

ADIT 63

Marie-Bénédicte RAHON – juriste au service des affaires sociales, des collectivités territoriales, du sport et de l'environnement (transports publics, énergie, habitat)

Jeudi 24 septembre 2026

De quoi parle-t-on?

➤ QU'EST CE QUE LA CNIL ?

- Créée par la loi Informatique et Libertés du 6 janvier 1978, la CNIL est une **autorité administrative indépendante**.
- « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* » - Article 1^{er} de la LIL.

➤ QU'EST CE QUE LE RGPD ?

- Texte européen qui fixe et harmonise les règles en matière de protection des données à caractère personnel.
- C'est un texte qui protège des libertés fondamentales.
- Protection de la personne concernée (client, usager, administrés...) → enjeu de confiance

DE QUOI PARLE-T-ON ?

➤ QU'EST CE QU'UNE DONNÉE À CARACTÈRE PERSONNEL ?

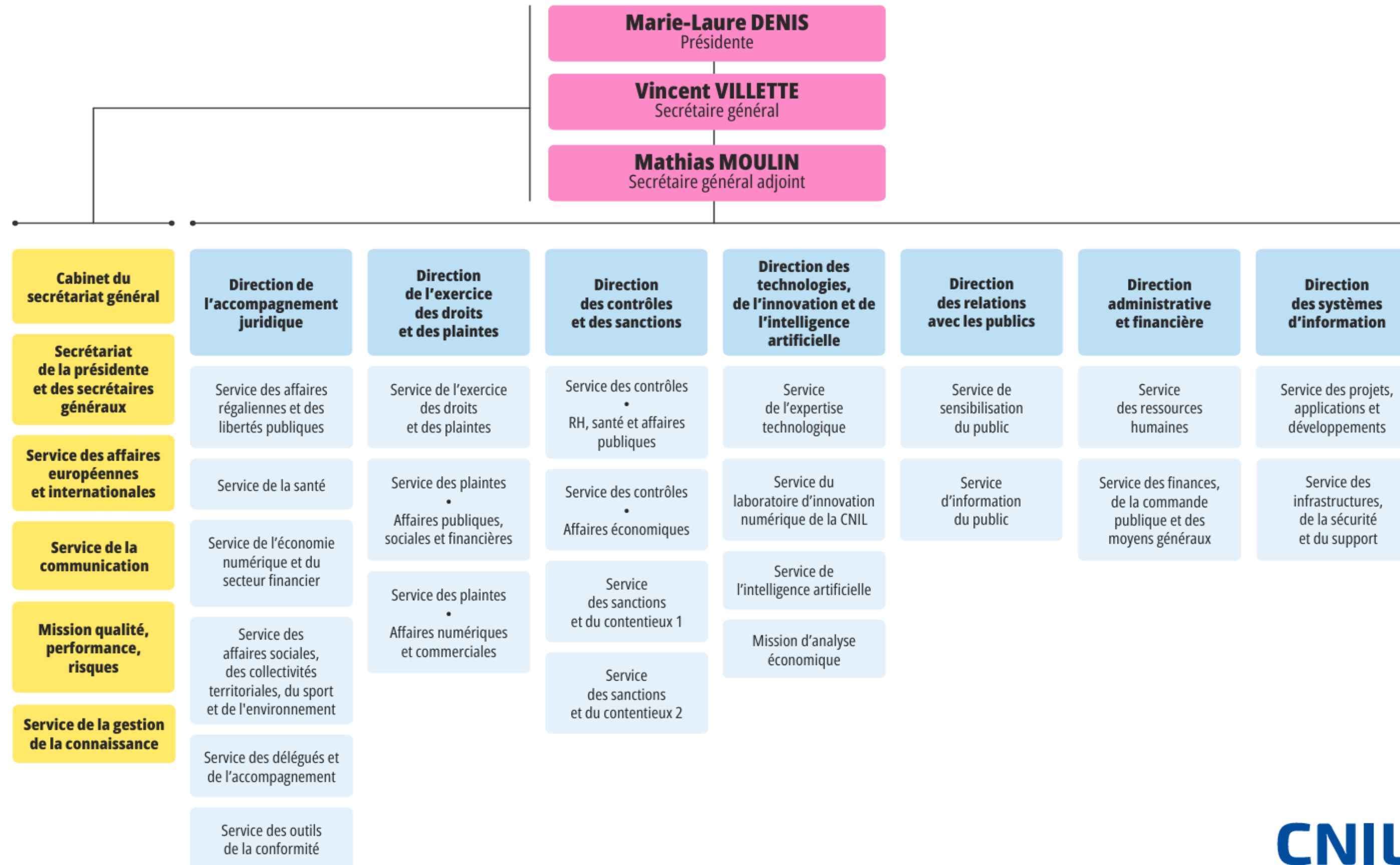
- Toute information se rapportant à une personne physique identifiée ou identifiable.
- L'identification d'une personne physique peut être réalisée à partir d'une seule donnée ou à partir du croisement d'un ensemble de données.
- Exemples : données d'un administré, image de vidéosurveillance, coordonnées d'un fournisseur...

