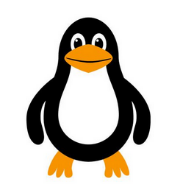
**CEJMA : les données à caractère personnel (B 3.1)**



Toute entreprise ou organisation (comme le lycée) collecte des données à caratère personnel (**DCP)** or les entreprises **ont l’obligation légale de protéger les DCP**, le non-respect de cette obligation serait une faute sanctionnée

**Compétences** : **Appliquer la réglementation en matière de collecte, de traitement et de conservation des données à caractère personnel**

A partir des resssources jointes et de vos recherches, répondez aux questions suivantes :

**Mission 1  : comprendre ce qu’est une donnée à caractère personnel**

**Document 1 : les DCP**



**Source : CNIL :** [**https://www.cnil.fr/fr/definition/donnee-personnelle**](https://www.cnil.fr/fr/definition/donnee-personnelle)

1. **A la lecture de cette définition, recensez quelques données à caractère personnel que vous avez transmises au lycée**

identité, contact, adresse.

1. **Consultez ce lien :** [**https://www.cnil.fr/cnil-direct/question/492?visiteur=pro**](https://www.cnil.fr/cnil-direct/question/492?visiteur=pro) **, à partir de quand une donnée peut-elle devenir anonyme. Est-ce facile ?**

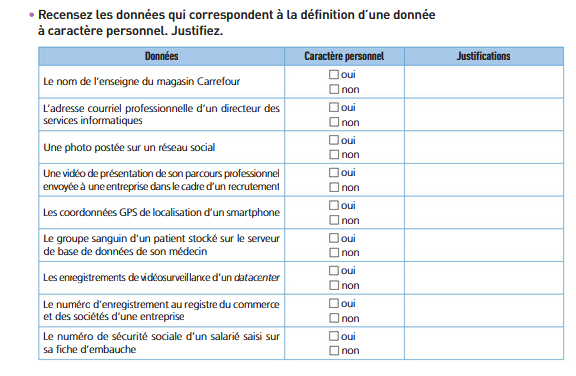
Pas facile car on peut toujours identifier quelqu’un en recoupant des informations.

1. **Consultez ce lien :** [**https://www.cnil.fr/cnil-direct/question/495?visiteur=pro**](https://www.cnil.fr/cnil-direct/question/495?visiteur=pro)

**Parmi les DCP, certaines sont dites sensibles, donnez des exemples de données sensibles**

Ethnie/race, biométrie, santé, sexualité, opinion politique, religion, philosophique, syndicalisme,...

1. **Précisez si le lycée peut recueillir des données sensibles. Justifiez votre réponse**



Uniquement si la personne y a consenti, si ces données sont nécessaires dans un but médical, et si leur utilisation est justifiée par l’intérêt public et autorisé par la CNIL.

1. **Les coordonnées, le nom …du lycée sont-elles des données à caractère personnel ?**

Non, car le lycée n’est pas une entité individuelle et de notoriété publique (personne morale).

|  |  |  |
| --- | --- | --- |
| Le nom de l’enseigne du magasin Carrefour | Caractère personnel | Justifications |
| Le nom de l’enseigne du magasin Carrefour | non | Personne morale et non physique |
| L’adresse courriel professionnelle d’un directeur des services informatiques | non | Donnée professionnelle, pas personnelle. |
| Une photo postée publiquement sur un réseau social | non | Publication volontaire |
| Une vidéo de présentation de son parcours professionnel envoyée à une entreprise dans le cadre du recrutement | oui | Informations personnelles contenues dans la vidéo |
| Les coordonnées GPS de localisation d’un smartphone | oui | Localisation de l’individu ou de sa propriété |
| Le groupe sanguin d’un patient stocké sur le serveur base de données de son médecin | oui | Données médicales |
| Les enregistrements de vidéo surveillance d’un datacentre | oui | Permet d’identifier les personnes |
| Le numéro d’enregistrement au registre du commerce et des sociétés d’une entreprise | non | Personne morale |
| Le numéro de Sécurité Sociale d’un salarié saisi sur sa fiche d’embauche | oui | Donnée permettant d’identifier le salarié |

**Application**

**Mission 2: le RGPD : le règlement général sur la protection des données**

**Vidéo 1 : le RGPD expliqué par Cookie connecté :** [**https://www.youtube.com/watch?v=u4M5lVYv3UI**](https://www.youtube.com/watch?v=u4M5lVYv3UI)



**à partir de cette vidéo, répondez aux questions suivantes :**

1. **Qu’est ce que le RGPD**

Règlement Général de Protection des Données, appliqué à tous les organismes au sein de l’Union Européenne et/ou qui traitent les données de citoyens de l’Union Européenne.

