EPD
ÉQUIPE PROTECTION DES DONNÉES

CENTRE DE GESTION
de la fonction publique territoriale

RGPD

Les Actus

Un tour d'horizon des actualités sur la protection des données des derniers mois

Avril-Juin 2025

La CNIL publie son rapport annuel 2024

Le bilan annuel de la CNIL pour l'année 2024 est marqué par une activité répressive en hausse, un encadrement progressif de l'IA et une vigilance accrue face à l'augmentation des violations de données.

Une activité répressive en forte hausse

En 2024, un record de plaintes a été enregistré, avec **17 772 réclamations**, soit une hausse de **+8 % par rapport à 2023**.

La CNIL a également mené 321 contrôles en 2024, autour de plusieurs thématiques prioritaires :

- La collecte des données dans le cadre des Jeux Olympiques et Paralympiques ;
- La protection des données des mineurs en ligne ;
- Les programmes de fidélité et tickets de caisse dématérialisés ;
- Le droit d'accès des personnes : un établissement public a d'ailleurs été rappelé à l'ordre pour non-respect de ce droit fondamental.

Côté sanctions, l**e nombre de décisions a doublé** par rapport à 2023 :

- 87 sanctions ont été prononcées
- 180 mises en demeure ont été adressées,
- 64 rappels aux obligations légales ont été formulés.

Encadrement de l'intelligence artificielle

Suite à l'entrée en vigueur du Règlement européen sur l'IA en aout 2024, la CNIL a publié ses premières recommandations pour encadrer le développement et l'utilisation des systèmes d'IA. Elle met à disposition sur son site internet un ensemble de 12 fiches thématiques, permettant de concilier l'utilisation et le développement des systèmes d'IA avec le respect du RGPD.

La sécurité des données face à des risques de plus en plus élevés

L'année 2024 a été marquée par une hausse sans précédent des violations de données, touchant tous les secteurs d'activité.

Dans son rapport, la CNIL alerte sur la persistance de failles de sécurité récurrentes exploitées par des attaquants aux modes opératoires souvent similaires.

Pour faire face à cette menace, la CNIL rappelle les mesures de base essentielles à adopter pour assurer la sécurité des données :

- Effectuer les mises à jour de sécurité le plus tôt possible ;
- Utiliser des mots de passe robustes et uniques pour chaque compte ;
- Sensibiliser régulièrement les utilisateurs aux risques et à la protection des données ;
- Sécuriser l'accès à la messagerie professionnelle ;
- Réaliser des sauvegardes régulières des données.

https://www.cnil.fr/fr/rapport-annuel-2024

Cybersécurité et protection des données : la CNIL renforce ses contrôles auprès des collectivités territoriales en 2025

La CNIL dispose du pouvoir de contrôler l'ensemble des acteurs traitant des données à caractère personnel. En 2024, elle a ainsi mené 321 contrôles.
Chaque année, l'autorité décide de porter son attention sur des grandes thématiques identifiées en raison de leur impact sur la vie privée des personnes. En 2025, la CNIL concentre son attention sur quatre grandes thématiques :

- La collecte de données par le biais des applications mobiles ;
- Les traitements de données par l'administration pénitentiaire ;
- Les conditions de mise en œuvre du droit à l'effacement ;
- **La cybersécurité des collectivités territoriales.**

Ce dernier axe revêt une importance particulière dans un contexte de hausse des violations de données constaté par la CNIL en 2024 (+20% par rapport à 2023). Les collectivités territoriales, compte-tenu du volume et de la nature souvent sensible des données qu'elles traitent, apparaissent comme particulièrement exposées aux risques.

C'est à ce titre, et dans le cadre de l'entrée en application de la directive NIS2, que la CNIL souhaite renforcer son action sur cette thématique.

https://cnil.fr/fr/les-controles-de-la-cnil-en-2025

Sanctions de la CNIL : 10 décisions rendues en 2025

Depuis le 1er janvier 2025, la CNIL a prononcé dix sanctions dans le cadre de sa procédure simplifiée, pour un montant total de 104 000 €.

Ces sanctions couvrent principalement trois thématiques :

- **Surveillance des salariés (vidéosurveillance, géolocalisation des véhicules…)** : La CNIL rappelle qu'un employeur ne peut exercer une surveillance continue de ses employés. Des garanties doivent impérativement être mises en place afin de respecter leur vie privée dans le cas où des dispositifs de vidéosurveillance ou de géolocalisation sont mis en œuvre.
- **Sécurité des données** : Une société a été sanctionnée pour la faiblesse des mots de passe protégeant son système de vidéosurveillance. Le mot de passe, composé de dix caractères, n'avait jamais été modifié, et ce malgré les changements de personnel ayant accès au système.
- **Violation de données et information des personnes concernées** : La CNIL souligne que toute violation de données présentant un risque pour les droits et libertés des personnes doit être déclarée. Si ce risque est jugé élevé, les personnes concernées doivent également en être informées.

https://www.cnil.fr/fr/dix-nouvelles-sanctions-2025-procedure-simplifiee

Rentrée scolaire : la CNIL rappelle les bonnes pratiques pour l'affichage des listes de classes

À l'approche de la rentrée ou en fin d'année scolaire, il est courant que les établissements scolaires, du primaire au secondaire, publient les listes de répartition des élèves dans les classes. Cependant, cette pratique n'est pas sans risques pour la vie privée des élèves.

