Le compte rendu avec les différentes idées comprises

Module 1:

Le RGPD et ses notions clés

J’ai appris l’histoire du RGPD comme sa date de création.

Puis, j’ai vu la définition d’un traitement de données à caractère personnel donc c’est tout ce qui est :

collecte, stockage, usage, etc.

J’ai appris ensuite a que le RGPD s'applique aux :
les organisations, entreprises, administrations, et dans quelles situations le RGPD est applicable.

J’ai appris dans ce module le but principal du RGPD, a qui il s'adresse et surtout son histoire, sa création

Module 2:

Le principe de la protection des données.

On n’a appris les régle d’or du RGPD, il y en n’a 8, qui sont :

1. **Les principes clés que toute organisation doit respecter pour être conforme.**
2. **Finalité du traitement — expliquer pourquoi les données sont traitées, dans quel but et de façon légitime.**

3. **Licéité du traitement — les bases légales possibles : consentement, contrat, obligation légale, etc.**

4. **Minimisation des données — ne collecter que les données strictement nécessaires.**

5. **Protection particulière de certaines données — certaines données sont “sensibles” (données de santé, opinions politiques, etc.) et nécessitent des précautions renforcées.**

6. **Conservation limitée des données — durée de conservation des données, afin d'éviter qu'elles soient gardées indéfiniment sans justification.**

7. **Obligation de sécurité — garantir la sécurité des données : protéger contre les pertes, accès non autorisés, fuites, etc.**

8. **Transparence à l'égard des personnes concernées — informer les individus (via des politiques de confidentialité, des formulaires, etc.) sur la manière dont leurs données sont utilisées.**

9. **Droits des personnes — droit d'accès, de rectification, d'effacement, de portabilité, etc.**

10. **Encadrement des transferts de données hors de l'UE — règles à respecter quand des données sont transférées en dehors de l'Union européenne.**

Module 3 : Les responsabilité des acteurs :

1. **La protection des données dès la conception**

   La protection des données par défauts

2. **Dans cette activité numéros 2, on apprend le partage de la responsabilité avec des exemples et dès illustrations.**
3. **Içi on n'apprend; Le contrats des sous-traitants (ou de traitements contraintes) avec leurs obligations qui sont :**
   - **Transparence et traçabilité**
   - **Sécurité des données traitées**
   - **Encadrement de la sous-traitance ultérieure**
   - **Accompagnement du responsable de traitement**

On n'apprend aussi les DPO et le registre des traitements

4. **Les sanctions et voies de recours.**

   On peut avoir plusieurs types de sanctions, comme :

   - **Le rappel à l'ordre**
   - **L'injonction de mettre le traitement en conformité, y compris sous astreinte**
   - **Limitation temporaire ou définitive du traitement**
   - **Suspension des flux de données adressée à un destinataire situé dans un pays tiers**
   - **Ordre de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte.**
   - **Retrait d'une certification**
   - **Amende administrative, cela peut varier entre 10 millions d'euros ou 2% du chiffre d'affaires mondial si c'est un non-respect des dispositions sur le DPO, ou 20 millions d'euros ou 4% du chiffre d'affaires mondial si**

c’est un non-respect des principes fondamentaux ou des droits des personnes.

Voies de recours :

C’est une réclamations auprès d’une autorité de contrôle, comme :

Il peut sagir de l’autorité appartenant a l’Etat membre:

- **où se situe sa résidence habituelle.**
- **où se situe son lieu de travail.**
- **où la violation a été commise.**

Il y a, alors a ce moment-là :

Des réparation effective, comme :

Des préjudices.

Des dommages causés par la partie responsable.

Le registre des activités de traitement doit être tenu par : Les responsables de traitement et les sous-traitants

Module 4 :

1. **Le délégué à la protection des données :**

   Il a des missions :

   Informer et conseiller l’organisme

   Contrôler la conformité

   Jouer un rôle d’interface entre l’organisme, la CNIL et les personnes concernées.

   Les conditions requises, sont :

   Compétences et aptitudes.

   Absence de conflit d'intérêt.

   Moyens suffisants.

   Indépendance dans l’accomplissement des missions

   Il n’est pas obligatoire d' élire ou désigner un délégué.

Dans, plusieurs cas cela devient obligatoire, avec :

Activités de base

Suivi régulier et systématique

Grande échelle

et, il faut que sa sont volontaire et l'externalité.

Et il n'est pas forcément certifié.

2. **Le registre :**

On n'a appris :

À quoi sert précisément cette collecte de données ?

Ai-je vraiment besoin de cette donnée en particulier dans le cadre de mon projet ?

Est-il pertinent de conserver toutes les données aussi longtemps ?

Les données sont-elles suffisamment protégées ?

Ect… .

Organismes concernés.

