CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

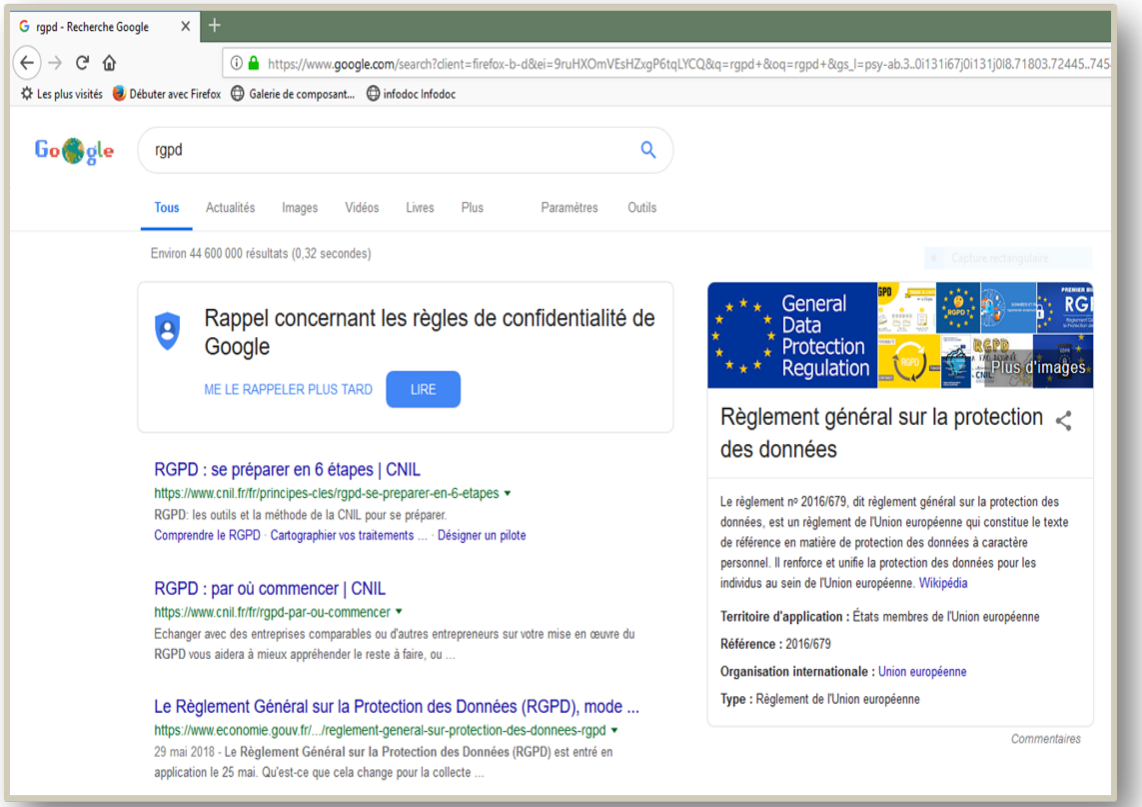
PROTÉGER les données personnelles
ACCOMPAGNER l'innovation
PRÉSERVER les libertés individuelles

La stratégie du régulateur et les priorités pour 2022

Conférence FVD - 04 novembre 2021

Sophie NERBONNE – Directrice chargée de co-régulation économique

#RGPD = la régulation à l'heure de l'économie numérique



LES CHIFFRES CLÉS 2020

CONSEILLER & RÉGLEMENTER

20 AUDITIONS PARLEMENTAIRES

8 QUESTIONNAIRES ADRESSÉS AU PARLEMENT OU À UN PARLEMENTAIRE EN MISSION

423 AUTORISATIONS DE RECHERCHE EN SANTÉ DONT
- **89** AUTORISATIONS DE RECHERCHE SUR LA COVID-19
- **45%** DES DOSSIERS COVID-19 TRAITÉS EN MOINS DE DEUX JOURS

139 DÉLIBÉRATIONS DONT
- **96** AVIS SUR DES PROJETS DE TEXTE

ACCOMPAGNER LA CONFORMITÉ

73 331 ORGANISMES ONT DÉSIGNÉ UN DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

25 494 DPO DÉSIGNÉS

+21% PAR RAPPORT À 2019

109 472 COMPTES CRÉÉS SUR LE MOOC* ATELIER RGPD**

2 825 NOTIFICATIONS DE VIOLATIONS DE DONNÉES

1 MOOC : Massive Open Online Course (outil de formation à distance).
2 RGPD : règlement général sur la protection des données.

