

## TP PIA (Privacy Impact Assessment)

### Contexte

Le contexte de la société « CentreCall » reste valide.

Nous allons continuer la sécurisation des données personnelles dans cette entreprise avec l'outil PIA (Privacy Impact Assessment). C'est un outil qui aide à construire un traitement conforme au RGPD et soucieux de la vie privée. Cette analyse est obligatoire lorsque les traitements sont susceptibles d'engendrer un risque élevé.

Dans notre cas le PIA porte sur le processus d'étude de marché mis en œuvre par CentreCall. Mme Azri est responsable du traitement des données manipulées dans le cadre de ce processus. L'objectif des études de marché est de collecter et d'analyser des informations qui identifient les caractéristiques d'un marché. Les données traitées sont ensuite mises à disposition des différents clients

### Sommaire

1.)	Scénarios : .....	2
2.)	Vraisemblances et gravités : .....	3
3.)	Matrice des risques : .....	4
4.)	Synthèse et plan d'actions : .....	5
5.)	PIA (Privacy Impact Assessment) : .....	6

## 1.) Scénarios :

Lister des scénarios d'attaques / risques qui peuvent impacter directement ou indirectement les données personnelles. Rajouter un commentaire concernant la complexité de l'attaque et son impact éventuel.

**Scénario #1** : Suppression ou vol de données dans la base de données par un salarié mécontent, dans l'objectif de nuire à CentreCall, voire de les communiquer à un concurrent.

**Commentaire** : action facile à mener car les salariés ont accès à la BDD (hypothèse) avec de lourdes conséquences.

**Scénario #2** : Un hacker attaque les données personnelles par rançongiciel et demande une rançon à CentreCall en échange de donner la solution pour déchiffrer les données qu'il a chiffré.

**Commentaire** : La possibilité qu'un hacker s'en prenne aux données personnelles dans le but d'une rançon est rare mais serait très embêtant pour la société.

**Scénario #3** : Un employé de CentreCall qui a accès à la base de données, est victime d'une attaque par Phishing. De ce fait l'hacker possède lui aussi accès à la base de données

**Commentaire** : Le Phishing est une attaque tendance du moment, elle énormément utilisée. Par la suite l'hacker peut simplement s'abotter les données, les rendre publique ou bien les prendre en rançon. Dans tout les cas l'intrusion d'un Hacker dans la base de données est très problématique.

**Scénario #4** : Une personne créer un site internet identique et se fait passer pour l'entreprise CentreCall dans le but de récupérer des données personnelles.

**Commentaire** : On pourrait alors avoir des personnes qui sont enregistrer dans notre base de données et aussi dans la base de données du site internet usurpateur, donc à la porté de la personne malveillante.

**Scénario #5 :** Un employé qui utilise un ordinateur de CentreCall connecté au réseau ouvre un fichier vérolé par malware qui se propage jusqu'à la base de données personnelles et la met hors service.

**Commentaire :** Cet incident rendrait la base de données personnelles inutilisable le temps de supprimer le virus et de remettre la base de données en services. Ce qui peut poser problème dans plusieurs situations comme par exemple : Si un client demande des informations sur ses données personnelle, CentreCall à le devoir de lui fournir etc....

## 2.) Vraisemblances et gravités :

Source de la menace	Type de menace	Vraisemblance	Gravité	Commentaire
Scénario #1 : Employé interne	Sabotage	1	4	L'objectif est de nuire à CentreCall
Scénario #2 : Attaquant externe	Cybercriminalité	1	4	L'objectif pour l'attaquant est de demander une rançon
Scénario #3 : Attaquant par le biais d'un employé interne	Sabotage Ou Cybercriminalité	3	4	L'objectif de cette attaque peut varier selon l'attaquant
Scénario #4 : Attaquant externe	Usurpation de l'entreprise	1	3	L'objectif pour l'attaquant est de créer un faux site internet pour récupérer des données
Scénario #5 : Virus externe ouvert par le biais d'un employé interne	Sabotage	2	3	L'objectif pour l'attaquant qui à crée le virus est qu'il se propage le plus possible pour saboter un maximum de service

3.) Matrice des risques :

Impact Maximum	Scénario #2	3	3	3	3	Scénario #3	3
	Scénario #4	Scénario #1	3	3	3	3	3
	2	2	2	2	Scénario #5	3	3
	2	2	2	2	2	3	3
	1	1	2	2	2	3	3
	1	1	2	2	2	3	3
0	Probabilités Maximum						

#### 4.) Synthèse et plan d'actions :

Afin de réduire au minimum les risques évoqués précédemment avec le tableau et la matrice des risques. Je vous propose un plan d'action qui est le suivant :

Dans un premier temps il faudrait limiter l'accès aux données en interne. C'est-à-dire que les employés peuvent enregistrer des données dans le cas de leur travail dans une étude de marché. Mais sont limités à cela et ne peuvent en aucun cas ni les saboter où ni les voler, cette action est possible par l'intégration d'une hiérarchie de droit sur la base de données.

Une fois la menace interne réduite par cette première action il faudrait faire une grosse campagne de prévention sur les attaques phishing afin de réduire encore plus la menace interne. Car la prévention reste la meilleure défense sur ce type de menace très courante. Une fausse attaque phishing peut être utilisé pour renforcer la prévention sur ce type de menace, afin de vérifier si la prévention a été efficace.