Quels sont les risques ?
La CNIL alerte sur certains dangers liés à l'affichage des listes de classes, notamment lorsque celles-ci sont visibles depuis l'extérieur de l'établissement :

- L'affichage extérieur permet de localiser un enfant tout au long de l'année scolaire.
- Cette pratique peut poser problème dans des situations sensibles, par exemple en cas de retrait de l'autorité parentale à l'un des parents.

Quelles bonnes pratiques adopter ?

Afin de protéger au mieux les données personnelles des élèves, la CNIL recommande les mesures suivantes :

- **Limiter le nombre de personnes ayant accès à l'affectation de l'élève dans sa classe**.

Lorsque cela est possible, la CNIL préconise aux établissements d'éviter d'afficher les listes scolaires à l'extérieur du bâtiment. Plusieurs alternatives peuvent être envisagées :

- Affichage à l'intérieur du bâtiment
- Information de l'affectation par courriel auprès des parents de l'élève

Dans le cas où un affichage extérieur est tout de même réalisé, la CNIL recommande :

- De limiter l'affichage à une courte période
- De limiter les noms des élèves à leur seul prénom (éventuellement avec l'initiale du nom de famille lorsque c'est nécessaire)
- De traiter en amont les cas particuliers pouvant conduire à enlever un nom de la liste (risques spécifiques).

- **Informer les parents en amont de l'affichage, afin que ceux-ci puissent s'y opposer**

- **N'afficher que les informations strictement nécessaires sur la liste scolaire**, conformément au principe de minimisation des données (par exemple, ne pas indiquer le 2e prénom).

https://cnil.fr/fr/rentree-scolaire-et-affichage-des-listes-des-classes-quelles-sont-les-bonnes-pratiques

Focus : la sécurité des données

Dans le cadre de leurs missions, les collectivités territoriales et les établissements publics manipulent de nombreuses données à caractère personnel. La protection de ces données est essentielle pour garantir le respect de la vie privée des administrés et des usagers.

Conformément au RGPD, cette exigence de sécurité impose aux responsables de traitement de mettre en place des mesures adaptées, qu'elles soient physiques, logiques ou organisationnelles, en fonction des spécificités de chaque traitement et des risques associés.

La sécurité des données doit être abordée sous les trois angles suivants :

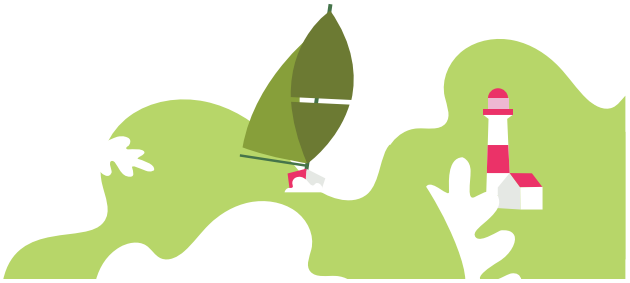
- La confidentialité des données : les données ne doivent être accessibles qu'aux personnes autorisées
- L'intégrité des données : les données ne doivent pas être altérées ou modifiées de manière non autorisée
- La disponibilité des données : les données doivent être en permanence accessibles pour les personnes autorisées.

Toute atteinte à l'un de ces trois principes constitue une violation de données.

Pour prévenir ces risques, différents types de mesures peuvent être mises en place. Vous trouverez ci-dessous quelques exemples de mesures pouvant être mises en place (liste non exhaustive) :

Mesures physiques

- Installation d'alarmes anti-intrusion ;
- Verrouillage des locaux ;
- Fermeture des bureaux en cas d'absence ;
- Rangement des dossiers contenant des données dans des placards fermant à clé.



Mesures logiques

- Mise en place d'une politique de mots de passe et de gestion des accès : identifiant personnel par utilisateur, mot de passe robuste (un outil dédié est disponible sur le site de la CNIL : Générer un mot de passe solide) ;
- Sécurisation des postes de travail, par exemple via un verrouillage automatique après un certain temps d'inactivité ;
- Protection du réseau contre les attaques extérieures (antivirus, pare-feu) ;
- Prévention de la perte de données par des sauvegardes régulières et un stockage sécurisé.

Mesures organisationnelles

- Définir une politique d'accès aux données : gestion des droits selon les mouvements de personnel et révision régulière des accès ;
- Sensibilisation des utilisateurs, notamment via une charte informatique ;
- Mise en place d'une politique de gestion des incidents, comme une procédure en cas de perte ou de vol de données personnelles.

Enfin, il est recommandé de se rapprocher de votre service informatique, de votre prestataire et de votre Délégué à la protection des données pour être conseillé sur les mesures les plus adaptées à chaque traitement de données.

Pense-bête

La rentrée scolaire approche, pensez à mettre en conformité vos formulaires d'inscription et à rédiger vos fiches de registre !

N'hésitez pas à contacter votre Délégué à la protection des données pour qu'il vous accompagne.

EPD
ÉQUIPE PROTECTION DES DONNÉES

Service protection des Données
Direction Développement Numérique
et Assistance Métiers
02 96 58 63 66
cil@cdg22.fr