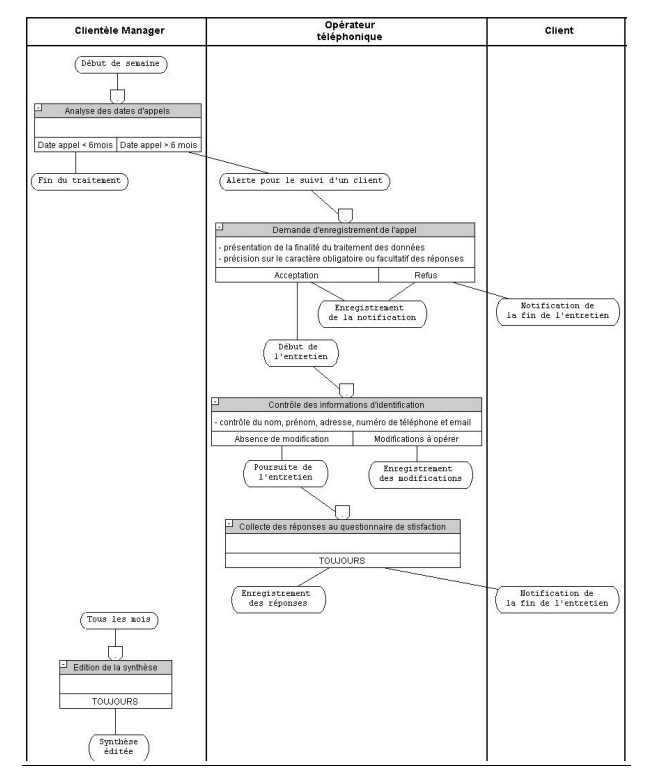
**Présentation du dossier documentaire**



-------------------------------------------------------------------------------------------------------------------------



**Document 2 : processus de fidélisation des clients de la société Artémis**



A partir **des réponses aux questions de la vidéo et des documents**, répondez aux questions suivantes

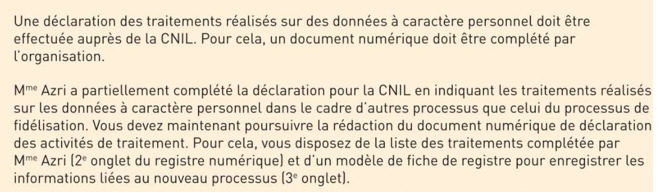
* 1. **Identifiez les données à caractère personnel liées au processus de fidélisation (rappelez la définition d’une DCP)**

Une donnée à caractère personnel est une donnée qui permet d’identifier une personne physique. Dans le processus de fidélisation de CentreCall sont les dcp concernées :

* Appels enregistrés
* Nom, prénom
* Adresse
  1. **Recensez les opérations réalisées sur les données à caractère personnel lors du processus de fidélisation**

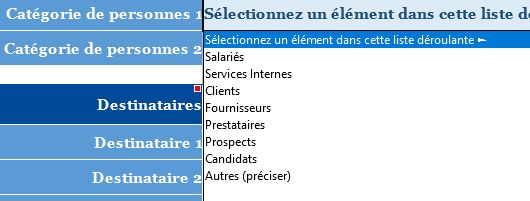
5 opérations peuvent être recensées :

* l’analyse des dates d’appel ;
* la demande d’enregistrement d’un appel ;
* le contrôle des informations d’identification ;
* la collecte des réponses au questionnaire de satisfaction ;
* l’édition de la synthèse



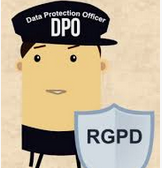
**Document 3 : informations complémentaires**

**Document 4 : catégorie de personnes (onglet 3 du fichier)**



* 1. **À l’aide du document 3 et de vos réponses à la vidéo, complétez le registre numérique des activités de traitement (2e et 3e onglets du document numérique) en tenant compte des réponses apportées aux questions précédentes pour le processus de fidélisation**. (**fichier Excel déposé sur Moodle)**

**2eme obligation : désigner un délégué à la protection des données (DPD ou DPO)**



**A partir de ce document 2 et de vos recherches sur internet, répondez aux questions**



1. **Présentez le rôle d’un DPO (ou DPD : délégué à la protection des données). Quel est le texte qui l’impose ?**

Celui qui met en place la conformité au RGPD et chargé de la protection des dcp dans l’organisation

1. **Citez les organisations qui devront obligatoirement nommer un DPO**

* Les organismes publics
* Les organismes traitant régulièrement des données à grande échelle
* Les organisations qui traitent à grande échelle des données sensibles.

