FMS ACADEMY

FORMATION SUPPORT Niveau 2 Airbus

M02 Cybersécurité – la RGPD

V2 22.12.21

Objectifs de ce module

Connaître les notions de données personnelles et de systèmes d'informations.

Comprendre les enjeux et les obligations de la RGPD en situation de travail

Définition de la RGPD

RGPD : Réglementation Générale de Protection des Données

Cadre législatif pour protéger les données personnelles des utilisateurs ou personnes physiques en relation avec les systèmes d'information de l'entreprise **au sein de l'Union Européenne.**

Le RGPD s'applique:

- aux **entreprises ou entités** qui traitent des **données à caractère personnel** dans le cadre des activités de l'une de leurs filiales **établie au sein de l'UE**, indépendamment de l'endroit où les données sont traitées;

ou

aux entreprises **établies en dehors de l'UE** qui proposent des biens ou des services (payants ou gratuits), ou surveillent le comportement **de personnes dans l'UE.**

Qui est impliqué ?

Le RGPD ne vise aucun type ou taille de société particulière.

Tout organisme doit respecter le RGPD si :

- ✓ elles traitent des données personnelles, pour leur compte ou non

- ✓elles sont établies **sur un territoire de l'Union Européenne** ou ciblent des **résidents européens**

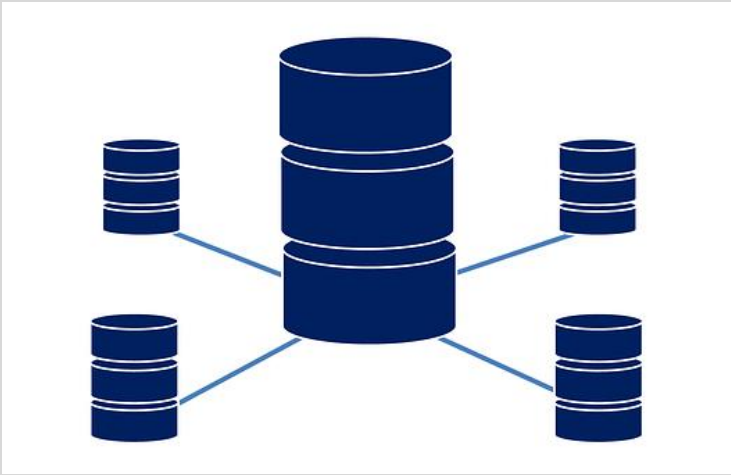
Le RGPD **concerne aussi les sous-traitants** qui traitent des données personnelles pour le compte d'autres organismes.

Application et histoire de la RGPD

Histoire

Les Systèmes d'informations

Le système d'informations de l'entreprise est l'ensemble des supports (**numériques ou non**) contenant les informations transitant ou utilisées par l'entreprise.



Qu'est-ce qu'une donnée personnelle ?

« Toute information se rapportant à une personne physique identifiée ou identifiable »

que ce soit :

- **Directement** (nom, prénom…)
- **Indirectement** (identifiant client, téléphone, voix, religion, croisement du plusieurs données…)

Qu'est-ce qu'une donnée personnelle ?

L'identification d'une personne physique peut être réalisée :

- **à partir d'une seule donnée** (exemple : numéro de sécurité sociale, ADN)

- **à partir du croisement d'un ensemble de données** (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association)
- *Données sensibles: origine raciale ou ethnique, opinions politiques ou religieuses, données génétiques,*

Le traitement des données personnelles

Le terme de traitement des données correspond à :

- ✓ la collecte
- ✓ l'enregistrement / conservation
- ✓ la modification
- ✓ l'utilisation
- ✓ l'organisation (statistique, par exemple)
- ✓ le rapprochement / croisement de données
- ✓ **la communication de ces données** à un tiers

Des exemples?

Le traitement des données personnelles

Si une société ne traite pas directement la donnée, par exemple parce qu'elle fait **appel à un prestataire extérieur** pour analyser ses informations clients, elle peut être considérée comme responsable du traitement.

Le prestataire sera considéré comme **sous-traitant** soumis au RGPD d'une façon particulière.

QUE DOIVENT FAIRE LES SOUS-TRAITANTS ?

Les sous-traitants sont tenus de respecter des **obligations spécifiques** en matière de sécurité, de confidentialité et de documentation de leur activité.

