CHELLE Raymond 05/11/2025

Rapport de TP : PIA 1

Sommaire :

I. Introduction

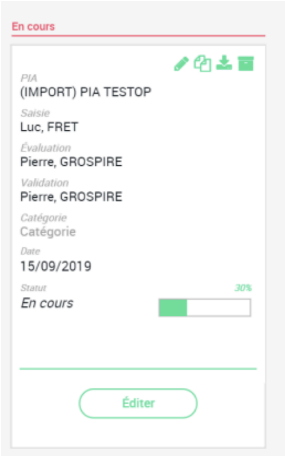
Nous cherchons à développer notre savoir-faire afin de répondre aux exigences de sécurité du système d'information d'une organisation, en prenant en compte l'ensemble de ses dimensions. Pour atteindre cet objectif, nous allons réaliser plusieurs exercices pratiques d'application.

II. Le travail à réaliser

Pour pouvoir réaliser les exercices suivants, nous allons d'abord installer le logiciel **PIA** sur notre ordinateur en utilisant le lien suivant :
https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

Une fois l'installation terminée, nous importerons le travail fourni sous forme de fichier **.json**, disponible à cette adresse :
lienmini.fr/6988-106

Après avoir installé le logiciel, il suffit d'**importer le projet** dans PIA pour commencer à travailler dessus.



2.

Nous allons maintenant évaluer les **niveaux de gravité** et de **vraisemblance** pour trois situations possibles :

- Accès illégitime à des données,
- Modification non désirée de données,
- Disparition de données.

Définition des niveaux de gravité :

1. **Négligeable** : Aucun impact réel, aucune perturbation notable.
2. **Limité** : Impact faible, facilement réversible, peu coûteux.
3. **Important** : Conséquences sérieuses pouvant affecter l'activité, les clients ou engendrer des impacts financiers ou juridiques.
4. **Maximal** : Effets catastrophiques, irréversibles ou très lourds (sanctions, atteinte à la réputation, interruption de l'activité).

Définition des niveaux de vraisemblance :

1. **Négligeable** : Situation exceptionnelle, peu susceptible de se produire.
2. **Limitée** : Risque rare mais possible.
3. **Importante** : Risque régulier, se produisant fréquemment.
4. **Maximale** : Risque quasi certain, constant en l'absence de mesures de sécurité.

Analyse des trois cas

1. Accès illégitime à des données

- **Niveau de gravité : 5**
  Les coordonnées personnelles des salariés constituent des informations hautement sensibles. Un accès non autorisé peut entraîner une atteinte grave et irréversible à la vie privée. Parmi les menaces potentielles, on retrouve les attaques ciblant le serveur de bases de données ou l'interception des échanges lors du transfert vers l'hébergement (par exemple, chez OVH).
- **Niveau de vraisemblance : 4**
  Ce type d'incident est plausible en raison de la fréquence des attaques menées par des acteurs externes ou des concurrents. Ces menaces sont courantes dans la plupart des secteurs d'activité.

2. Modification non désirée de données

- **Niveau de gravité : 4**
  Une altération non souhaitée des données personnelles peut générer des incohérences dans les profils des salariés, fausser les offres de formation ou bloquer les propositions de mutation ou de promotion. De telles erreurs ont un impact direct sur la carrière et les droits des employés.
- **Niveau de vraisemblance : 3**
  Ce risque peut résulter d'un accès non autorisé au disque de sauvegarde, d'une interception lors du transfert vers la base de données ou d'un vol d'identifiants de connexion. Ces situations sont plausibles, bien que moins fréquentes qu'une attaque externe.

3. Disparition de données

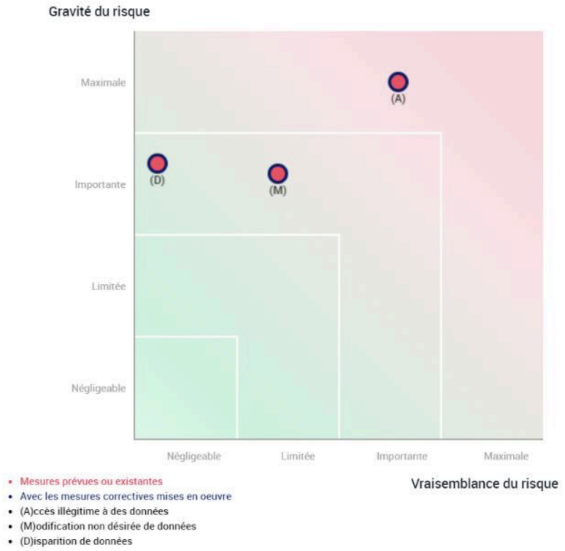
- **Niveau de gravité : 4 (voire 5 sans sauvegarde)**
  La perte de données personnelles peut entraîner la disparition

d’éléments essentiels des parcours professionnels des salariés. Cela peut imposer la répétition de tests de compétences ou empêcher temporairement l’accès à certaines formations.

