BTS SIO 1ere année

Cours de cybersécurité

2021/2022

# 4 axes

## 1 Protéger les données à caractère personnel

## 2 Préserver l’identité numérique de l’organisation

## 3 Sécuriser les équipements et les usages utilisateurs

## 4 Garantir la disponibilité, l’intégrité et la confidentialité des services informatiques et des données de l’organisation face à des cyberattaques

# 1 PROTEGER LES DONNEES A CARACTERE PERSONNEL

## Chapitre 1 Identifier les risques liés aux données soumises à caractère personnel

### Données à caractère personnel

Une donnée personnelle est une information qui se rapporte à une personne physique identifiée ou identifiable. Ces personnes doivent en conserver la maîtrise.

Une personne physique peut être identifiée soit :

* Directement (exemple : nom et prénom) ;
* Indirectement (exemple : par un numéro de téléphone ou de plaque d’immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l’image).

L’identification d’une personne physique peut être réalisée à partir d’une seule donnée (exemple : nom) ou à partir du croisement d’un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association).

Par contre, des coordonnées d’entreprises (par exemple, l’entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.

**Source : CNIL**

<https://www.cnil.fr/fr/definition/donnee-personnelle>

### DPO

Le délégué à la protection des données (DPO) est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l’organisme qui l’a désigné s’agissant de l’ensemble des traitements mis en œuvre par cet organisme.

Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions. Pour garantir l’effectivité de ses missions, le délégué doit disposer de qualités professionnelles et de connaissances spécifiques et doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement adéquats.

**Source : CNIL**

### Le traitement des données à caractère personnel

Un traitement de données personnelles est une opération, ou ensemble d’opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).Un traitement de données personnelles n’est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation. Si les enfants des salariés et leur âge figurent dans la base de données, un usage doit en être fait (par exemple cadeau de Noël)

Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.

Chaque traitement de donnée doit avoir une finalité déterminée.

**Source : CNIL**

### Vulnérabilité, menace et risque

Il convient de distinguer trois termes :

La vulnérabilité informatique est une faiblesse de la sécurité du système d’information qui peut affecter son fonctionnement normal.

La menace est une cause intentionnelle ou non intentionnelle qui peut entrainer des dommages sur le SI.

Le risque de sécurité du SI est la probabilité de l’exploitation d’une vulnérabilité par une menace. Les objectifs de la sécurité informatique consistent à limiter les vulnérabilités du SI.

**Source : CNIL**

### Conversations téléphoniques

Comment informer les clients à propos des enregistrements de conversations téléphoniques ?

Chaque interlocuteur doit être informé au moment de l’appel :

* De l’objectif de l’opération
* Des destinataires des écoutes ou enregistrements
* De son droit d’opposition
* De son droit d’accès aux enregistrements

Cette information peut être réalisée par la diffusion d’un message en début d’appel ou par une mention particulière dans les contrats ou documents d’information.

**Source : CNIL**

# 2 La typologie des risques informatiques

Il existe maintenant de nouvelles méthodes, qui sont recommandées pour les entreprises pour la sécurité informatique.

Comme en qualité, avec la sortie de l’ISO 9000, puis les suivants, il existe maintenant des référentiels concernant la sécurité informatique, et les entreprises vont devoir les suivre.

Vous pouvez être amené à y contribuer.

## Différence entre sûreté et sécurité

### La sécurité

La sécurité informatique concerne la protection des données. Il s’agit d’avoir une authentification forte (login, mot de passe). On évite que les personnes non autorisées aient accès à des données sensibles et puissent les utiliser.

### La sûreté

La sûreté informatique, c’est s’assurer que le logiciel va s’exécuter de la manière dont il a été programmé, et avec un minimum de bugs. Concernant les données, on s’assure que les manipulations involontaires ou les erreurs n’engendrent pas de dégâts dans les données.

## La méthode EBIOS

C’est une méthode en 5 points ou ateliers.

Données à consulter et à télécharger :

<https://www.ssi.gouv.fr/administration/guide/la-methode-ebios-risk-manager-le-guide/>

