Mission 2 Gérer les risques sur les données personnelles

Le premier travail à réaliser en matière de gestion des risques sur les données personnelles est de déterminer **dans quelle mesure les traitements réalisés font peser un risque élevé sur les personnes**.

Selon les cas, il s'agira alors :

* au minimum, d'appliquer les règles de bonnes pratiques en matière de sécurité des données ;
* si le risque est important, le RGPD recommande, voire parfois oblige à réaliser une analyse des risques plus poussée : une « analyse d'impact relative à la protection des données personnelles » (AIPD).

Contexte et cahier des charges

La mission 1 vous a permis d'assurer un premier niveau de conformité au RGPD du site de Permabook. Cependant, aucun des aspects liés spécifiquement à la sécurité n'a été traité : c'est l'objet de cette mission 2.

M. Pouget considère que la sécurité des données personnelles de ses clients est fondamentale. Cela correspond aux principes éthiques qu'il prône dans sa librairie. Il a aussi conscience que cet aspect est essentiel dans le rapport de confiance qui doit s'engager entre un site de vente en ligne et ses clients.

Il vous demande de ne pas vous limiter forcément aux mesures obligatoires. Il est prêt à dépenser un peu plus d'argent que nécessaire à court terme dans la mise en place d'une véritable politique de sécurisation des données personnelles en espérant que cet investissement sera récompensé à moyen et long terme.

**SOMMAIRE**

[I Identifier le niveau de risque 3](#_Toc53569543)

[II Application des règles de bonnes pratiques (pour un site de vente en ligne) 3](#_Toc53569544)

[III Analyse d'Impact relative à la Protection des Données (AIPD) 4](#_Toc53569545)

[1 Préalable : observer l'AIPD existante 4](#_Toc53569546)

[2 Méthodologie d'AIPD 4](#_Toc53569547)

[2.1 Analyse des risques actuels 5](#_Toc53569548)

[2.1.1 Evaluation des mesures existantes 5](#_Toc53569549)

[2.1.2 Appréciation des risques : les atteintes potentielles à la vie privée 5](#_Toc53569550)

[2.2 Finalisation de l'AIPD (4H) 6](#_Toc53569551)

[IV ANNEXES 7](#_Toc53569552)

[1 ANNEXE 1 : Analyse des mesures existantes de sécurité sur les données personnelles 7](#_Toc53569553)

|  |
| --- |
| **Organisation du travail**  Vous travaillerez par groupe de 3/4 étudiants.  Vous réaliserez dans un premier temps les TAF 1 et 2 en vous répartissant le travail (2h).  Vous travaillerez ensuite sur le TAF 3 en vous répartissant l'étude des mesures de sécurité. Vous réaliserez un document texte qui servira à compléter l'AIPD sur le logiciel PIA (4h).   * **Dossier documentaire à rendre**  1. Analyse du risque : justification de l'AIPD 2. Règles de bonnes pratiques appliquées à un site web 3. Fichier json contenant l'AIPD complétée et document texte associé.  * **Durée prévue** : 6h classe |

|  |
| --- |
| **Ressources**   * Fiche savoir 1 Traitement des données à caractère personnel * Fiche savoir 2 Sécurité vs sureté, c'est l'intention qui compte * Fiche savoir 3 Principes de sécurité des données * Fiche savoir 4 Gérer les risques portant sur les données personnelles * Fiche méthode 1 Démarche de conformité au RGPD => page 3 * Site web [http://permabook.si24.fr](http://permabook.si24.fr/) * > ressources > R\_Mission 2 |

#### Identifier le niveau de risque

1. Répondre aux questions préalables ci-dessous en vous appuyant sur la fiche savoir 1.
   1. Lors de la mission 1, avez-vous mis en évidence des traitements portant sur des **données sensibles** au sens RGPD ou **hautement personnelles** ? Si oui, lesquelles ?
   2. Analyser, les bons de commande 162 et 163 d'Agathe et de Jean. Peut-on en déduire des informations portant sur leur état de santé, leurs opinions philosophiques, politiques... ?
   3. Imaginer des situations dans lesquelles le fait de révéler ces informations serait hautement préjudiciable à Agathe et Jean. Pensez aux contextes personnels et professionnels.
2. Rédiger une note expliquant à Permabook s'il est nécessaire, judicieux ou inutile de réaliser une AIPD. Vous reprendrez les réponses du TAF0 et vous utiliserez la **fiche savoir 4**.

|  |
| --- |
| **Ressources** :   * Fiche savoir 1 Traitement des données à caractère personnel * Fiche savoir 4 §I Quand doit-on mener une AIPD ? |

#### Application des règles de bonnes pratiques (pour un site de vente en ligne)

Quelles que soient les réponses apportées précédemment, Permabook est censée mettre en œuvre au minimum les règles de bonnes pratiques en matière de sécurité des équipements numériques pour assurer la sécurité des données personnelles qu'elle traite.

