

PROTÉGER LES DONNÉES À CARACTÈRE PERSONNEL (PIA) **(Partie 1)**

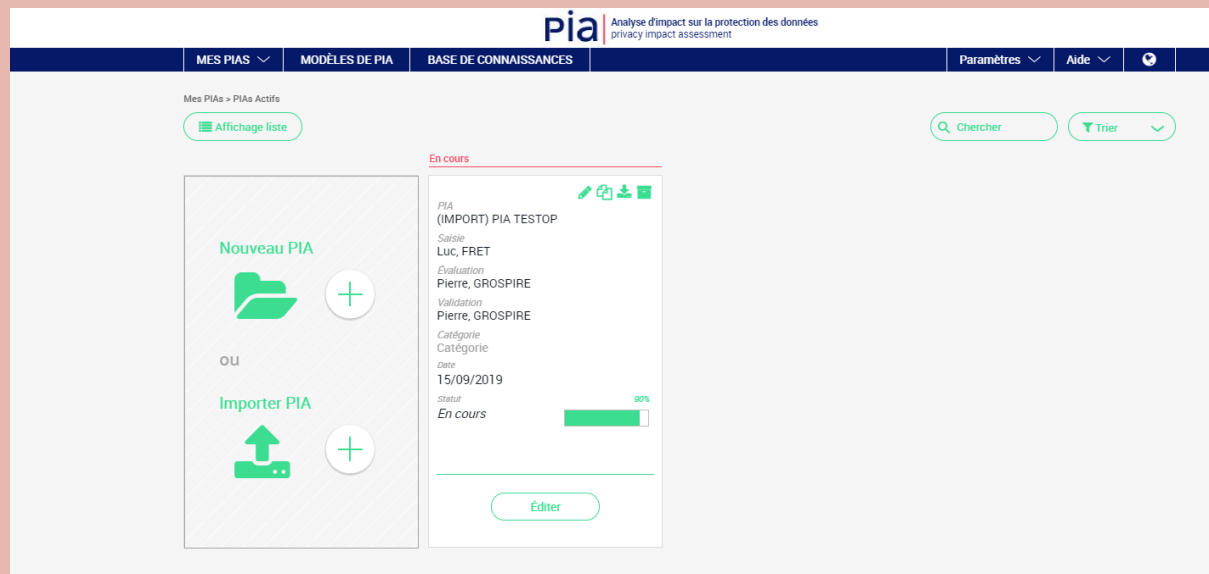


- [1- Analyser un PIA](#)
- [2- Cartographier le traitement des données à caractère personnel](#)
- [3- Repérer l'utilisation des données à caractère personnel](#)
- [4- Traitements et risques sur les données à caractère personnel](#)
- [5- Dissocier les notions de sécurité et sûreté informatique](#)
- [6- Identifier les données à caractère personnel](#)