1. **Présentez les missions d’un DPO**

* **Contrôle la conformité des traitements**
* **Aide à la réalisation du registre des traitements (carthographier les traitements)**
* **Informe et conseille les salariés sur la protection des DCP**
* **Mène des analyses d’impact sur la protection des données**
* **Coopère avec la CNIL**

**Qu’autorise le RGPD si l’organisation n’a pas les compétences en interne pour ce métier de DPO ?**

L’organisation peut avoir recours à un DPO externe ou elle mutualise l’activité du DPO avec une autre organisation. Le métier de DPO indépendant se développe.

**3eme obligation : Réaliser une étude d’impact comprenant privacy by design privacy by default**

**NB : Etude d’impact = un PIA (Privacy Impact Assessment), terme plus commun utilisé dans d’autres régions du monde**

**Vidéo 2 :** [**https://www.youtube.com/watch?v=BSFk9qlZmIU**](https://www.youtube.com/watch?v=BSFk9qlZmIU) **(la minute RGPD)**

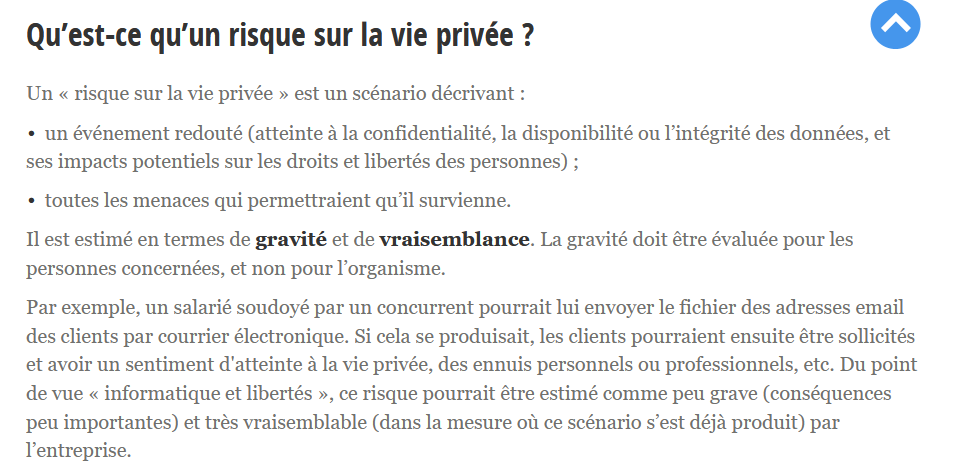
**Document 2 : qu’est-ce que l’analyse d’impact ?**

L’AIPD est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée. Elle concerne les traitements de données personnelles qui sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

L’AIPD est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au Règlement général sur la protection des données (RGPD). Elle est obligatoire pour les traitements susceptibles d’engendrer des risques élevés.

Source : CNIL

**Document 3 : qu’est-ce qu’un risque sur la vie privée ?**



**Document 4 : Liste des types d’opérations de traitement pour lesquelles une analyse d’impact relative à la protection des données n’est pas requise (**[**https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf**](https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf)**)**

**A partir de la vidéo, des documents 2,3 et 4 et de vos recherches sur internet, répondez aux questions**

1. **Qu’est-ce que l’étude d’impact, quels sont ses objectifs ? à quel moment a-t-elle lieu ?**

Cette étude a lieu avant la mise en place du traitement des données.

Elle a pour objectif d’anticiper les risques et de prévoir les mesures pour diminuer les impacts des dommages potentiels sur les DCP

Cela oblige les organisations à être responsable et à démontrer leur conformité.