- **Niveau de vraisemblance : 2**
  Le risque peut provenir d’attaques sur les serveurs, de pannes matérielles ou d’erreurs humaines. Toutefois, grâce aux mesures de sauvegarde mises en place, la probabilité d’une perte totale reste faible, bien que non négligeable.

3.

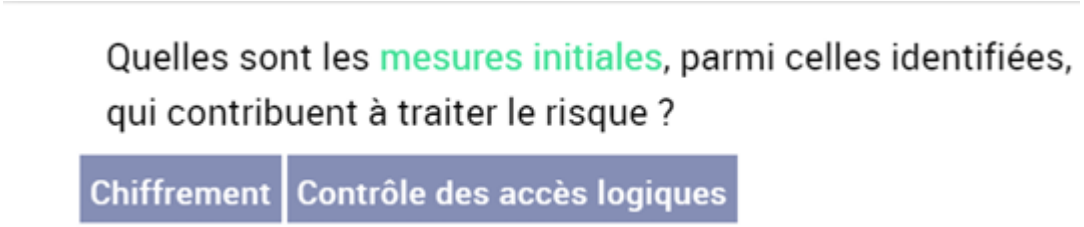
En commentant et en évaluant les niveaux de gravité et de vraisemblance, et après demande d’évaluation cela va remplir la cartographie des risques :



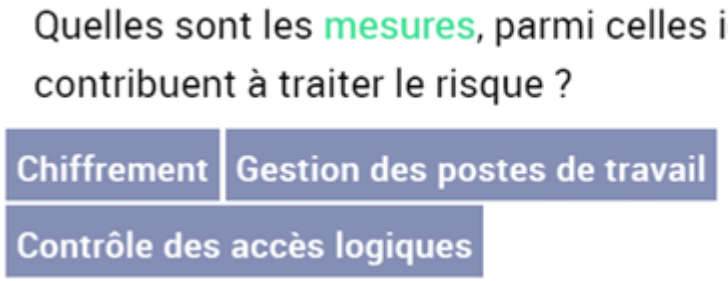
Comme nous pouvons le constater, l’accès illégitime aux données représente le risque le plus probable et le plus critique.
La disparition de données, bien que moins fréquente, conserve un niveau de gravité élevé, même en présence de sauvegardes.
Et la modification non désirée de données apparaît plus probable qu’une disparition, mais moins que l’accès illégitime.

4. Les mesures correctrices envisageables sont déjà données par 3 le fichier .json du lien donné, donc nous allons simplement les répertorier ici :

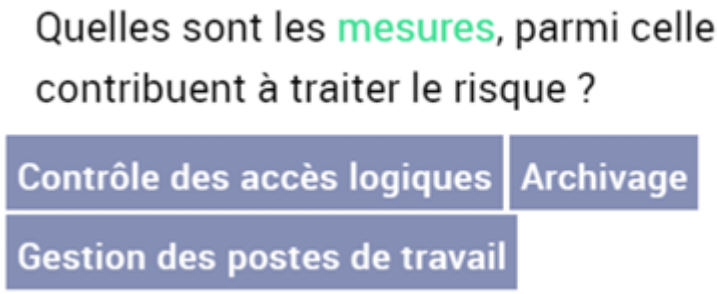
Accès illégitime :



Modification non désirée des données :



Disparition des données :



5. Les mesures correctives étaient déjà apparentes sur le schéma d'avant, mais pour préciser à ce qu'elles changent, elles modifient le niveau de gravité et de vraisemblance des cas par rapport aux mesures correctrices qui leurs sont attribuées.

2) Cartographie du traitement des données à caractère personnel

La cartographie des traitements des données à caractère personnel consiste à identifier l'emplacement des données au sein de l'entreprise et à recenser l'ensemble des traitements qui leur sont appliqués. Elle permet d'avoir une vision claire de toutes les informations détenues et de comprendre comment elles sont collectées, utilisées et stockées.

Cette démarche repose sur un recensement précis des données traitées par chaque service ou collaborateur. Elle est généralement menée par le Délégué à la Protection des Données (DPO). L'objectif principal est de garantir la mise en conformité de l'entreprise avec le Règlement Général sur la Protection des Données (RGPD). Sans cette cartographie, il serait

impossible d'établir des documents essentiels tels que le registre des traitements ou de repérer les risques liés à la gestion des données. Elle constitue donc une étape indispensable pour assurer la sécurité et la bonne utilisation des données personnelles au sein de l'entreprise.

Le registre des traitements représente la trace écrite de ce recensement. Il précède la cartographie et en constitue la base : c'est grâce à lui que l'on peut ensuite dresser une cartographie claire et exhaustive de tous les traitements effectués sur les données.

3) Repérer l'utilisation des données à caractère personnel

Lorsqu'un utilisateur saisit ses données personnelles sur le site **Castorama.fr**, celles-ci peuvent être partagées avec d'autres entités du groupe **Kingfisher**, qui possède plusieurs enseignes comme **Brico Dépôt** ou **B&Q**. Ce partage a pour objectif d'améliorer les services numériques du groupe et de proposer des offres adaptées aux besoins et aux centres d'intérêt des utilisateurs.