1. **Que prévoit le RGPD ? A qui s’applique-t-il ? Quels sont ses objectifs ? Les entreprises chinoises ou américaines doivent-elles respecter le RGPD ?**

Le RGPD prévoit le respect de la confidentialité des données des citoyens de l’Union Européenne et leur sécurisation. Il s’applique à toute entreprise, association, administration publique du monde traitant les données de citoyens de l’Union Européenne, et aux entreprises européennes, même si celles-ci traitent les données de citoyens étrangers à l’Union Européenne.

1. **Repérez les grands principes du RGPD et expliquez les**

* Accountability : L’entreprise doit pouvoir démontrer administrativement qu’elle respecte le RGPD.
* Privacy by design : Le respect de la confidentialité des données est inclus dans la conception de l’application.
* DPO : Délégué à la Protection des Données, veille au respect du RGPD. Nécessite des compétences, ce qui fait que des entreprises font appel à des agents externes.
* Security by default : La sécurité est incluse dans la conception de l’application, et le système d’information de l’entreprise est sécurisé à tous les niveaux, du logique au physique.
* Etude d’impact : analyse d’impact d’atteintes potentielles à la protection des données dès la mise en œuvre de nouveaux traitements des données. Débouche sur des mesures pour diminuer l’impact des dommages.

1. **Quelles sanctions prévoit le RGPD ?**

Amendes (4% du chiffre d’affaire ou vingt millions d’euros), réparation,...

1. **Qu’est-ce qu’un traitement des données ? Que doit avoir tout traitement de données ?**

Un traitement de données est une opération effectuée sur une DCP (extraction, communication, stockage, suppression,...). Ce traitement doit avoir une finalité et être inscrit dans le registre des traitements de données.

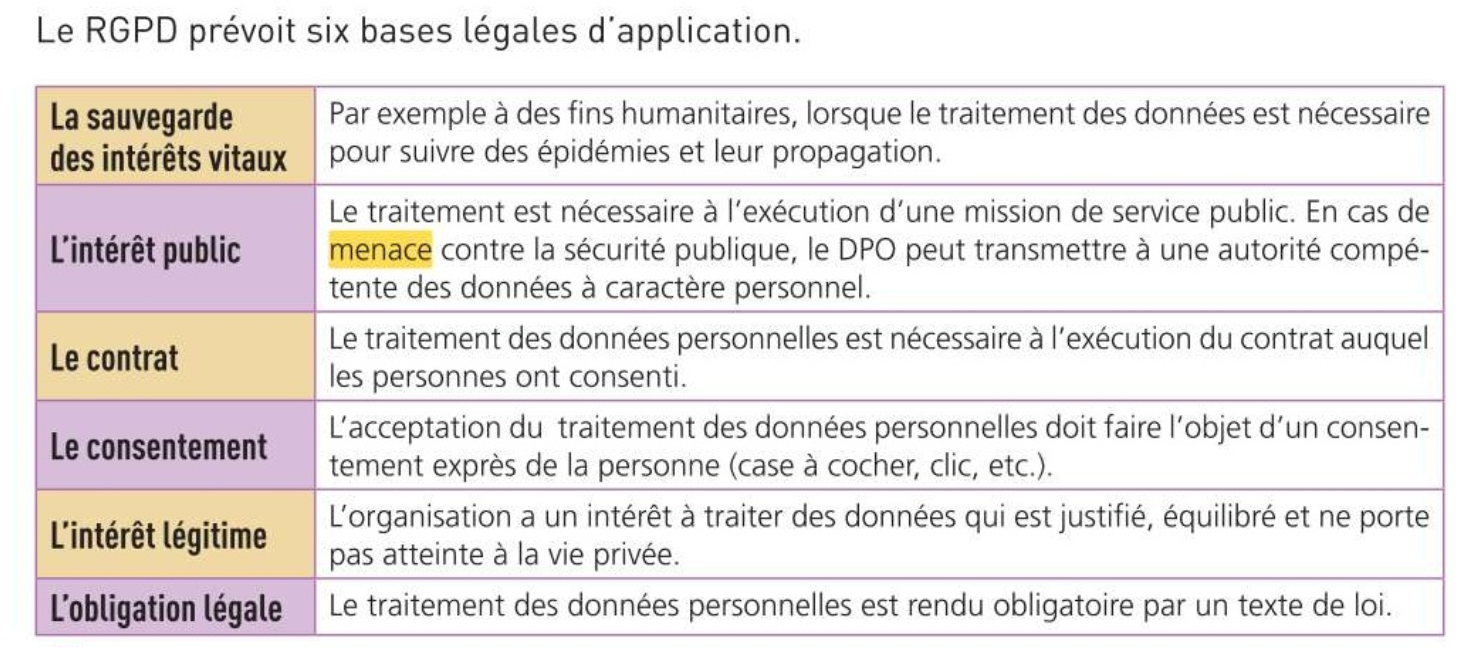
1. **Les bases légales d’application du RGPD**