- **Exemples?**

QUE DOIVENT FAIRE LES SOUSTRAITANTS ?

Les sous-traitants ont également une **obligation de conseil** auprès de leurs clients

exemple : insister auprès de ses clients pour les mises à jour de logiciel.

Ils doivent **les aider dans la mise en œuvre de certaines obligations du règlement**

exemple : étude d'impact sur la vie privée, notification de violation de données, sécurité, etc.

Le traitement des donnés personnelles

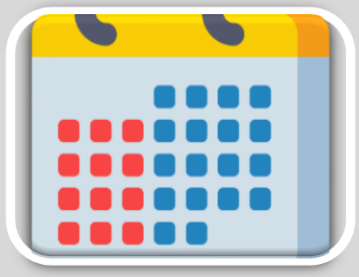
- Un mineur peut, **à partir de 15 ans**, consentir seul au traitement de ses données personnelles si celui-ci est effectué dans le cadre de services en ligne et s'il repose sur le consentement. Lorsque le mineur est âgé de moins de 15 ans, le consentement doit être donné par le mineur concerné et le titulaire de l'autorité parentale.

Quelles sont les obligations de l'entreprise?

Données vraiment nécessaires?

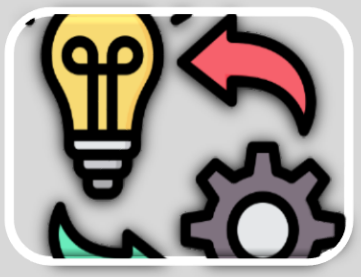
Transparence

Faciliter l'exercice des droits



Durées de conservation

Sécurisez



Démarche Continue

Données nécessaires?

Les données ne doivent être collectées que si elles sont **nécessaires** dans un but **déterminé et légitime**.

La collecte doit suivre deux principes :

- principe de **finalité** : restreint l'utilisation des données au but fixé, éviter le « au cas où »
- principe de **minimisation** : collecte du strict minimum pour l'objectif

L'accord doit être donné par une personne majeure sur internet, c'est-à-dire de plus de 15 ans.

Transparence

La collecte doit être **transparente** pour permettre aux personnes de rester **maître de leurs données** et d'accepter la collecte en étant **correctement informées.**

Les personnes doivent être informées dans un **langage adapté et compréhensible** :

- de l'existence de cette collecte
- de l'utilisation qui sera faite des données
- de leurs droits sur ces données et comment exercer ces droits

Organisez et facilitez l'exercice des droits

Les personnes doivent **pouvoir exercer leurs droits** sur **leurs données** facilement.

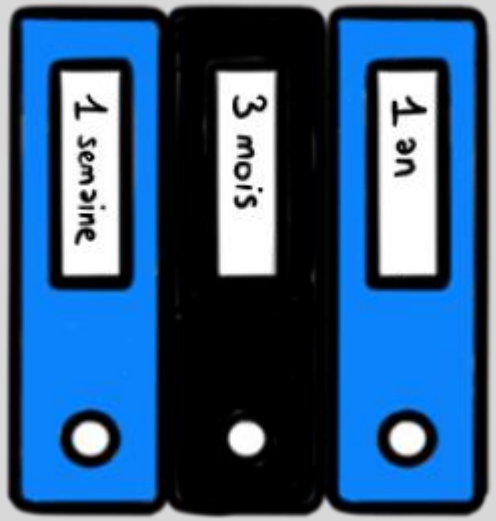
Cela implique notamment :

- mettre en place les outils pour exercer ces droits
- répondre aux demandes (accès, rectification, suppression, droit à l'oubli…) dans les meilleurs délais
- pouvoir effectuer ces requêtes via une adresse électronique dédiée

Fixez des durées de conservation

Les données doivent être collectées pour **une durée déterminée.**

Lorsque l'objectif est atteint les données doivent être **détruites**, **anonymisées** ou **archivées** selon les obligations légales pour le type de donnée concerné.



Par exemple, la CNIL recommande de supprimer les coordonnées d'un prospect, en l'absence d'échange, au bout de 3 ans.

Sécurisez les données

Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage

- **Sécurité physique et informatique**
- **Gestion stricte des droits d'accès**

Ces mesures doivent s'adapter à la sensibilité des données et aux risques en cas d'incident de sécurité.

Qu'est ce qu'une faille de sécurité?