PROTÉGER

13 585 PLAINTES QUI ONT CONDUIT À
- **4 528** RÉPONSES RAPIDES
- **9 057** ÉTUDES PLUS APPROFONDIES

3 996 DEMANDES VALABLES DE DROIT D'ACCÈS INDIRECT (DAI)

3 286 VÉRIFICATIONS EFFECTUÉES

INFORMER

121 439 APPELS REÇUS

20 452 REQUÊTES REÇUES PAR VOIE ÉLECTRONIQUE **+18%**

9 677 000 VISITES SUR LES SITES WEB DE LA CNIL **+21%**

124 059 *FOLLOWERS* SUR TWITTER **+7%**

37 418 FANS SUR FACEBOOK **+7%**

133 053 ABONNÉS SUR LINKEDIN **+16%**

CONTRÔLER & SANCTIONNER

247 CONTRÔLES ONT ÉTÉ EFFECTUÉS DONT
- **82** CONTRÔLES EN LIGNE
- **74** CONTRÔLES SUR PIÈCES

49 MISES EN DEMEURE DONT
- **3** PUBLIQUES
- **4** ADOPTÉES EN COOPÉRATION AVEC D'AUTRES CNIL EUROPÉENNES

38 rappels à l'ordre prononcés par la présidente
2 avertissements prononcés par la présidente

14 SANCTIONS DONT
- **11** AMENDES D'UN MONTANT TOTAL DE 138 489 300 EUROS
- **2** RAPPELS À L'ORDRE DE LA FORMATION RESTREINTE
- **1** INJONCTION SOUS ASTREINTE NON ASSOCIÉE À UNE AMENDE

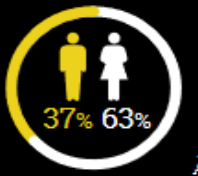
1 NON-LIEU

RESSOURCES HUMAINES

BUDGET : **20,1** MILLIONS D'EUROS

8 ANS ANCIENNETÉ MOYENNE DES AGENTS DE LA CNIL

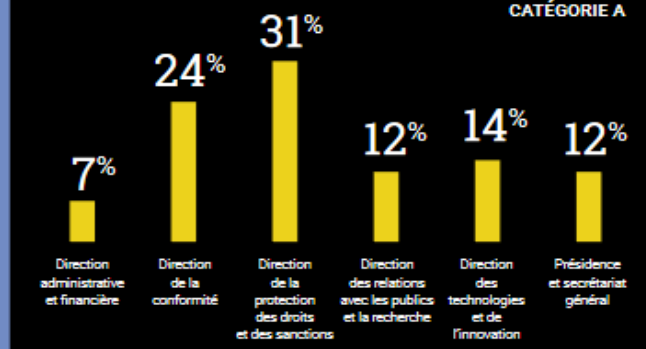
225 emplois



39 ans Âge moyen

59% D'AGENTS ARRIVÉS ENTRE 2015 ET 2020

80% DES AGENTS OCCUPENT UN POSTE DE CATÉGORIE A



L'application cohérente du RGPD : Les deux enjeux pour la CNIL

- **Accompagner les acteurs professionnels dans leur transition numérique**
  - Apporter de la sécurité juridique
  - Aider l'innovation - prospective - LINC
  - Du CIL au DPO
  - Des labels à la certification
  - Guides pratiques, tutoriels, vidéo, MOOC
- **Réussir le pari de la gouvernance européenne**
  - Gestion des plaintes
  - Contrôles sur place et à distance
  - Sanctions (relèvement conséquent des plafonds)