Forme et contenu :

Contenu :

Les parties prenantes (représentant, sous-traitants, co-responsables, ect.) qui interviennent dans le traitement des données

Les catégories de données traitées

à quoi servent les données

qui accède aux données et à qui elles sont communiquées

combien de temps elles sont conservées

comment elles sont sécurisées

Dérogation :

Les traitements récurrents.

Les traitements susceptibles de comporter un risque pour les droits et libertés des personnes.

Les traitements qui portent sur des données sensibles.

Modèle de registre

Méthodes :

Etape 1 : rassembler les informations disponibles

Identifier

Analyser

Identifiée les données collectées

Utiliser la liste des traitements déclarés à la CNIL.

Etape 2 :

Lister

Exploiter

Remplir une fiche de registre par activité.

Etape 3 :

Sur la base de ce registre :

Identifier et analyser les risque

Élaborer un plan d'action en conformité avec la RGPD.

Suivis

Communication

Bonnes pratiques

3. **L'Analyse d'impact relative à la protection de données (AIPD)**

Elle a 4 Objectifs qui sont, je cite :

Décrire un traitement de données de façon détaillée

Évaluer sa conformité au RGPD

Identifier les risques, que ce traitement peut engendrer pour les droits et libertés des personnes physiques concernées.

Le cas échéant, traiter ces risques pour les réduire à un niveau acceptable.

Ils sont au coeur de la réflexion, avec : une question clé en tête, qui est :

Que risquent les personnes dont je vais traiter les données ?

Risque pour la vie privée :

Un événement redouté

Toutes les menaces qui rendent cet évènement possible

La source de cette menace

Les impacts potentiels de cet évènement

Le risque est estimé par une appréciation :

entre sa :

Gravité : Quelle est l'ampleur du préjudice pour les personnes concernées ?

Vraisemblance : quelle est la possibilité que l'événement redouté se réalise ?

L'AIPD : a 3 traitements, et est facultative, les méthodes, et les sanctions, comme : (2% de chiffre d'affaires annuel mondial, est pouvant aller jusqu'à 10 000 000 euros.

Les traitements antérieur au RGPD

4. **La notification des violations de données.**

J’ai appris, que pour avoir une violation de données personnelles, il faut que ces deux conditions soient réunis :

L’organisme a effectué un traitement de données personnelles.

Ces données ont fait l’objet d’une perte de disponibilité, d’intégrité ou de confidentialité, de manière accidentelle ou illicite.

J’ai vu aussi :

Les causes.

Les délais de notification, (72 heures)

Suites de la notification

Sanctions :

Amende / 10 000 000 euros

2% du CA

Le CNIL privilégie l’accompagnement des organismes et limite les conséquences d’une violation.

5. **Code de conduite et certification**

J’ai vu dans cette unité :

Les objectifs du code de conduite

La conception

La validation

Le contrôle

L’objectif de la certification

Organismes certificateurs

Rôles des pouvoirs publics

Incitatif

Participatif

Coercitif

Certification des compétences du DPO

Les référentiels élaborés par la CNIL :

Le référentiel d'agrément

Le référentiel de certification

Module 5 : Les collectivités territoriales

Objectif général
Dans ce module, plusieurs cas concrets sont présentés pour illustrer comment le RGPD s'applique dans les collectivités avec :

- **L'utilisation de caméras individuelles par des agents de police municipale. Ces dispositifs posent des questions de vidéosurveillance, de finalité, de sécurité et d'information des personnes.**

- **La gestion de la liste électorale : comment une collectivité peut traiter des données d'électeurs tout en respectant le RGPD.**

- **La gestion des fichiers d'état civil : naissances, décès, actes d'état civil contiennent des données personnelles sensibles dans certaines limites.**

- **La désignation d'un DPO (délégué à la protection des données) dans une collectivité : les collectivités doivent parfois nommer un DPO pour gérer la conformité RGPD.**

- **Les traitements liés à la communication politique : par exemple comment la collecte de données dans le cadre d'une campagne politique doit être encadrée.**

- **La mise à disposition de téléservices : les services en ligne municipaux ou territoriaux (portails citoyens) impliquent des traitements de données, d'où la nécessité d'une conformité.**

- **Les registres communaux d'alerte ou de protection des populations : gestion des données de vulnérabilité, d'urgence, ou d'alerte, ce qui nécessite des mesures de sécurisation et de limitation.**

- **La communication de renseignements aux "tiers autorisés" : certaines collectivités partagent des données avec des entités tierces (par exemple d'autres administrations), donc l'importance des bases légales et des garanties.**

- **Les fichiers de communication institutionnelle : newsletter, bulletins municipaux, etc. – comment collecter et envoyer des communications tout en**

respectant les droits des personnes.