➤ QU'EST CE QU'UN TRAITEMENT DE DONNÉES ?

- Il s'agit de toute opération portant sur ces données.
- Exemples : collecte de la donnée, enregistrement dans un dossier, suppression ...

La CNIL et ses missions

Organigramme des directions et services de la CNIL



Organisation des équipes

Une cinquantaine d'agents composent la DAC

- 4 services sectoriels :
 - Affaires économiques
 - Affaires régaliennes
 - Santé
 - SACSE (Affaires sociales, collectivités territoriales, sport et environnement)
- 2 services thématiques :
 - Délégués à la protection des données et de l'accompagnement
 - Outils de la conformité



LES MISSIONS DE LA CNIL

INFORMER LES PERSONNES ET PROTÉGER LEURS DROITS

- Répondre aux demandes des particuliers et des professionnels.
- Mener des actions de communication à travers ses réseaux, les médias, le site web, les réseaux sociaux ou en mettant à disposition des outils pédagogiques.

CONTRÔLER ET SANCTIONNER

- Le contrôle permet à la CNIL de vérifier la mise en œuvre concrète de la loi.
- Elle peut imposer à un acteur de régulariser son traitement (mise en demeure) ou prononcer des sanctions (amendes, etc.).

ACCOMPAGNER LA CONFORMITÉ ET CONSEILLER

- Aider les organismes privés et publics à se conformer au RGPD en proposant une boîte à outils adaptée à leurs tailles et leurs besoins.
- Recherche de solutions leur permettant de poursuivre leurs objectifs légitimes dans le strict respect des droits et des libertés des citoyens.

ANTICIPER ET INNOVER

- Détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée.
- Contribuer au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de privacy by design.

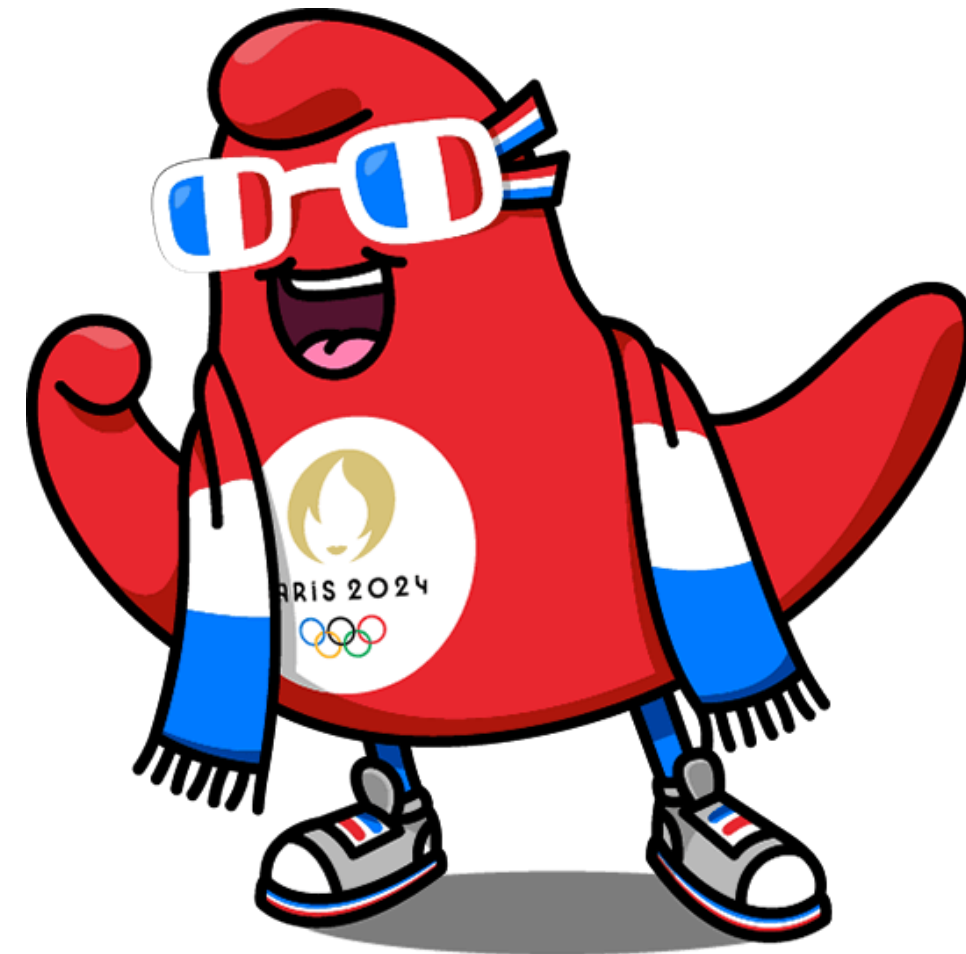
Focus sur le conseil et l'accompagnement

