

B3 TP Compte Rendu
Cyb Thème 1

Sommaire :

PIA

**Cartographier le traitement de données à caractères
personnelles.**

**Répertorier l'utilisation des données à caractère
personnel**



**Traitements et risques sur les données à caractère
personnel**

Dissocier notions sécurité et sûreté informatique

Identifier données à caractères personnel

PIA

1)



Nom du modèle
Exemple : PIAF Objets connectés

Secteur associé
IoT

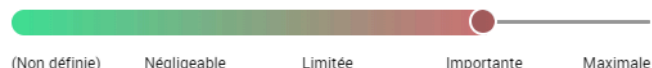
Date
21/11/2018

[Consulter le modèle](#)

2) Accès illégitime à des données, Modification non désirées de données, disparition de données

3) Accès illégitime aux données Gravité: Importante Vraisemblable: Maximale

Comment estimez-vous la **gravité du risque**, notamment en fonction des impacts potentiels et des mesures prévues ?



En cas de divulgation de leurs données, les personnes concernées pourraient connaître des **conséquences significatives**, qu'elles devraient pouvoir **surmonter**, mais avec **des difficultés réelles et significatives** (perte d'opportunités ciblées, sentiment d'atteinte à la vie privée, etc.).

0 commentaire(s)

21/02/2018

Commenter

Comment estimez-vous la **vraisemblance du risque**, notamment au regard des menaces, des sources de risques et des mesures prévues ?



Il semble **extrêmement facile** pour un employé, une personne de l'entourage de l'utilisateur ou un éventuel attaquant **d'avoir accès aux données**.

0 commentaire(s)

21/02/2018

Commenter

Disparition de données: Gravité: Maximale Vraisemblable: Important

Comment estimez-vous la **gravité du risque**, notamment en fonction des impacts potentiels et des mesures prévues ?



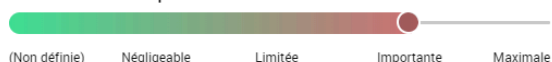
Les personnes concernées pourraient connaître des **désagréments significatifs**, qu'elles pourront **surmonter malgré quelques difficultés** (indisponibilité temporaire du service, problème de réveil, etc.).

0 commentaire(s)

21/02/2018

Commenter

Comment estimez-vous la **vraisemblance du risque**, notamment au regard des menaces, des sources de risques et des mesures prévues ?



Il semble **peu probable** que les données soient durablement indisponibles, au vu de la **politique de sécurité de l'hébergeur BETA**.

Modif données : Gravité : Important Vraisemblable: Important

Comment estimez-vous la **gravité du risque**, notamment en fonction des impacts potentiels et des mesures prévues ? ^



(Non définie) Négligeable Limitée Importante Maximale

Les personnes concernées pourraient connaître des **désagréments significatifs**, qu'elles pourront surmonter malgré quelques difficultés (nécessité de refaire certains réglages, erreur dans les heures de réveil programmées, etc.).

0 commentaire(s)

21/02/2018

Commenter v

Comment estimez-vous la **vraisemblance du risque**, notamment au regard des menaces, des sources de risques et des mesures prévues ? ^



(Non définie) Négligeable Limitée Importante Maximale

Au vu du niveau de protection, il **semble difficile**, qu'un employé, un membre de l'entourage de l'utilisateur ou un attaquant parvienne à **modifier les données d'un compte utilisateur**.

Gravité du risque

21/02/2018

Maximale

Importante

Limitée

(M)

(A)

(D)

5)

Le point M correspond aux risques de modification non désirés de données, le point A aux accès illégitimes à des données et le point D aux disparition de données. On voit donc que les risques sont importants pour le point A et M. Le point D lui est limité. Donc la sécurité est assez encadré mais des améliorations peuvent être poursuivies pour le point A et M.

Cartographier le traitement de données à caractères personnelles.

1)

Partout dans les entreprises il y a des données à caractère personnel.