1. **Tous les traitements de DCP sont-ils concernés par l’étude d’impact ?**

Non, seulement ceux qui soont susceptibles d’engendrer des risques élevés sur les droits et libertés des personnes.

1. **Rappelez ce que signifie privacy by design et cherchez le privacy by défault  ?**

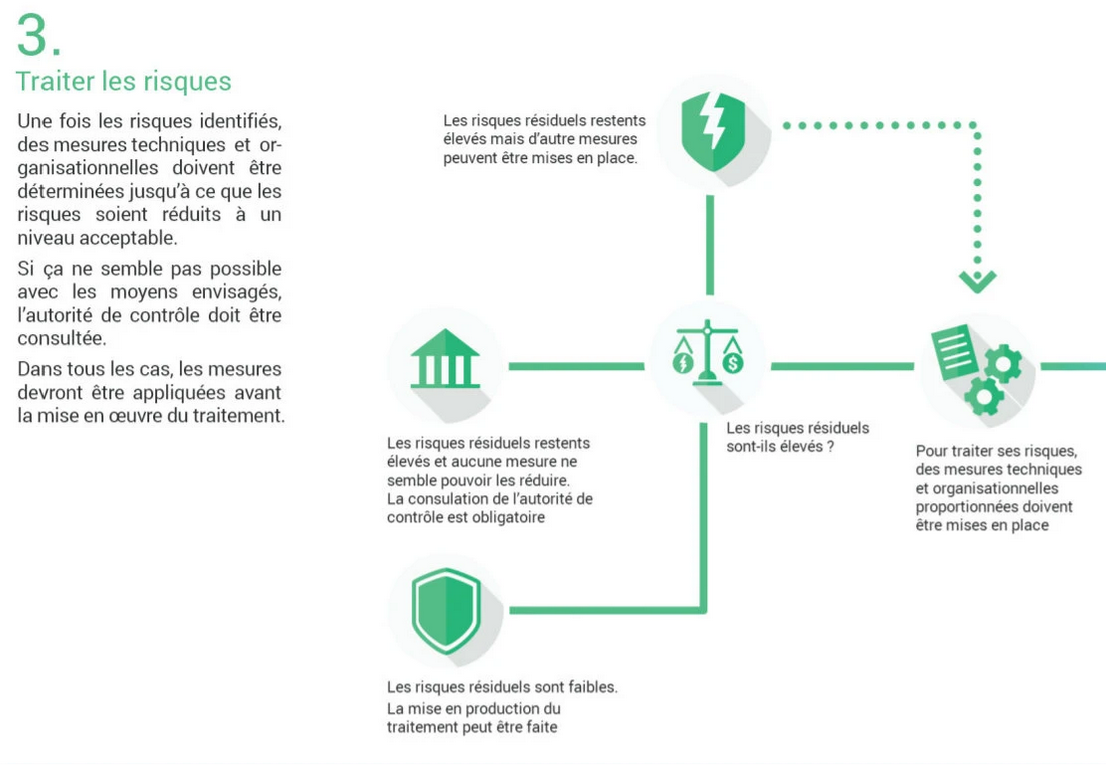
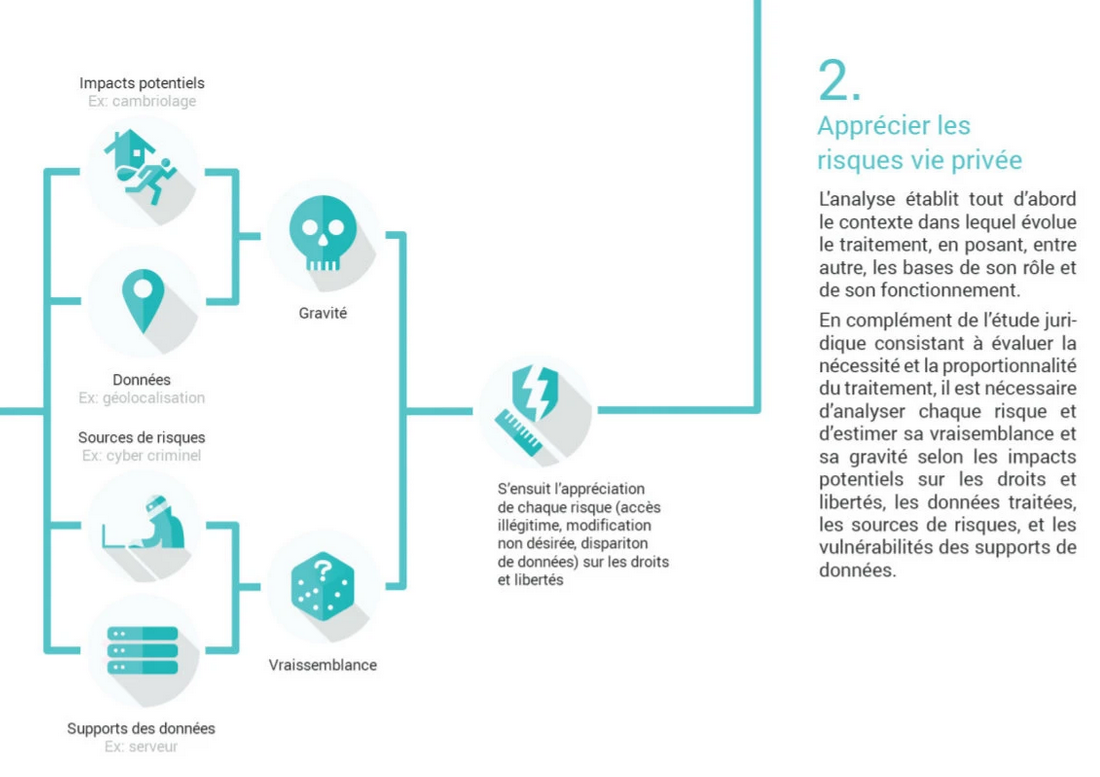
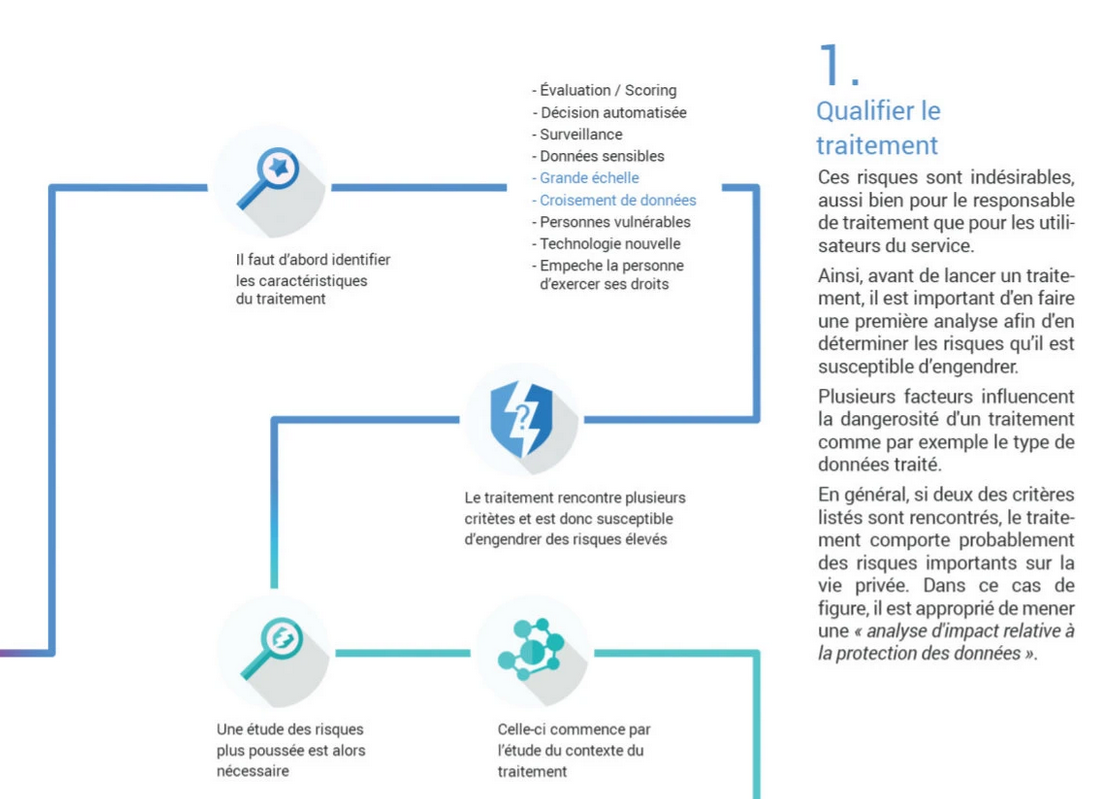
Privacy by design : la protection des dcp est prise en compte dans la conception du produit.