1. Analyser les règles de bonnes pratiques édictées par l'ANSSI et reprises par la CNIL : les règles applicables de façon générales et les règles spécifiques aux sites web. Pour chaque règle applicable au site web de Permabook, en déduire des implications concrètes en ce qui concerne le site web et l'entreprise Permabook.

Modèle de tableau d'analyse (à mettre en format paysage)

|  |  |  |  |
| --- | --- | --- | --- |
| **Règle** | **Applicable ?** | **Situation actuelle** | **Préconisations** |
|  | ⬜ |  |  |

|  |
| --- |
| **Ressources** :   * Fiche méthode 1 partie « Sécuriser les données »   + **N1 Les bonnes pratiques**   <https://www.cnil.fr/fr/securite-des-donnees-les-regles-essentielles-pour-demarrer>  <https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-douze-questions/>   * Spécificité des sites web :   + **Règles minimales**  <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf> p.19   + Sécurité approfondie : <https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Securite_Web_NoteTech.pdf> <https://www.ssi.gouv.fr/entreprise/guide/recommandations-pour-la-securisation-des-sites-web/> |

#### Analyse d'Impact relative à la Protection des Données (AIPD)

Une AIPD a donc été jugée utile. Elle devra permettre de gérer de façon précise et durable les risques sur les données personnelles.

Pour réaliser une AIPD, votre responsable au sein de l'ESN utilise l'outil dédié mis à disposition par la CNIL : le logiciel PIA.

Il a réalisé une analyse de l'existant en reprenant le travail de la mission 1 et en analysant les mesures de sécurité actuelles.

Votre travail va consister :

* à proposer des mesures correctrices pour que le niveau de risque résiduel sur les données personnelles soit jugé « limité » ;
* à compléter l'AIPD existante.

Vous commencerez par prendre connaissance de la méthodologie à respecter pour mener une AIPD.

|  |
| --- |
| Ressources   * Fichiers à enregistrer dans > Ressources > Kit RGPD > PIA > documents   + <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf>   + [https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf p. 13](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf)   + <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf> * AIPD partielle : > ressources > R\_Mission 2 > PIA > pia-Permabook-evaluation\_commencée.json |

##### Préalable : observer l'AIPD existante

Objectif : installer l'environnement de travail et observer l'AIPD partiellement réalisée

* Installer le logiciel PIA : <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>
* Importer l'AIPD partielle :
  + ouvrir PIA puis choisir d'importer ;
  + utiliser le fichier pia-Permabook-evaluation\_commencée.json

##### Méthodologie d'AIPD

Nous ne reviendrons pas sur les parties « Contexte » et « Principes fondamentaux » qui ont été réalisées en tenant compte du travail effectué dans la mission 1. Ces parties ont déjà été validées par votre supérieur.

Seule la partie risque sera étudiée ici.

La démarche d'AIPD comporte deux étapes :

* + **dans un premier temps**, une appréciation des risques tenant compte des **mesures existantes** est réalisée : cette étape a déjà été effectuée par votre responsable.
  + **dans un deuxième temps**, il est nécessaire d'évaluer ces mesures au regard des risques identifiés précédemment, d'évaluer les risques eux-mêmes et de **proposer des mesures pour rendre ces risques acceptables**.

###### Analyse des risques actuels

Voici une synthèse du travail déjà réalisé. Vous aurez besoin de comprendre ce qui a été fait pour compléter l'analyse.

Evaluation des mesures existantes

|  |
| --- |
| Ressources :   * <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-fr-methode.pdf> * <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf> mesures p. 13 |

Voici un classement des principales mesures identifiées par la CNIL :

* + mesures portant sur les données de traitement : chiffrement, anonymisation, cloisonnement, contrôle d'accès physiques et logiques, traçabilité, contrôle d'intégrité, archivage, sécurité des documents papier ;
  + mesures générales de sécurité du système dans lequel le traitement est mis en œuvre : sécurité de l'exploitation, lutte contre les logiciels malveillants, gestion des postes de travail, sécurité des sites web, sauvegardes, maintenance, sécurité des canaux informatiques, surveillance, contrôle d'accès physique, sécurité des matériels, éloignement des sources de risque, protections contre les sources de risque non humaines ;
  + mesures organisationnelles (gouvernance) : organisation, politique, gestion des risques, gestion des projets, gestion des incidents et violations, gestion des personnels, relations avec les tiers, supervision.