L'objectif est de définir où se trouvent les données et où sont les risques. Un DPO (pour les Grandes entreprises) ou bien une à plusieurs personnes peuvent être engagés sur le traitement de données à caractère personnel. Cela aide à identifier les données personnelles au sein de l'entreprise et leur circulation, pour cela il est important de lister les données, quels traitements (pourquoi elles sont utilisées), le flux des données. Le PIA permet de voir la mesure des fuites de données et quels sont les risques pour les personnes (ex: prospect) et de gérer les moyens à mettre en place (ex: accès à empreinte digitale au sein d'une entreprise) .

2)

Cette étape permet de répertorier les caractéristiques appliquées au sein des données et savoir où peuvent intervenir les risques. Cela permet également de savoir les positions susceptible de contenir des données personnelles, de savoir qui y a accès.

Répertorier l'utilisation des données à caractère personnel

1)

Castorama partage les données personnelles des clients avec kingfisher qui peut les utiliser à des fins marketing et de référencement(ex: sites web, services numériques) tout en ciblant des produits/services susceptibles de nous intéresser au vue de nos achats chez Conforama. L'entreprise Castorama partagent également des données avec des tiers ou avec leur(s) assureur(s) de façon anonyme ou agrégées selon certains cas (ex: en cas d'action intentée contre l'entreprise).

2)

La seule lecture est susceptible de nous laisser penser que la confidentialité n'est pas assurée car les données circulent entre plusieurs tiers ce qui multiplie les risques. Cependant nous ne

connaissons pas les moyens employés par Conforama et leurs tiers pour protéger ces données à caractère personnel.

Traitements et risques sur les données à caractère personnel

1)

La collecte de données à lieu par des formats papier ou informatiques par exemple des questionnaire, des vidéos ou vocaux, des jeux concours, les réseaux sociaux, des applications mobiles, les banques et centre

2)

Les données sont d'abord stockés dans une base données pour les adhérent sous forme de fichier clients, elles peuvent être consulté et communiquer par email/ téléphone puis revendues ou échangées.

3)

Les employeurs peuvent traiter les données pour la gestion du personnel par exemple les

contrôles d' accès par badges ou contrôles de messagerie par responsable conformément par le cadre des obligations juridiques des protections des données collectées. Les données doivent être nécessaires et pertinentes au regard des finalités puis elles doivent être supprimées. Son rôle est d'assurer la sécu et la confidentialité(ex: vérifier les personnes autorisées à voir des données)

4)

En cas de violation des principes un montant de 4% des Chiffres D'affaires à 20 Millions d'euros ou 2% des Chiffres D'affaires et 10 Millions d'euros, des peines d'emprisonnement peuvent être accorder(~5 ans)

Dissocier notions sécurité et sûreté informatique

Tableau :

5 Dissocier les notions

► 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 l'entreprise qui doit s'assurer de la sauvegarde de ses données car une attaque malveillante
Les données d'un hôpital sont illisibles à la suite d'une attaque de type ransomware.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	personne Malveillante
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"/>	Erreur techniques
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"/>	

Identifier données à caractères personnel

Tableau :

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	Pas de représentant à proprement parler.
L'adresse courriel professionnelle d'un directeur des services informatiques	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	propre à 1 personne
Une photo postée sur un réseau social	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	Paysage → pas personnel
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	personnelles
Les coordonnées GPS de localisation d'un smartphone	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	données personnelles
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	/ /
Les enregistrements de vidéosurveillance d'un datacenter	<input type="checkbox"/> oui <input checked="" type="checkbox"/> non	Sécurité aux données personnelle
Le numéro d'enregistrement au registre du commerce et des sociétés d'une entreprise	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	caractère perso de l'entreprise
Le numéro de sécurité sociale d'un salarié saisi sur sa fiche d'embauche	<input checked="" type="checkbox"/> oui <input type="checkbox"/> non	données perso.