|  |
| --- |
| Contexte 1 – Protéger les données à caractère personnel  Chap1 : Identifier les risques liés aux données à caractère personnel |

Table des matières

[Qu’est-ce qu’un risque ? 2](#_Toc84336437)

[Mission 1 – Recenser les traitements sur les données à caractères personnelles. *(Page 12)* 2](#_Toc84336438)

[Q1 - 2](#_Toc84336439)

[Q2 2](#_Toc84336440)

[Q3 2](#_Toc84336441)

[Q4 2](#_Toc84336442)

[Mission 2 – Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractères personnel *(Page 16).* 3](#_Toc84336443)

[Q1 3](#_Toc84336444)

[Q2 3](#_Toc84336445)

[Q3 4](#_Toc84336446)

[Q4 4](#_Toc84336447)

[Q5 5](#_Toc84336448)

# Qu’est-ce qu’un risque ?

Risque : probabilité de l’exploitation d’une vulnérabilité du SI par une menace.

# Mission 1 – Recenser les traitements sur les données à caractères personnelles. *(Page 12)*

Q1 - Données personnelles : Selon la CNIL, une donnée personnelle est une « information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement. »

Au regard ce cette définition, les données à caractères personnelles recueillis lors de la réalisation d’une étude de marché sont le nom, le prénom, l’adresse complète, le courriel car ces données permettent d’identifier directement (nom, prénom, courriel) la personne physique ou indirectement (adresse complète).

Q2 - Selon la CNIL, chaque interlocuteur doit être informé de la finalité de l’appel, du destinataire des écoutes ou des enregistrements, de son droit d’opposition et de son droit d’accès aux enregistrements.

Au regard des directives de la CNIL, on peut dire que la situation décrite n’est pas conforme à ces directives, car malgré la demande de l’enregistrement et l’information du droit d’opposition, ils ne précisent pas le droit d’accès aux enregistrements, ni même les destinataires de l’enregistrement.

Q3 -

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Description de l’opération** | **Référence** | **Finalité de l’opération** | **Catégories des données personnelles concernées** | **Catégorie de personnes concernés** | **Destinataires** |
| Enregistrement d’un appel téléphonique | OP-01 | Preuve de l’appel | Vie personnelles | Prospect | Client et services internes de CentreCall |
| Collecte des réponses aux questionnaires | OP-02 | Sauvegarde des données | Données personnelles | Prospect | Osiris |
| Vérification de l’enregistrement de l’entretien | OP-03 | Vérification des réponses collectées | Vie perso | Prospect | Osiris |
| Traitement des données | OP-04 | Synthèse étude de marché | Vie perso | Prospect | Osiris |

Q4 - Les plateformes 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.

Solution Ticket 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 ticket 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.

# Mission 2 – Identifier les risques liés à la collecte, au traitement, au stockage et à la diffusion des données à caractères personnel *(Page 16).*

Q1 - 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.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Source de menace | Type de menace | Bien support | Niveau de vraisemblance | Confidentialité | Disponibilité | Intégrité |
| Scénario 1 : Attaquant extérieur | Espionnage | Ordi Opérateur | 2 | Authentification plus assurée aux seuls personnes habilités |  |  |
| Scénario 2 :  Attaque interne : salariés | Vol de données | Ordi | 4 |  | Données plus disponibles après suppression |  |
| Scénario 3 : employé non-habilité | Consultation de donnée | Ordinateur de l’employé | 2 | Les données sont accecible à des personnes non habilités |  |  |
| Scénario 4 : attaquant exterieur | Déstabilisation | Ordinateur extérieur | 3 |  |  | Les données sont altérées |
| Scénario 5 : attaquant extérieur | Arrêt des serveurs de la BDD | Ordi extérieur | 4 |  | Données plus accecible pour les opérateurs |  |

Q2 -

|  |  |  |
| --- | --- | --- |
| Scénario | Evènement redoutés | Niveau de gravité |
| Exemple : scénario 1 | Usurpation d’identité | Niveau de gravité : **3** (important).  Les données confidentielles peuvent être exploitée par une entité malveillante. |
| Exemple : scénario 2 | Vol de données | Niveau de gravité : **3** (important).  Certaines données ne seront plus accecible |
| Exemple : scénario 3 | Consultation de données | Niveau de gravite :**2** (limité).  La consultation se limite à un périmètre restreint. |
| Exemple : scénario 4 | Altération de données | Niveau de gravité : **3** (important).  La modification altère le résultat de l’étude de marché. |
| Exemple : scénario 5 | Attaque DDOS | Niveau de gravité : **4** (important).  Plus aucune donnée n’est accecible |