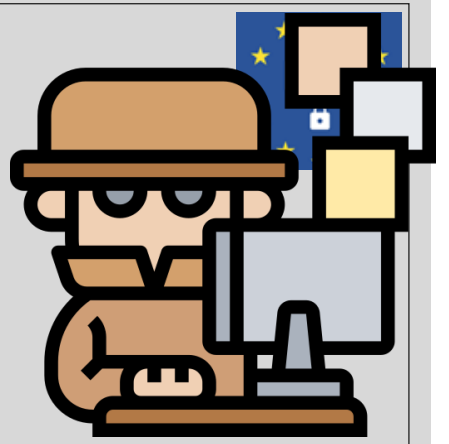
Toute atteinte non contrôlée aux données personnelles, ce qui comprend :

- Perte de disponibilité (suppression)
- Perte d'intégrité (modification)
- Perte de confidentialité

…. de manière ACCIDENTELLE ou ILLICITE.

DICT

Que faire en cas de violation ?



1- Documenter en interne l'incident :

- la nature de la violation
- catégorie et nombre approximatif de personnes concernées
- conséquences probables de la violation des données
- mesures prises ou envisagées pour éviter reproduction de l'incident et pour en atténuer les conséquences négatives

2- Notifier l'incident auprès de la CNIL dans les 72 heures.

3- Informer aux personnes si le risque est élevé

Quelles sont les obligations?

il n'est pas juridiquement responsable en cas de non-conformité du traitement

Un **Délégué à la Protection des Données** (DPO) chargé du RGPD est garant du respect de la bonne application de la RGPD au sein de l'entreprise.

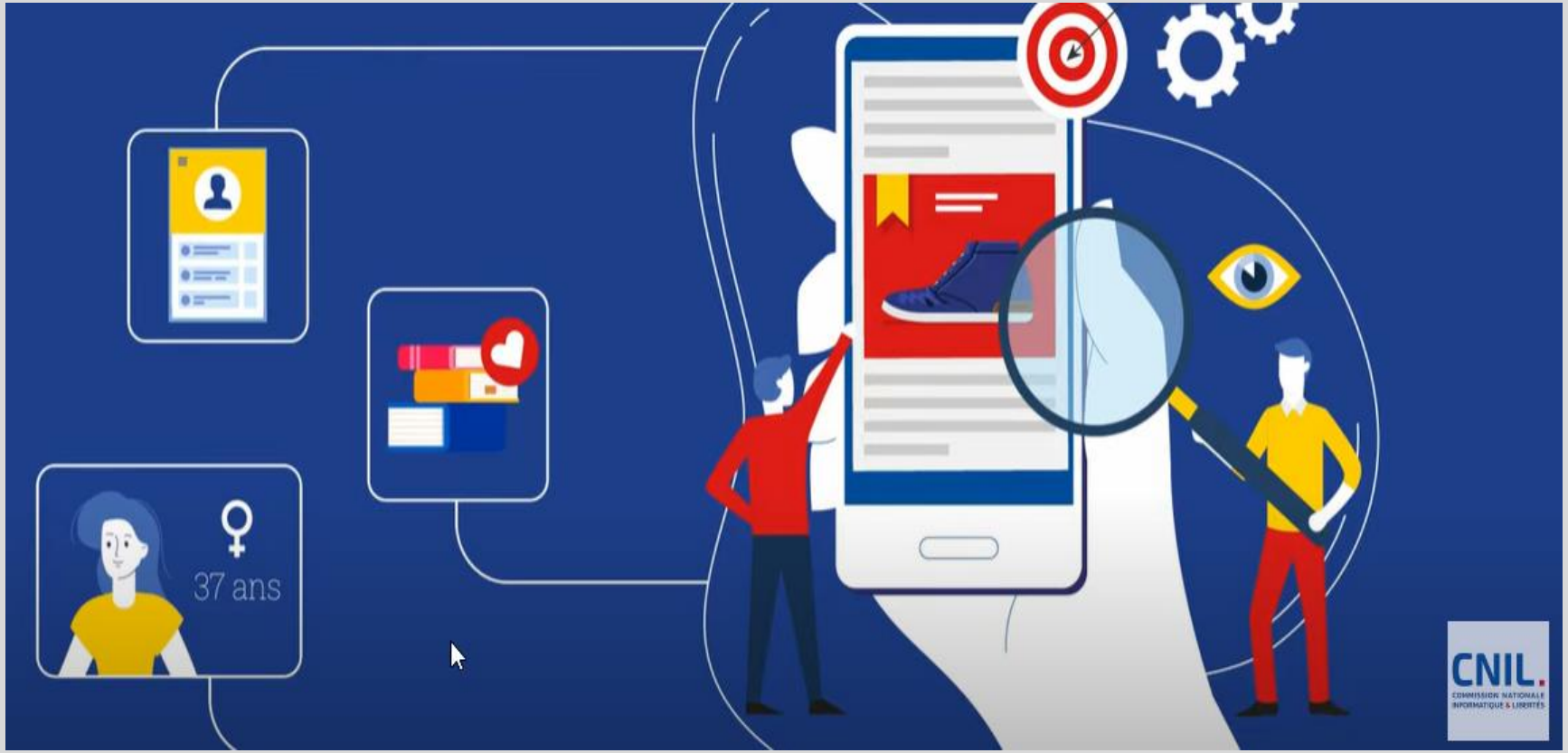
Quelles sont les sanctions?

Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- prononcer un rappel à l'ordre
- enjoindre de mettre le traitement en conformité, y compris sous astreinte
- limiter temporairement ou définitivement un traitement
- suspendre les flux de données
- ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte
- prononcer une amende administrative

Le montant des amendes est le maximum entre 4% du CA Mondial pour les entreprises à forte visibilité en ligne ou jusqu'à 20 Millions d'Euros.

Les cookies



Quels sont vos droits ?

Rester informé

- vous devez avoir accès facilement aux modalités de la collecte de données (qui ? comment ? pourquoi ? combien de temps ?...)
- vous devez être prévenu si vos données sont compromises (perdues, piratées, inaccessibles…)

Vous opposer à tout moment à la collecte de données s'il s'agit de prospection commerciale ou si ce refus est justifié par votre situation.

Demander une intervention humaine et contester des décisions prises uniquement grâce à un algorithme.

Quels sont vos droits ?

Vérifier vos données pour confirmer ce qui a été collecté à condition de rester dans les limites (fichier interdit d'accès par la loi, atteinte aux libertés d'autrui, requête excessive…).

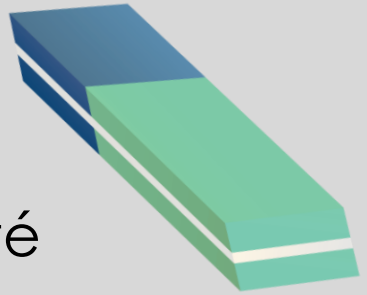
Rectifier vos données si elles sont erronées sauf pour les traitements littéraires, artistiques et journalistiques ou certains fichiers au fonctionnement particulier (police, renseignement…).

Demander vos données dans un format exploitable dans la mesure du possible pour permettre de **les exporter** vers un tiers (pour un changement de plateforme ou prestataire par exemple).

Quels sont vos droits ?

Déréférencer un contenu pour que les résultats des moteurs de recherche n'associent plus un contenu à votre identité (nom prénom uniquement).

ATTENTION le contenu n'est pas supprimé pour autant !



Effacer vos données si cette action ne vas pas à l'encontre de la loi (délai légal de conservation de facture par exemple) ou de la liberté d'expression et d'information.

Geler l'utilisation de vos données pour que les données ne soient plus utilisées même si elles sont conservées, par exemple dans l'attente d'un examen de ces données pour une procédure judiciaire.

Bibliographie

QUIZ: https://www.efficacd.com/rgpd-quizz.php#:~:text=Afin%20de%20s%C3%A9curiser%20les%20donn%C3%A9es,entreprise%20peuvent%20y%20avoir%20acc%C3%A8s.&text=Faux%20%3A%20L'acc%C3%A8s%20aux%20donn%C3%A9es,en%20fonction%20des%20objectifs%20poursuivis.

QUIZ: https://forms.office.com/r/wt2MkeuzFX

Bibliographie

Icônes conçues par Uniconlabs from www.flaticon.com

https://www.cnil.fr/sites/default/files/atoms/files/bpi-cnil-rgpd_guide-tpe-pme.pdf

https://www.cnil.fr/fr/comprendre-le-rgpd