- **Les fichiers des activités scolaires et périscolaires : les collectivités gèrent des données d'élèves ou de participants à des activités municipales.**

- **Le recensement de la population : traitement de données de population pour des besoins démographiques tout en respectant la confidentialité.**

- **Les fichiers sociaux et médico-sociaux : traitement des données sensibles liées à des aides, des services sociaux ou médico-sociaux.**

- **Le droit d'accès aux documents administratifs : comment les citoyens peuvent exercer leurs droits (accès, rectification) via des demandes d'accès aux documents publics qui contiennent des données personnelles.**

- **Un point sur les rançongiciels (ransomware) : la menace des rançongiciels pour les collectivités, et l'importance de sécuriser les données pour limiter les risques.**

Méthode pédagogique
Le module utilise des cas concrets, des vidéos, des textes explicatifs et des illustrations pour rendre la théorie vivante dans le contexte des collectivités. Il y a aussi des quiz pour tester la compréhension.
À la fin du module, une attestation de suivi peut être délivrée si on répond correctement à une proportion des questions (80 %) selon les conditions du MOOC.

Ce que j'en ai retenu / ce que je trouve important

- **Les collectivités ont des responsabilités particulières car elles traitent des données très variées (électeurs, usagers, population, scolaires, etc.).**

- **Il ne suffit pas de "faire comme une entreprise" : certains traitements (comme les téléservices ou les listes électorales) demandent des justifications claires de finalité, de sécurisation, et de transparence.**

- **Le rôle du DPO est central dans ce contexte : il peut aider la collectivité à structurer ses registres, ses processus, et à former les agents.**

- **Les risques (ex : rançongiciels) sont réels : il faut anticiper la sécurité des données au niveau des collectivités, car elles sont des cibles.**

Module 6 : Travail et données personnelles

Objectif général
Ce module (nouveau) vise à couvrir les traitements des données personnelles dans le contexte du travail — c'est-à-dire les données des salariés, stagiaires, intérimaires,

etc. Il permet de comprendre comment appliquer le RGPD spécifiquement dans les RH (ressources humaines).

Structure du module
Le module est structuré en 5 thématiques, totalisant 14 unités.

Voici les grandes thématiques et ce qu'elles couvrent :

1. **Le recrutement**
    - **Les données collectées lors du recrutement (CV, lettre de motivation, éventuellement données sensibles)**
    - **Comment la base légale du traitement (ex : consentement, intérêt légitime, obligation légale) s'applique au recrutement**
    - **Les obligations d'information des candidats (transparence)**
2. **La gestion du personnel**
    - **Données administratives des employés (identité, adresse, contact)**
    - **Données de carrière (poste, évaluations)**
    - **La conformité RGPD dans les systèmes RH (SIRH, registres du personnel)**
3. **La gestion de l'activité et de l'équipement**
    - **Données liées à l'usage des équipements professionnels (ordinateur, téléphone, outils informatiques)**
    - **Le télétravail : collecte des données, suivi d'activité, contrôle des horaires, accès aux locaux**
    - **Sécurisation des équipements, conservation des logs, etc.**
4. **Le dialogue social**
    - **Les échanges avec les représentants du personnel (syndicats) : comment traiter les données de façon conforme**
    - **Les élections professionnelles et le vote électronique : spécificité des traitements dans ce contexte**
    - **La transparence à l'égard des collaborateurs en matière de collecte des données**

5. **L’exercice des droits des personnes au travail**

    - **Droit d’accès, de rectification, de suppression : comment un salarié peut exercer ses droits sur ses données**

    - **Le périmètre du pouvoir de contrôle de l’employeur : limites légales, respect des droits fondamentaux**

    - **Le traitement des données sensibles (par exemple dans le cadre de la santé au travail)**

    - **La fin de contrat : que deviennent les données quand l’employé quitte l’entreprise (archivage, suppression)**

- **Ces deux modules (5 et 6) m’ont permis de relier la théorie du RGPD à des contextes concrets : collectivités et entreprises / RH.**

En conclusion : Cette certification, m’a aidée a analyser, et comprendre ce que c’était le RGPD? et plus particuliérement au fil de c’est module et de c’est certification j’en savait d’avantage sur le RGPD? beaucoup trop d’information toute suite, mais je recommande cette certification si l’on veut connaitre et savoir plus en détaille ce que c’est a quoi sa sert les différents objectifs, poste, mission sanctions qui se ressemble généralement, tout ce qui concerne et se qui touche le RGPD.

- **Le module 1 permet de bien comprendre le cadre général : ce qu’est le RGPD, à qui il s’applique, et les définitions de base.**

- **Le module 2 installe les principes concrets : ce sont les règles que toute organisation doit appliquer pour traiter légalement et de manière responsable les données personnelles.**