Privacy by default : la protection des données est appliquée par défaut lors de l’utilisation

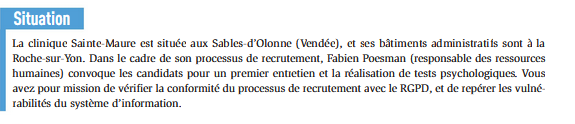
1. **Identifiez les 4 étapes de l’étude d’impact (aide de la vidéo)**

* Une description détaillée du traitement
* Identifier les mesures de protection des dcp existantes ou prévues
* Apprécier les risques et évaluer leur gravité
* Valider les mesures techniques et organisationnelles à mettre en place

**Document 3 : PIA : vue d’ensemble des obligations et de la méthode (source : CNIL)**



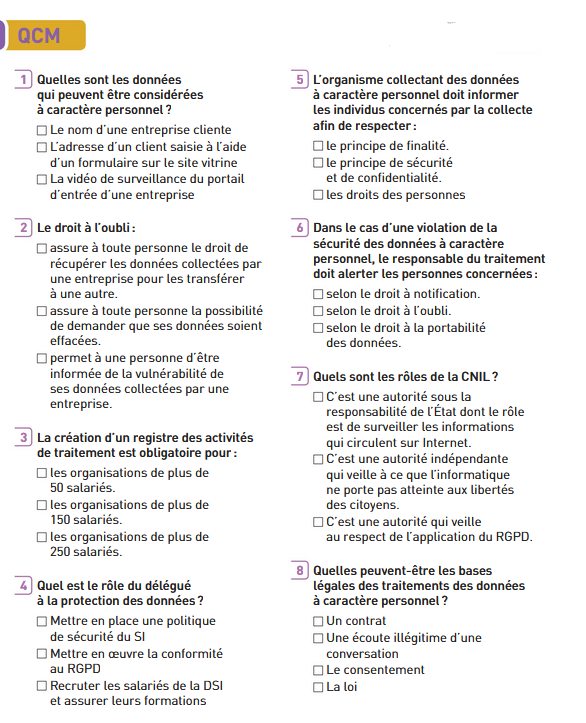
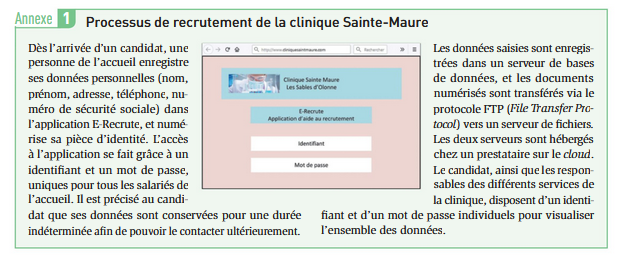
**Application :**



**Vérifiez la conformité du processus de recrutement avec la législation sur la protection des données à caractère personnel (annexe 1).**

Collectant nom, prénom, adresse et numéro de sécurité, le RGPD s’applique.

La protection des données n’est pas assurée : même identifiant pour tous les salariés et conservation des données pour une durée indéterminée.



**Mission 3 : réaliser un résumé**

TRAVAIL DE GROUPE : A l’aide de vos réponses et des ressources

Réaliser **une note d’information ou un résumé** sur :

**Les obligations du responsable de traitement**

Pour réaliser ce travail, **vous compléterez le pad collaboratf qui** est sur Moodle