EPD
ÉQUIPE PROTECTION DES DONNÉES

CDG 22
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 2026

Municipales 2026 : La CNIL dresse le bilan de son observatoire des élections

À l'occasion des élections municipales de mars 2026, la CNIL a dressé le bilan de son observatoire des élections, dans un contexte marqué par l'entrée en vigueur, en octobre 2025, du règlement européen sur la transparence et le ciblage de la publicité politique. La CNIL fait le bilan suivant :

• Entre fin janvier et le second tour en mars dernier, 739 signalements ont été enregistrés, en baisse par rapport à 2020. La majorité concerne des opérations de prospection par SMS (63 %), devant les courriers, courriels et appels téléphoniques.
• Parallèlement, 81 plaintes ont été instruites, portant principalement sur l'origine des données utilisées et sur des soupçons de détournement de finalité, notamment pour des candidats sortants.
• Enfin, la CNIL a engagé quatre contrôles ainsi qu'une procédure de sanction simplifiée à l'encontre d'un candidat n'ayant pas répondu à une demande d'exercice des droits, rappelant les obligations en matière de respect des droits des personnes.

Rapport annuel 2025, une hausse des plaintes et des sanctions

La CNIL a publié en mai 2026 son rapport annuel 2025, revenant sur une année marquée par une intensification de ses actions en matière d'accompagnement, de contrôle et de sensibilisation, dans un contexte d'essor des enjeux liés à l'intelligence artificielle et à la cybersécurité.

L'année 2025 se distingue par une hausse record des plaintes, atteignant 20 150 dossiers contre 17 772 en 2024, ainsi qu'un niveau inédit de sanctions, avec 83 décisions pour un montant total d'environ 487 millions d'euros. Plusieurs établissements publics ont été sanctionnés pour défaut de sécurité des données, entraînant une amende administrative allant de 20 000 à 5 millions d'euros assortie d'une injonction de mise en conformité. D'autres ont été rappelés à leur obligation de traiter les données de façon licite, notamment dans le cadre de la vidéoprotection, ainsi que de garantir une information des personnes.

Parallèlement, 323 contrôles ont été réalisés, portant notamment sur les traceurs, la cybersécurité des collectivités ou encore le respect des droits des personnes (en particulier le droit à l'effacement).
L'activité de la CNIL a également été marquée par une augmentation significative des violations de données, avec plus de 6 000 notifications, dont près de la moitié liée à des actes de piratage. Ces enjeux de cybersécurité représentent désormais une part importante des contrôles et des sanctions prononcées.

En matière d'accompagnement, la CNIL a poursuivi le développement de ses outils à destination des professionnels, avec de nombreuses consultations publiques, publications pratiques et activités de conseil, tout en s'impliquant dans la régulation émergente de l'intelligence artificielle.

Cyberattaque : le rôle clé du sous-traitant en cas de violation de données

Une cyberattaque touchant un prestataire informatique (sous-traitant) d'une collectivité, qu'il s'agisse par exemple d'un éditeur de logiciels ou d'un hébergeur, peut avoir des conséquences directes sur les données personnelles qui lui sont confiées. Elle est notamment susceptible d'entraîner une violation de données à caractère personnel.

Pour rappel, une violation de données à caractère personnel est un incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée ou l'accès non autorisé à des données personnelles.

Lorsqu'une cyberattaque vise un sous-traitant et compromet des données qu'il traite pour le compte d'une collectivité, il ne s'agit pas seulement d'un incident technique affectant le prestataire. Cet événement peut également engager les obligations de la collectivité en sa qualité de responsable de traitement.

En cas de violation de données affectant les traitements réalisés pour le compte de la collectivité, le sous-traitant est tenu de respecter plusieurs obligations. Il doit notamment informer le responsable de traitement dans les meilleurs délais afin de lui permettre de satisfaire à ses propres obligations, notamment documenter l'incident, notifier la violation à la CNIL lorsque cela est requis et, le cas échéant, informer les personnes concernées. Le sous-traitant doit également assister le responsable de traitement dans la gestion de l'incident et dans l'accomplissement des démarches de notification.

La gestion des violations de données impliquant un prestataire doit être encadrée contractuellement par les clauses de sous-traitance relatives à la protection des données personnelles. Ces clauses définissent notamment les modalités de notification des incidents, les obligations d'assistance du sous-traitant, les mesures de sécurité attendues ainsi que les procédures à mettre en œuvre afin de garantir une réaction rapide et coordonnée entre le responsable de traitement et son sous-traitant.

La CNIL a publié en mai dernier un article illustrant concrètement le rôle central du sous-traitant dans la gestion d'une cyberattaque et des violations de données qui peuvent en découler.

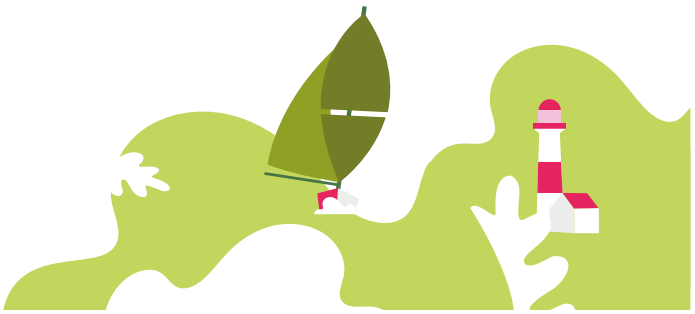
Sécurité des données : la CNIL publie une nouvelle fiche

Dans une nouvelle fiche dédiée, la CNIL rappelle les règles essentielles pour assurer la sécurité des données, dans un contexte où toutes les organisations sont exposées à des cyberattaques et où la mise en place de mesures de sécurité est incontournable, voire nécessaire.

Elle préconise l'adoption de mesures simples mais efficaces, comme l'utilisation de mots de passe robustes, la double authentification, la mise à jour régulière des systèmes, la réalisation de sauvegardes ou encore la sensibilisation des collaborateurs, ces premières actions permettant de réduire significativement les risques.

Le RGPD constitue également un levier de sécurité à travers les principes de minimisation et de limitation de la conservation, qui visent à réduire le volume de données exposées en cas d'incident.

Enfin, en cas de violation de données, la CNIL rappelle les réflexes essentiels à adopter : isoler le système concerné, conserver les preuves, ne pas payer de rançon, alerter les acteurs compétents et notifier la CNIL lorsque des données personnelles sont impactées.



Pour en savoir plus

• Municipales 2026, la CNIL dresse le bilan de son observatoire : Municipales 2026 : le bilan de l'observatoire des élections de la CNIL | CNIL
• Rapport annuel 2025 : une hausse des plaintes et des sanctions : Rapport annuel : le bilan et les actions marquantes de la CNIL en 2025 | CNIL
• Cyberattaque : le rôle clé du sous-traitant en cas de violation de données : Cyberattaque : le sous-traitant au centre de la crise | CNIL
• Sécurité des données : La CNIL publie une nouvelle fiche : Sécurité des données : les règles essentielles pour protéger les données et votre activité | CNIL

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