Thème 1 Partage des données a caractère personnel

Chapitre 1 : Identifier les risques liés aux données à caractère personnel

DSI

DM

DG

AMOA : Assistance maitrise d’ouvrage

DSI : Direction des systèmes informatiques

DG : Directeur Général

DM : Direction métier

--------------------------------------------------------------------------------------------------------------------------------------

MOA : maitrise d’ouvrage

Cahier des charges

MOE : maitrise d’œuvre

6 janvier 1978 : création du CNIL

* ***Identifier les risques liés aux données à caractère personnel :***

4 ***fonctions***du SI : (Système d’information)

* Collecte
* Traitement
* Stockage
* Diffusion

Organisationnelle, Finance, Humaine 🡪 COMPOSANT

Système d’information :

* Donnée : 25
* Information : °C
* Connaissance : Prévision météo

Mission 1 :

Question :

1. Comme donnée recueillis nous avons :

* Nom
* Prénom
* Adresse compète (rue, code postal, ville et département)
* Courriel

La CNIL définit une donnée à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable ».

Au regard de cette définition, parmi les données recueillies lors de la réalisation d’une étude de marché (document 1), celles à caractère personnel sont : le nom, le prénom l’adresse complète et l’adresse courriel de la personne interrogée.

1. Analysez la conformité de la situation décrite ci-dessus avec des directives de CNIL

CentreCall répond seulement aux points mentionner dans l’article de la CNIL :

* L’objectif de l’enregistrement de la conversation est précisé
* Des destinataires des écoutes ou enregistrements
* Qui sont les destinataires des écoutes ou enregistrements

Par contre les obligations suivantes ne sont pas respectées envers les personnes interrogées :

* L’information sur les droits d’auteurs

1. Schéma évènement résultat, modèle rationnelle

Prospect : c’est un futur client

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Description de l’opération | Référence | Finalité de l’opération | Catégories de données personnelles concernées | Catégories de personnes concernés | Destinataires |
| Enregistrement d’un appel téléphonique | OP-01 | Preuve d’appel | Vie personnel | Prospect | Client et service interne de CentreCall |
| Demande d’enregistrement de l’appel | OP-02 | Sauvegarde des données | Donnée personnel | Prospect | Osiris |
| Vérification de l’enregistrement de l’entretien | OP-03 | Vérification | identiter | Prospect | Client et service interne de centrecall |
| Traitement des données | OP-04 | Vérification | Donnée personnel | Prospect | Centre call |

1. Repérez les difficultés rencontrées avec la nouvelle application. Précisez en quoi elles contribuent à affaiblir la protection des données à caractère personnel :

La plateforme des centres d’appel sont désormais capables de gérer les demandes  
en provenance de plusieurs canaux (site internet, courriel, sms, appel vidéo, etc.).

La variété des technologies et des supports de collecte de données implique des protocoles réseau et des formats de fichier différents (xml, Json, csv, pdf, etc...) qui nécessitent différents traitements.

Le multicanal influence donc le traitement des données à caractère personnel pour les centres d’appel comme CentreCall.

Solutions tickets 1 :

Une inversion de date est constatée suite à l’utilisation de formats de données différents.  
C’est l’intégrité de la donnée qui est en jeu.

Les formats doivent être uniformisés pour toutes les données de type « date » quel que soit  
le canal utilisé pour collecter les données.

Solution tickets 2 :

Certaines données doivent être saisies par un opérateur, c’est le cas pour les données émanant des entretiens téléphoniques. Cette saisie peut entraîner des erreurs et toucher à l’intégrité  
des données.

* ***Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractère personnel***

Mission 2

1. L’intérêt d’une potentielle attaque réside dans la nature même des données collectées et dans la finalité de traitement de ces dernières.

Pour CentreCall, certaines données sont à caractère personnel.

Le cycle de vie des données lié au traitement (document 2) décrit les différentes opérations réalisées et permet d’identifier celles plus ou moins vulnérables à une attaque.

La collecte des réponses chez CentreCall peut engendrer des vulnérabilités sur les données à caractère personnel (enregistrement audio et sauvegarde par un opérateur des données collectées).

La liste des supports des données mobilisés lors du processus (document 2) permet de reconnaître le plus vulnérable à une attaque.

La communication via le téléphone IP peut être écoutée. L’ordinateur de bureau utilisé par l’opérateur peut subir une panne ou être la cible d’une attaque.

Une image contenant table

Description générée automatiquement

Une image contenant table

Description générée automatiquement

Une image contenant table

Description générée automatiquement