Appréciation des risques : les atteintes potentielles à la vie privée

Objectif : obtenir une bonne compréhension des causes et conséquences des risques.

* Pour chaque événement redouté (un accès illégitime à des données, une modification non désirée de données et une disparition de données) :
  + déterminer **les impacts potentiels** sur la vie privée des personnes concernées s'il survenait ;
  + identifier **les menaces** sur les supports des données qui pourraient mener à cet événement redouté **et les sources** de risques qui pourraient en être à l’origine ;
  + estimer sa **gravité**, notamment en fonction du caractère préjudiciable des impacts potentiels et, le cas échéant, des mesures susceptibles de les modifier ;
  + estimer sa **vraisemblance**, notamment en fonction des vulnérabilités des supports de données, des capacités des sources de risques à les exploiter et des mesures susceptibles de les modifier.
* Déterminer si les risques ainsi identifiés peuvent être jugés acceptables compte tenu des mesures existantes ou prévues.

|  |
| --- |
| Ressources :   * Annexe 1 de ce document : Analyse des mesures existantes de sécurité sur les données personnelles * Fichiers (disponibles dans Ressources > R\_Mission 2 > PIA > documents)   + <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-fr-modeles.pdf> p. 20   + <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf>     - Les sources : p.3     - Les menaces pp. 6 à 9     - Impact et gravité pp. 3 à 5     - Vraisemblance du risque pp. 5 à 6 |

###### Finalisation de l'AIPD (4h)

1. Finaliser l'AIPD en étudiant les risques actuels, en complétant les mesures actuelles ou en en proposant de nouvelles. Avant de compléter l'AIPD sur le logiciel, vous réaliserez un document texte de façon collaborative : ce document sera ensuite reporté par chaque personne responsable dans le PIA.

* Etudier les mesures et les risques actuels.
* Compléter les mesures actuelles.
* Pour chaque type de risque, identifiez de nouvelles mesures et les documenter.
* Procéder à l'évaluation finale des risques d'accès, de modification et de disparition des données.

**=> Vous remettrez**

* + **le document texte contenant l'analyse des mesures et des risques,**
  + **un fichier json contenant l'AIPD complétée en attente de validation par le DPD.**

|  |
| --- |
| Ressources :   * Fiche savoir 4 Gérer les risques portant sur les données personnelles * Annexe 1 de ce document * Fichier (disponible dans Ressources > Kit RGPD > PIA > documents) <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf>   + Les sources : p.3   + Les menaces pp. 6 à 9   + Impact et gravité pp. 3 à 5   + Vraisemblance du risque pp. 5 à 6 * Pia partielle : > Ressources > R\_Mission 2 > PIA > pia-Permabook-evaluation\_commencée.json |

#### ANNEXES

##### ANNEXE 1 : Analyse des mesures existantes de sécurité sur les données personnelles

*Les numéros de page indiqués font référence à la base de connaissance créée par la CNIL :*

[*https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf*](https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-fr-basesdeconnaissances.pdf)

**Contrôle des accès logiques p. 23**

Limiter les risques que des personnes non autorisées accèdent aux données à caractère personnel par voie électronique.

Mesures actuelles :

* Les utilisateurs reçoivent les droits nécessaires et suffisants pour assurer leurs missions. Plusieurs groupes sont définis : administrateur, gestionnaire de boutique...
* Un mot de passe fort n'est pas obligatoire. Seul un niveau « moyen » de complexité est exigé.

**Sécurisation de l'exploitation p. 87**

Politiques permettant de limiter la vraisemblance et la gravité des risques visant les biens supports utilisés en exploitation.

Mesures actuelles :

* Le site est mis à jour automatiquement : Wordpress, thème et extensions.

**Sauvegarde des données p. 79**

Assurer la disponibilité et/ou l'intégrité des données à caractère personnel, tout en protégeant leur confidentialité.

Mesures actuelles :

* La base de données est sauvegardée régulièrement par OVH.

**Protection des sites web p. 103**

Diminuer la possibilité que les caractéristiques des sites web soient exploitées pour porter atteinte aux données à caractère personnel.

Mesures actuelles :

* Les cookies sont déposés après consentement

**Gérer les risques p. 52**

Maîtriser les risques que les traitements de l'organisme font peser sur les droits et libertés des personnes concernées.

Mesures actuelles :

* Une AIPD est réalisée.