Q3 -

Q4 -

Gravité

Risque Inacceptable

Tolérable sous contrôle

Risque Acceptable

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Risque 5 |
|  | Risque 1 | Risque 4 | Risque 2 |
|  | Risque 3 |  |  |
|  |  |  |  |

Vraisemblance

|  |  |  |  |
| --- | --- | --- | --- |
| Risque | Vraisemblance | Gravité |  |
| 1 | 2 | 3 |  |
| 2 | 4 | 3 |  |
| 3 | 2 | 2 |  |
| 4 | 3 | 3 |  |
| 5 | 4 | 4 |  |

Q5 – Nous avons décelé 5 types de menaces que nous pouvions résoudre selon leur gravité et leurs vraisemblances. En premier, l’espionnage en usurpant un compte d’identification est peu probable mais cela implique un niveau de gravité important car l’authentification n’est plus assurée aux seules personnes habilitées, nous avons donc songer à renforcer d’avantage la sécurité des ordinateurs lors des maintenances. Ensuite, la suppression ou le vol de données que ce soit par le fait d’un attaquant extérieur ou d’un employé non habilité possède un niveau de gravité et de vraisemblance important, celui-ci doit donc être traité au plus vite, car les données supprimées ne sont plus disponibles et celles volées peuvent être exploités par une entité concurrente ou malveillante. Pour limiter ce risque, uniquement les personnes habilitées peuvent avoir accès aux bases de données et des sauvegardes doivent être effectuer régulièrement, cela éviterait qu’il y ait des erreurs de manipulations. Enfin, un autre cas de figure est envisagé, un DDOS du serveur de la base de données, c’est-à-dire un envoi constant de requête sur notre serveur par un attaquant extérieur afin que celui-ci plante. Ce risque a une gravité et une vraisemblance maximale, celui-ci doit être régler impérativement.

DDOS : Les attaques par déni de service distribué (Distributed Denial of Service ou DDoS) constituent une menace pour toute organisation disposant d’un système d’information connecté à internet. Ce guide présente les solutions existantes permettant d’anticiper cette menace, et de faire face à une attaque DDoS.

Correction Q5 :

Mme AZRI,

Cinq risques ont été identifiés (voir document 4) avec des particularités propres à chacun.

Les **sources de menace** identifiées sont des attaques de personnes malveillantes situées  
à l’intérieur (salarié) ou à l’extérieur de notre société.

Les **types de menaces** sont l’espionnage au profit de concurrents ou la recherche  
de déstabilisation de notre processus d’étude de marché. Il est à noter une menace non intentionnelle correspondante à une erreur de manipulation d’un salarié.

Pour chaque menace, vous trouverez une **évaluation de sa vraisemblance**. Il semble  
que la récupération de données à caractère personnel suite au départ d’un salarié mécontent soit la menace la plus vraisemblable.

Une liste des événements redoutés permet de **mesurer leur niveau de gravité** suivant leurs impacts prévisibles sur les données à caractère personnel. Ainsi, l’arrêt du serveur de base  
de données apparaît comme l’événement redouté dont l’impact serait le plus préoccupant.

Une hiérarchisation nous permet d’identifier les **risques majeurs** suivants à surveiller :

* **Risque 2 :** suppression de données dans la base de données de CentreCall par un salarié mécontent dans l’objectif de les communiquer à un concurrent.
* **Risque 4 :** altération de données sur le serveur de base de données par un attaquant extérieur à l’organisation afin de déstabiliser les campagnes d’études de marché  
  de CentreCall.
* **Risque 5 :** arrêt du serveur de base de données par une attaque extérieure en réalisant une multitude de requêtes.

Le risque 2 correspond à une **impossibilité de garantir la confidentialité** des données,  
il peut être enrayé par une politique des mots de passe plus rigoureuse.

Le risque 4 peut mettre à mal l’**intégrité des données** stockées. Un pare-feu peut être  
une solution envisageable pour limiter les attaques extérieures.