Castorama peut également transmettre certaines données à des **partenaires commerciaux** ou à des **assureurs**, notamment en cas de procédure judiciaire. Les informations peuvent aussi être utilisées de manière **anonyme** afin d'établir des statistiques. En résumé, les données saisies sur le site peuvent être exploitées à des fins commerciales ou partagées avec les filiales et partenaires du groupe Kingfisher.

Concernant la confidentialité, l'extrait étudié ne permet pas d'affirmer que celle-ci n'est pas assurée. Il précise que les données sont uniquement partagées avec des partenaires de confiance. Cependant, aucune information n'est donnée sur les mesures de sécurité mises en place, ce qui laisse la possibilité de failles potentielles. Il est donc recommandé de rester prudent et de limiter la quantité de données personnelles partagées sur les sites internet.

4) Traitement et risques liés aux données à caractère personnel

Les données personnelles peuvent être collectées, stockées et diffusées par différents moyens, tels que :

- Les formulaires en ligne ;
- Les applications mobiles ;
- Les enregistrements vocaux ou vidéo ;
- Les jeux-concours sur les réseaux sociaux ;
- Les organismes officiels (banques, services fiscaux, etc.).

Une fois recueillies, ces données sont généralement stockées dans des **bases de données internes** ou dans des **fichiers clients**. Elles peuvent ensuite être diffusées par différents canaux, comme le courrier électronique, le téléphone ou encore la revente de fichiers à des entreprises partenaires.

La vidéo étudiée met en évidence plusieurs types de traitements possibles : la **collecte**, l'**enregistrement**, la **conservation**, la **consultation**, la **communication** et la **suppression**. Ces traitements peuvent être réalisés manuellement ou de façon automatisée, et ils servent principalement à la gestion interne et au marketing.

Le **responsable du traitement** doit respecter plusieurs obligations prévues par le RGPD. Il doit notamment définir la finalité du traitement, s'assurer que seules les données nécessaires sont collectées, garantir leur sécurité et leur confidentialité, et supprimer les informations une fois leur utilisation terminée. Il doit également s'assurer que les sous-traitants respectent les mêmes exigences en matière de protection des données.

En cas de non-respect du RGPD, les sanctions peuvent être très lourdes. Les entreprises s'exposent à des **amendes pouvant aller jusqu'à 4 % du chiffre d'affaires mondial** ou **20 millions d'euros** pour les infractions les plus graves. En cas de manquement à la sécurité, la sanction peut atteindre **2 % du chiffre d'affaires** ou **10 millions d'euros**. Dans certains cas, des **peines d'emprisonnement pouvant aller jusqu'à cinq ans** peuvent être prononcées. Enfin, ces manquements peuvent fortement nuire à la réputation et à la crédibilité de l'entreprise.

5) Dissociation des notions de sécurité et de sûreté informatique

Scénarios	Sécurité	Sûreté	Justifications
L'ensemble des serveurs est hors-service à cause d'une inondation du local technique		✓	Il s'agit d'un événement naturel (inondation), donc lié à la sûreté (protection contre les accidents).
Les données d'un hôpital sont illisibles à la suite d'une attaque de type ransomware	✓		Le ransomware est une attaque informatique intentionnelle donc elle relève de la sécurité (protection contre les actes malveillants).
L'apparence du site vitrine d'une entreprise est modifiée pendant un week-end par des personnes malveillantes	✓		Modification malveillante du site par des hackers, donc problème de sécurité.
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs		✓	La panne est due à un incident technique non intentionnel (surcharge), donc liée à la sûreté.

6) Identifier les données à caractère personnel

Données	Caractère personnel	Justifications
Le nom de l'enseigne du magasin Carrefour	X non	Il s'agit d'une information liée à une entreprise et non à une personne identifiable.
L'adresse courriel professionnelle d'un directeur des services informatiques	V oui	Permet d'identifier une personne physique par sa fonction et ses coordonnées professionnelles.
Une photo postée sur un réseau social	V oui	Une photo permet souvent d'identifier une personne physique.
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	V oui	La vidéo contient des informations personnelles et permet d'identifier la personne.
Les coordonnées GPS de localisation d'un smartphone	V oui	Les données GPS permettent de suivre et d'identifier la localisation d'une personne.
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	V oui	Le groupe sanguin est une donnée de santé directement liée à une personne.
Les enregistrements de vidéosurveillance d'un datacenter	V oui	Les enregistrements peuvent permettre d'identifier une personne filmée.
Le numéro d'enregistrement au registre du commerce et des sociétés d'une entreprise	X non	Information liée à une personne morale (entreprise), pas à une personne physique.
Le numéro de sécurité sociale d'un salarié saisi sur sa fiche d'embauche	V oui	Le numéro de sécurité sociale identifie directement une personne physique.

III. Conclusion

En conclusion, ce TP m’a permis de mieux comprendre la gestion et la protection des données à caractère personnel, j’ai pu apprendre grâce aux exercices à identifier les données sensibles, à évaluer les risques et à proposer des mesures de sécurité adaptées à la menace.