Ancrer la CNIL comme facilitateur de la transition numérique

Assurer des réponses adaptées et évolutives au travers des outils de conformité et de l'action des DPO

- Compréhension des besoins des acteurs professionnels
- Au service des personnes concernées par les traitements
- Pour élaborer des outils de régulation agiles (vision facilitatrice du droit)
- A porter au niveau européen

dpo Délégué à la protection des données

Une co-régulation avec des publics ciblés

- Animation de multiples réseaux en privilégiant les têtes de réseaux (effet démultiplicateur)
- Pour construire une innovation durable et responsable

Bilan d'application du RGPD sur l'accompagnement des acteurs

- ✓ **Plus de 73 000 organismes ont désigné un DPO.**
- ✓ **Référentiels de certification des compétences du DPO et plusieurs dossiers de tiers certificateurs en cours d'instruction.**
- ✓ **Règlement type biométrie sur les lieux de travail.**
- ✓ **Un référentiel sur la gestion commerciale des clients et la gestion des impayés.**
- ✓ **Un MOOC ouvert à tous intitulé « L'atelier RGPD » pour découvrir ou mieux appréhender le RGPD, avec deux objectifs : initier une mise en conformité des organismes et aider à la sensibilisation des opérationnels (109 472 comptes créés en 2020)**
- ✓ **Publications sur le site : Un kit d'information à l'attention des travailleurs sociaux pour protéger les données des bénéficiaires d'un service social (mesures de sécurité été mentions d'informations)**
- ✓ **Le rappel des modalités pour exercer ses droits (y compris à la portabilité)**
- ✓ **Les principes à respecter en matière de transmission des données à des partenaires à des fins de prospection électronique avec la distinction B to B et B to C.**

Actions prioritaires en 2022

1. Amplification des actions d'accompagnement des professionnels :

- ✓ La déclinaison de la stratégie d'accompagnement des secteurs privés et publics
- ✓ Un dialogue étroit avec les têtes de réseaux pour les outils de conformité (code de conduite et mécanismes de certification)
- ✓ Un focus sur les infrastructures et plates-formes numériques de cloud

2. Une activité répressive plus affirmée :

- ✓ La cybersécurité des sites web
- ✓ Le contrôle du respect des règles applicables aux cookies et autres traceurs.
- ✓ Sécurité du traitement des données de santé

Focus : - Montant des sanctions cumulées 138 millions d'euros et 5 injonctions sous astreinte par la formation restreinte

- 49 mises en demeure dont 3 publiques et 4 adoptées en coopération avec les CNIL européennes

3. Une diplomatie de la donnée personnelle aux niveau européen et international

- ✓ Le renforcement de la coopération européenne
- ✓ Le RGPD comme un standard mondial

Quelques sanctions

- **CNIL c/ la société MONSANTO, 26 septembre 2021** :
  - Manquement à l'obligation d'information des personnes : La société MONSANTO, responsable de traitement, était tenu d'informer les personnes concernées de l'existence d'un fichier de contacts les mentionnant.
  - Manquement à l'obligation d'encadrer les traitements effectués pour le compte du responsable de traitement : La société MONSANTO, en tant que responsable de traitement, doit encadrer par un acte juridique, la réalisation du traitement effectué pour son compte par son sous-traitant.

  → Amende de 400 000 euros + décision rendue publique.

- **CNIL c/ un responsable de traitement et son sous-traitant (anonymes), 27 janvier 2021 :**
  - Manquement à l'obligation de préserver la sécurité des données personnelles des clients : Le responsable de traitement et le sous-traitant ont tardé à mettre en place des mesures permettant de lutter efficacement contre certaines cyberattaques. Des données de 40 000 clients environ étaient rendues accessibles à des tiers non autorisés pendant près d'un an.

  → Amende de 150 000 euros pour le responsable de traitement et 75 000 euros pour le sous-traitant.