Pour pouvoir **être mis en œuvre**, tout traitement de données doit **se fonder sur l’une** des « bases légales » prévues par le RGPD.

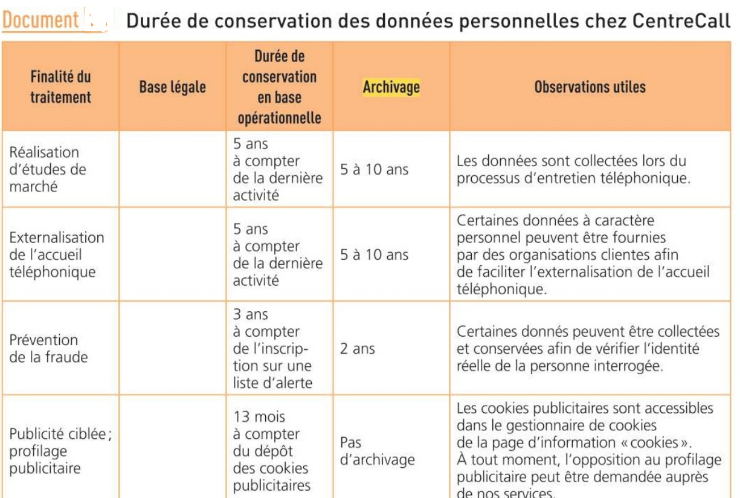
**La base légale d’un traitement est ce qui autorise légalement sa mise en œuvre**, ce qui donne le droit à un organisme de traiter des données à caractère personnel.

**Lorsqu’un même traitement de données poursuit plusieurs finalités, c’est-à-dire plusieurs objectifs, une base légale doit être définie pour chacune de ces finalités.** En revanche, il n’est pas possible de « cumuler » des bases légales pour une même finalité : il faut en choisir une seule.

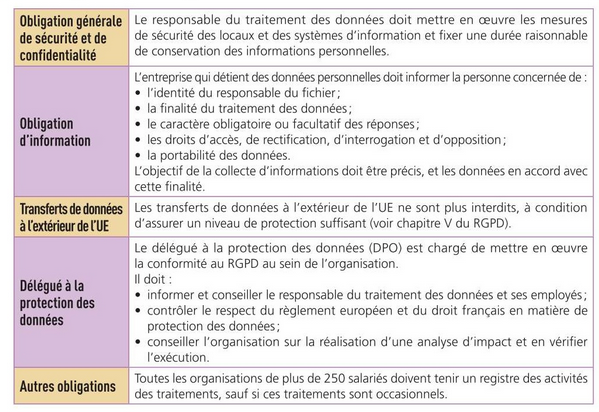
Exemple : un fichier « clients et prospects » d’une entreprise peut poursuivre plusieurs finalités, qui doivent chacune reposer sur une base légale : le contrat pour la gestion des commandes, des livraisons ou du service après-vente ; l’obligation légale pour la tenue de la comptabilité ; le consentement pour les opérations de prospection commerciale par voie électronique ; etc*.*



**Application : Centre Call est un centre d’appels téléphoniques, retrouvez les bases légales pour chaque finalité du traitement**

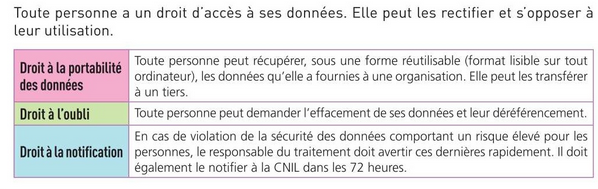


1. **Les obligations des organisations**



1. **Les droits de personnes**

<https://www.cnil.fr/fr/les-droits-pour-maitriser-vos-donnees-personnelles>



**Mission 3 : comprendre le rôle de la CNIL**

Créée en 1978 par la loi Informatique et Libertés, la CNIL est une **autorité administrative** **indépendante**, composée d’un Collège de 18 membres et d’une équipe d’agents contractuels de l’État.