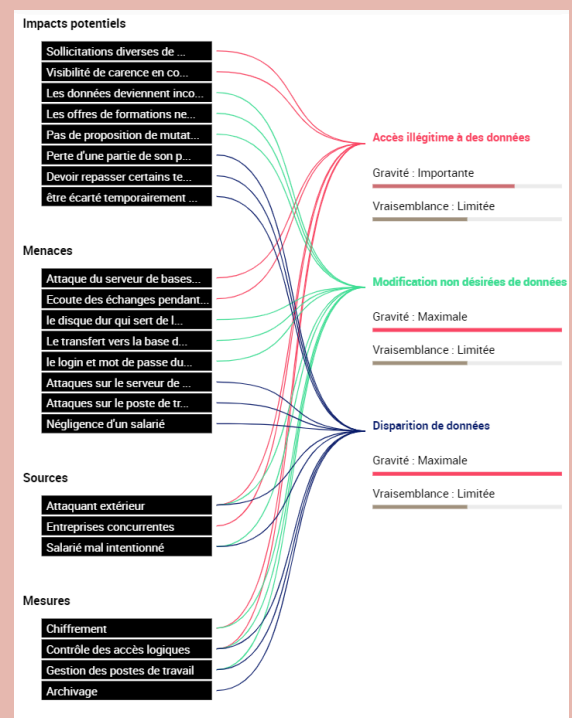
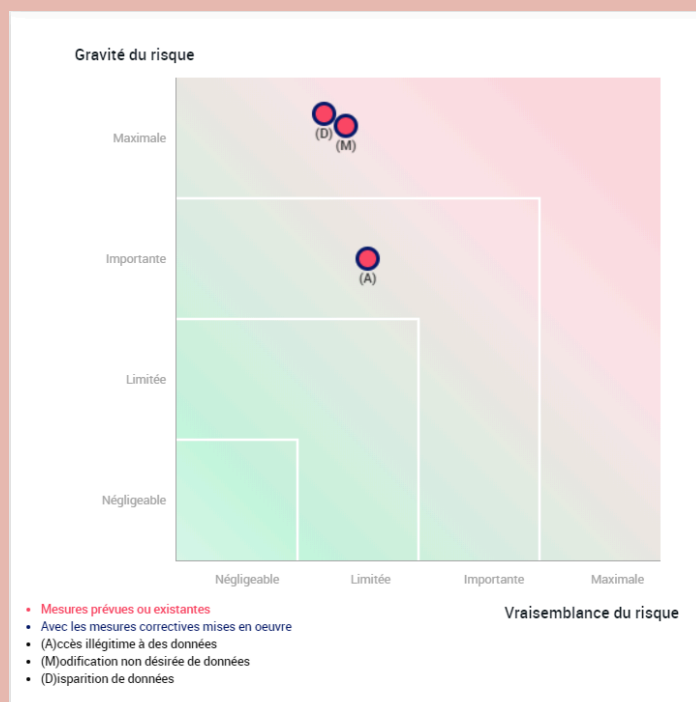
La problématique : Identifier des données à caractère personnel et évaluer les risques qui leur sont associés

1- Analyser un PIA

1- Nous devons importer le travail de M.Grospire dans l'application PIA.



2 et 3- Nous devons ensuite évaluer la gravité et la vraisemblance des trois risques principaux pouvant affecter les données à caractère personnel au vu des réponses déjà fournies.