Par la suite il faudrait renforcer la sécurité des attaques externes, il faut veiller à ce que tous les ordinateurs soient systématiques mis à jour notamment au niveau du par feu et de l'antivirus. On pourrait aussi envisager de copier et migrer toutes les données sur un cloud, ce qui permettrait en cas d'attaques externes d'avoir une réponse rapide le temps d'exterminer la menace. Ne pas avoir tous les œufs dans le même panier est une solution couteuse mais efficace.



## 5.) PIA (Privacy Impact Assessment) :

Mettre au propre les éléments du TP en utilisant le logiciel « PIA » de la CNIL et en complétant lorsque cela est nécessaire. Enregistrer les différents documents générés par l'outil.

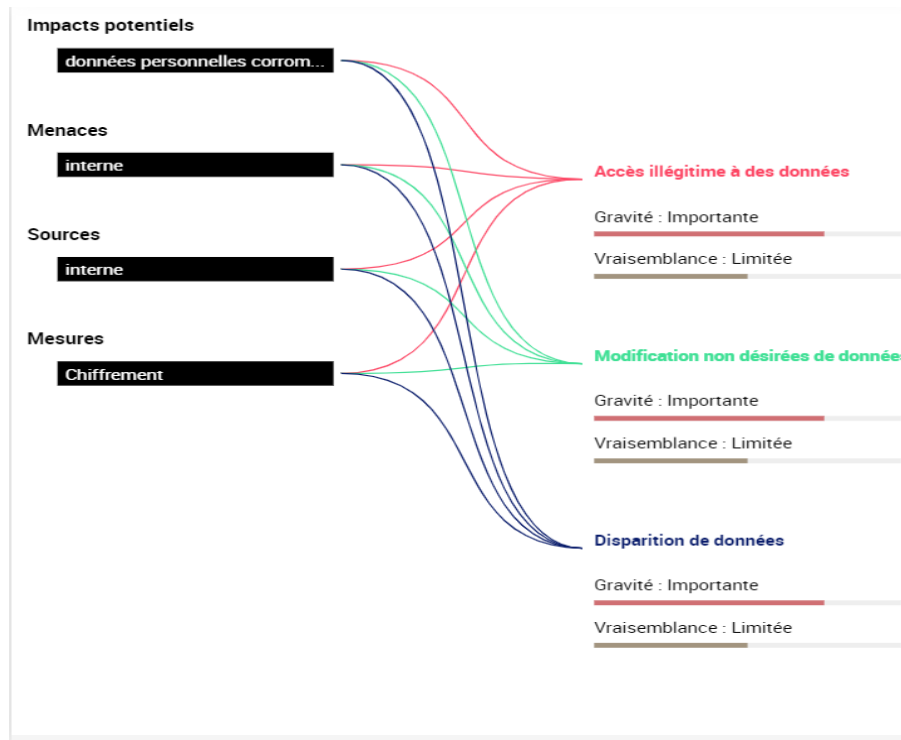


Après avoir compléter les catégories « Contexte, Principe Fondamentaux, Risque », en suivant les éléments du TP et en rajoutant par moment mes propres analyses. Le logiciel PIA ma permis de générer les éléments suivants :

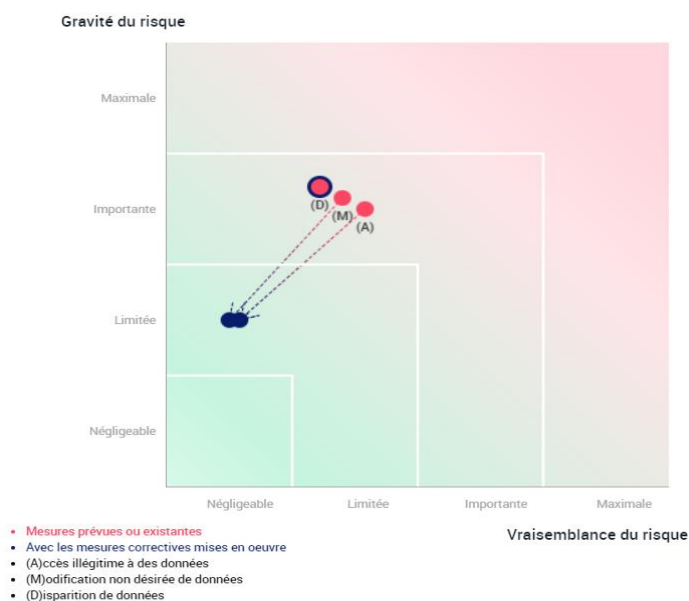
- \*Une vue d'ensemble des risques
- \*Une cartographie des risques
- \*Un plan d'action



## Vue d'ensemble des risques :



## Cartographie des risques :



























01/11/2022

## Plan d'action :

### Vue d'ensemble







#### Principes fondamentaux

Finalités		
Fondement		
Données adéquates		
Données exactes		
Durée de conservation		
Information des personnes		
Recueil du consentement		
Droit d'accès et à la portabilité		
Droit de rectification et d'effacement		
Droit de limitation et d'opposition		
Sous-traitance		
Transferts		

#### Mesures existantes ou prévues

		Chiffrement
		Archivage
		Minimisation des données
		Sauvegarde des données
		Journalisation

#### Risques

		Accès illégitime à des données
		Modification non désirée de données
		Disparition de données

Mesures Améliorables  
Mesures Acceptables