* A **partir de ce site, et de vos recherches répondez aux questions**

<https://www.cnil.fr/fr/les-missions-de-la-cnil>

1. **Recensez les 4 missions de la CNIL** ?

Informer : Communication et information des personnes

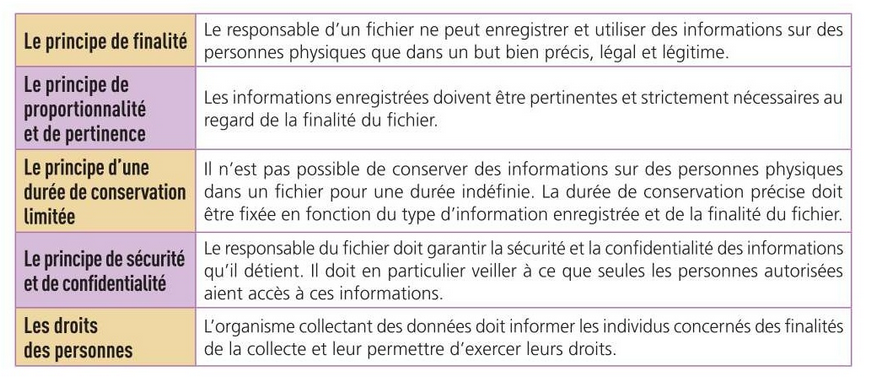
Conseiller : Aider à se conformer au RGPD

Innover : La CNIL organise des débats et expositions de nouvelles solutions de sécurité et de l’avenir des traitements de données

Contrôler et sanctionner : La CNIL contrôle des entreprises et les flux de données retransmises selon les problématiques du moment et prononce des sanctions envers qui déroge au RGPD

1. **Les 6 principes ou bons réflexes préconisés par la CNIL**

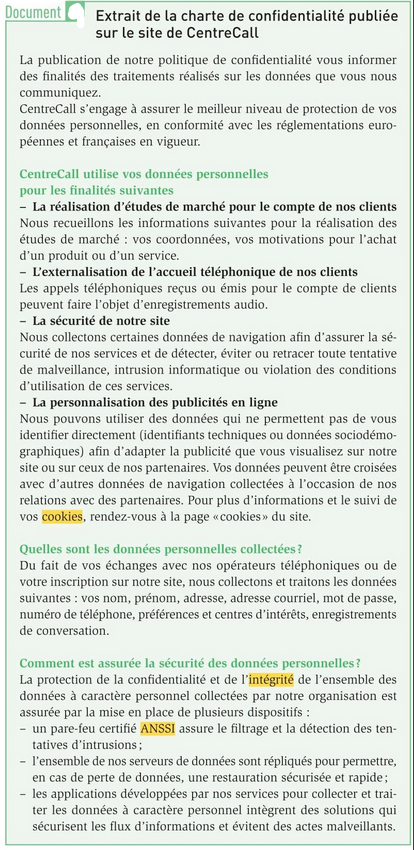
<https://www.cnil.fr/fr/adopter-les-six-bons-reflexes>



**Application : vérifiez (en complétant ce tableau) la conformité de la charte informatique (document ci-dessous) de Centre Call avec les principes fondamentaux préconisés par la CNIL**

Le principe de finalité est bien respecté dans cette charte car on en connaît les quatre principes. Les données collectées (nom, prénom,...) par Centre Call sont pertinentes par rapport aux finalités mentionnées.

* Les durées de conservation sont limitées donc le principe de conservation est bien respecté.
* Le principe de sécurité est bien respecté car pare-feu certifié ANSSI, serveurs de données répliqués, solutions sécurisées.
* Aucune information ne rappelle aux personnes comment exercer leurs droits.



**Mission 4: réaliser un résumé**

TRAVAIL DE GROUPE : A l’aide de vos réponses et des ressources

Réaliser **une note d’information ou un résumé**

**Les données à caractère personnel : définition, règlementation et rôle de la CNIL**

Pour réaliser ce travail, **vous compléterez le pad collaboratf qui** est sur Moodle