Mise en conformité = objectif **prioritaire** de la CNIL

- Idée générale de *mise en conformité a priori*
- Activité variée :
 - avis sur des projets de texte créant des nouveaux fichiers par exemple,
 - conseils aux pouvoirs publics, participation à des auditions (parlementaires, cour des comptes, corps d'inspection...)
- Développements d'outils adaptés aux besoins et aux particularités des organismes et des publics : **MOOC, référentiel, guides...**

Quelques illustrations récentes

- Recommandations **sur le déploiement d'IA génératives**
- Avis au gouvernement pendant les JOP, la crise sanitaire...
- Bac à sable sur l'« **IA et services publics** » ou encore sur la « **Silver économie** » et accompagnement renforcé...
- Référentiels : « accompagnement social et médico-social », « gestion RH », « gestion commerciale » ...
- Consultations publiques sur le déploiement des caméras dites « intelligentes », vidéo dans les EHPAD, alertes professionnelles...



La logique du RGPD en deux mots

- L'« *accountability* » et le « *privacy by design* »
 - Changement de culture
 - Rééquilibrage des situations RT/ST
 - Outils de conformité et documentation de la conformité
 - Exemple des violations de données
- Le renforcement des droits et des sanctions
- Un champ d'application très large



Les grands principes

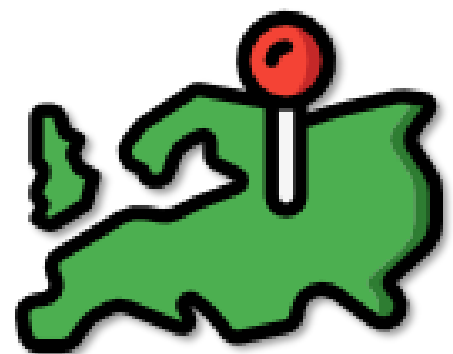
LA LOGIQUE DU RGPD EN DEUX MOTS

- Responsabilisation des organismes et accompagnement
- Le renforcement des droits et des sanctions
- Un champ d'application très large

LE CHAMP D'APPLICATION

1 Un traitement de données personnelles...

2 ...effectués par un RT ou un ST...



établi sur le
territoire de l'UE
*critère de
l'établissement*

ou

visant des
personnes de l'UE
critère du ciblage



LES PRINCIPES DE LA PROTECTION DES DONNÉES

- 01**  **Licéité**
Tout traitement de données n'est licite que s'il repose sur une « **base légale** »
définie par le responsable de traitement
- 02**  **Finalité**
Les DCP contenues dans un traitement ne sont recueillies et traitées que pour un
usage déterminé et légitime, préalablement défini
- 03**  **Minimisation**
Seules les données pertinentes et nécessaires au regard des objectifs poursuivis
doivent être traitées
- 04**  **Durée limitée de
conservation**
Tant qu'elles présentent un caractère identifiant, **les données ne peuvent être
conservées de façon indéfinie dans les fichiers**
- 05**  **Sécurité**
Le responsable du traitement doit **prendre les mesures nécessaires pour garantir
l'intégrité et la confidentialité des données**
- 06**  **Droits des personnes**
Toute personne dont les données sont utilisées dans un traitement disposent d'un
droit d'accès, de rectification et d'opposition...

LES DROITS DES PERSONNES



1. Information
2. Accès
3. Rectification
4. Effacement
5. Opposition
6. Limitation
7. Portabilité des données
8. Décision individuelle automatisée

L'OBLIGATION DE DESIGNER UN DPO

- Les autorités et organismes publiques ont l'obligation de désigner un Délégué à la protection des données (DPD) ou *Data protection officer (DPO)*.
- Le DPO doit détenir les compétences requises et disposer de moyens suffisants.
- Le DPO doit pouvoir agir en toute indépendance et pouvoir rendre compte directement au responsable de traitement.
- Le DPO peut être interne ou externe ou encore mutualisé.

L'OBLIGATION DE DESIGNER UN DPO

« **Chef d'orchestre** » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé de :

- Informer et conseiller ;
- Contrôler le respect de la réglementation ;
- Coopérer avec l'autorité de contrôle (CNIL) ;
- Être le point de contact avec les personnes concernées.

Merci de votre attention!

Echanges libres