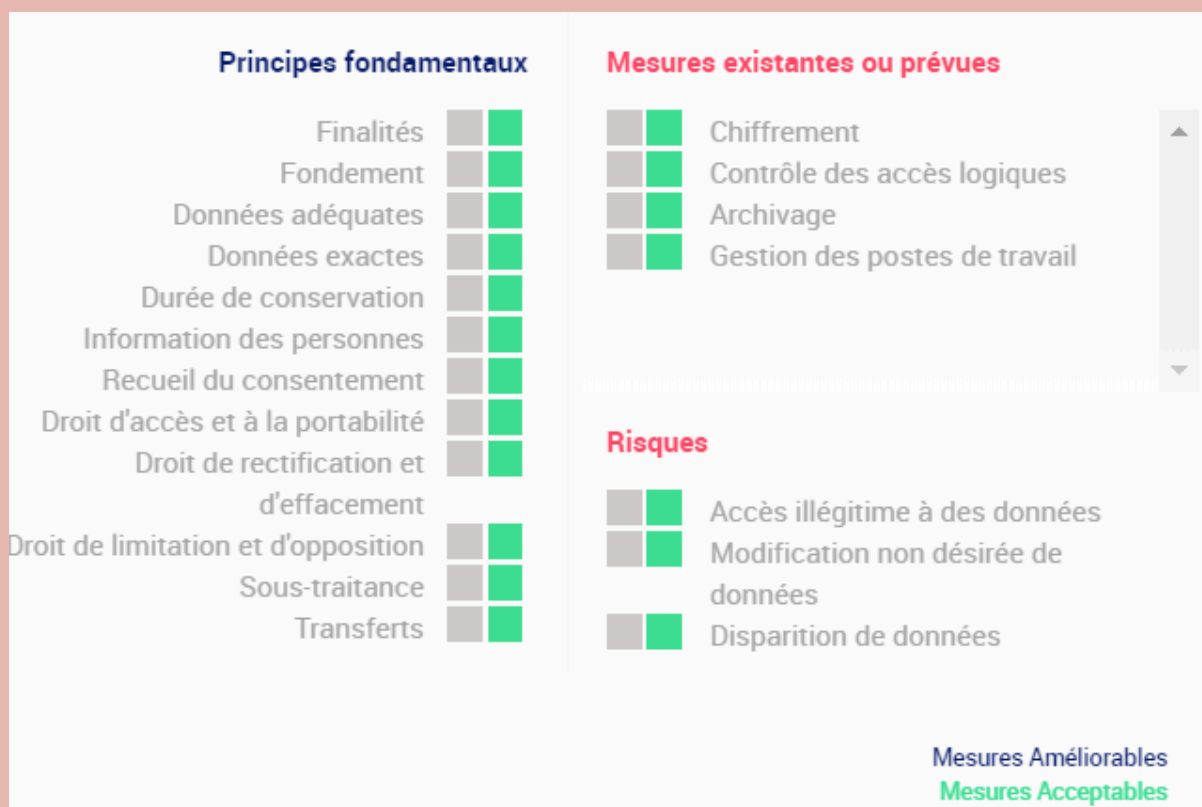


Les mesures déjà existantes sont le chiffrement des données , le contrôle des accès logiques, l'archivage et la gestion des postes de travail.
 Nous remarquons donc que déjà beaucoup de mesures ont été prises pour assurer la sécurité des données.

Accès illégitime à des données : mesures acceptables car beaucoup de moyens ont été mis en place pour la protection des données cependant le risque zéro n'existe pas.

Modification non désirées de données : (idem)

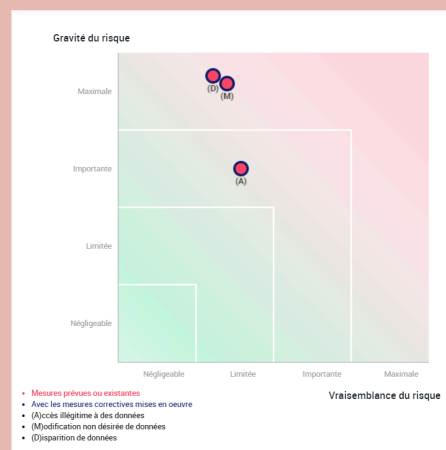
Disparition de données : (idem)



4- Nous pourrions imaginer renforcer la protection des données avec par exemple l'installation d'un VPN, un pare-feu ainsi que des sauvegardes fréquentes des données pour éviter leur perte.

5-

Nous remarquons que pour des risque de gravité maximale à importante la vraisemblance de ceux-ci reste tout de même limité au vu des moyens mis en place pour contrer ceux-ci.



2- Cartographier le traitement des données à caractère personnel

1-

Définition: La cartographie des traitements des données personnelles est une démarche qui consiste à identifier, décrire et visualiser l'ensemble des traitements de données personnelles réalisés au sein d'une organisation.

Enjeux:

- Permet de maîtriser les flux de données
- Aide à évaluer les risques pour la vie privée
- Facilite la mise en conformité du RGPD
- Favorise la transparence

2-

Le registre identifie et décrit les traitements, structure les informations et permet la détection d'incohérences avant de visualiser tout ça sous forme cartographiée.

3- Repérer l'utilisation des données à caractère personnel

1- Les conséquences de la saisie de données personnelles sur un formulaire d'inscription au site castorame.fr sont que les données collectées peuvent être utilisées à des fins stratégiques.

Tout de même avant l'enregistrement, le traitement et l'utilisation des données, le consentement de l'utilisateur doit être demandé.