Transfert des données hors de l'UE: mesures supplémentaires à prendre

Deux objectifs du RGPD : libre circulation des données personnelles (DP) au sein de l'UE et préservation des droits et libertés des personnes en matière de protection de leurs DP, ce qui est un droit fondamental.

Schlems II : dans sa décision du 16 juillet 2020, la CJUE rappelle que les DP voyagent hors UE avec un niveau de protection essentiellement équivalent (et non identique). Dès lors :

- ✓ nécessité pour l'exportateur des DP (le cas échéant avec l'importateur) de vérifier, au cas par cas, si la loi ou les pratiques du pays destinataire portent atteinte aux droits,
- ✓ dans ce cas, des mesures complémentaires, non précisées par la Cour, doivent être mises en œuvre en vertu du principe de responsabilité (5.2).

Le CEPD, conscient de la complexité de ces 2 tâches, a adopté le 18 juin 2021 des recommandations sur le mode opératoire et des exemples de mesures complémentaires :

1. **Cartographie des transferts** : vérifier où vont les DP et si elles sont bien pertinentes et non excessives au regard de la finalité poursuivie.
2. **Vérifier l'outil de transfert** : décision d'adéquation de la commission européenne évitant de procéder à cette analyse ; sinon recourir à l'un des cinq outils de transfert (CCT ou ad hoc, BCR, codes de conduite ou certification) ou aux dérogations de l'article 49 (consentement, sauvegarde de la personne…) sachant qu'elles ne peuvent devenir la règle (cf. guidelines spécifiques)

Synthèse des recommandations CEPD du 18 juin 2021 (suite)

3. **Evaluation des lois et pratiques du pays destinataire des DP** : des pratiques contraires aux lois de PD locales ou aux garanties offertes par les outils de transfert entrainent la suspension des transferts ou l'application de mesures complémentaires; en cas de doute sur l'application problématique de lois non conformes au RGPD (surveillance par les autorités publiques), outre les 2 cas supra, il est aussi possible de poursuivre les transferts après avoir documenté le fait qu'il n'y a pas de raison de croire à leur application (due diligence). Des sources d'information sont listées en **annexe 3** (jurisprudence CJUE et CEDH ou des tribunaux locaux, rapports d'organisation internationales, d'autorités publiques gouvernementales ou parlementaires, d'organisations professionnelles ou académiques, d'ONG, ou même de rapports de transparence (mentionnant l'absence de demandes d'accès pour des motifs de sécurité publique)

4. **Identifier et adopter les mesures supplémentaires** : liste non exhaustive de mesures dont l'effectivité dépend des pays, du contexte du transfert, de l'outil de transfert, à combiner le cas échéant et toujours à documenter (en **annexe 2**, nombreux exemples de :

- **mesures techniques** avec divers scenarii : cas identifiant des solutions (stockage de DP sans besoin d'accès en clair; données pseudonymisées...) ou non (recours à des clouds ou autres ST ayant besoin d'accéder aux données en clair, accès à distance à des bases RH ou clients) ;
- **mesures contractuelles additionnelles** : sur l'obligation de recourir à certaines mesures techniques, renforcement de la transparence de l'importateur sur les demandes d'accès, des droits d'information et recours des personnes concernées ;
- **mesures organisationnelles** : règles internes de gouvernance des transferts de données ; documenter la conformité RGPD (minimisation des données, accès et durée limités ;

5. **Procéder, le cas échéant, aux formalités nécessaires** : En fonction des outils de transferts
(ex : autorisation de l'autorité de PD nécessaire pour clause ad hoc)

6. **Réévaluer régulièrement le niveau de protection** : et contrôler la bonne application du dispositif (à documenter).

Les autorités de protection des données contrôleront et pourront suspendre ou interdire les transferts non conformes, tout en continuant à prodiguer des conseils aux exportateurs de données, dans le cadre d'une coordination européenne permettant d'assurer l'application cohérente du RGPD.

MERCI POUR VOTRE ATTENTION ET PLACE AUX QUESTIONS