2-On ne peut pas dire qu'il y a une totale absence de confidentialité mais il y a tout de même de nombreux renseignements présent sur ce formulaire pouvant s'avérer sensibles.

4- Traitements et risques sur les données à caractère personnel

1-

Les différents moyens de collecte, stockage et diffusion des données à caractère personnel sont :

- les questionnaires en ligne
- les enregistrements vocaux ou vidéo
- les jeux concours
- les réseaux sociaux
- les banques
- les applications mobiles
- le centre des impôt

2 -

Les traitements de données à caractère personnel présentés sont :

- la consultation de celles-ci
- la revente
- les échanges
- la gestions du personnel
- les contrôles pour les accès avec badges
- les systèmes de surveillance (internet ou messagerie)

3-

Les obligations légales sont :

- une finalité du traitement définie
- collecte uniquement des données nécessaire au traitement
- collecte de données pertinentes au regard de la finalité du traitement
- suppression des données après que le traitement est été réalisé
- assurer la sécurité et la confidentialité des données

4-

Les sanctions encourues en cas de non-respect de la sécurité des données à caractère personnel sont :


4% du chiffre d'affaire et 2 millions d'euros -> violation des principes

2% du chiffre d'affaire et 10 millions d'euros -> sécurité inadaptée

(+ potentielle peine de prison allant jusqu'à 5 ans

5- Dissocier les notions de sécurité et sûreté informatique


5 Dissocier les notions de sécurité et de sûreté informatique

>  Fiche savoirs technologiques 3

- Retrouvez, dans les scénarios proposés ci-dessous, ceux qui relèvent de la notion de sécurité et ceux qui relèvent de la notion de sûreté. Justifiez.

Scénarios	Sécurité	Sûreté	Justifications
L'ensemble des serveurs est hors-service à cause d'une inondation du local technique	<input type="checkbox"/>	<input checked="" type="checkbox"/>	C'est une cause imprévisible et naturelle
Les données d'un hôpital sont illisibles à la suite d'une attaque de type ransomware.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	C'est une attaque volontaire d'une tierce personne sur le SI
L'apparence du site vitrine d'une entreprise est modifiée pendant un week-end par des personnes malveillantes.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Idem
Une surcharge électrique temporaire due à des travaux réalisés dans les bâtiments de la société provoque une panne des routeurs.	<input type="checkbox"/>	<input checked="" type="checkbox"/>	accident technique et imprévisible

6- Identifier les données à caractère personnel

>  Fiche savoirs CEJMA 1

- Recensez les données qui correspondent à la définition d'une donnée à caractère personnel. Justifiez.

Données	Caractère personnel	Justifications
Le nom de l'enseigne du magasin Carrefour	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	Ce n'est pas une personne physique, c'est une enseigne
L'adresse courriel professionnelle d'un directeur des services informatiques	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	L'adresse permet l'identification d'un individu
Une photo postée sur un réseau social	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	une photo permet l'identification d'un individu
Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre d'un recrutement	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	elle peut contenir l'image et la voix d'un individu
Les coordonnées GPS de localisation d'un smartphone	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	nous savons où se situe la personne
Le groupe sanguin d'un patient stocké sur le serveur de base de données de son médecin	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	cela permet d'identifier un individu grâce à des données médicales
Les enregistrements de vidéosurveillance d'un datacenter	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	la personne étant filmée apparaît clairement sur les vidéos
Le numéro d'enregistrement au registre du commerce et des sociétés d'une entreprise	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	c'est une personne morale et il n'y a donc pas de risque
Le numéro de sécurité sociale d'un salarié saisi sur sa fiche d'embauche	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	c'est un numéro propre à un individu

Conclusion : Ce TP m'a permis d'avoir une idée sur ce que sont vraiment des données à caractère personnel, la multitude de risques mais aussi de solutions qui y sont liées. Cela aide à moins d'honneur sur la protection de celles-ci au risque de lourdes peines