CNIL, communiqué du 9 novembre 2026, Cybersécurité des collectivités territoriales : la CNIL prononce dix sanctions

Source officielle : https://www.cnil.fr/fr/sanctions-cybersecurite-collectivites-territoriales

Cybersécurité des collectivités territoriales : la CNIL prononce dix sanctions

09 novembre 2026

En novembre 2026, la CNIL a prononcé dix sanctions simplifiées à l'encontre de collectivités territoriales et d'un établissement public, pour des manquements relatifs à la cybersécurité.

Le contexte

Les collectivités territoriales (communes, départements, régions) traitent un grand nombre de données, pour certaines sensibles (gestion de l'état civil des usagers, versement de prestations sociales, données financières, ou encore données concernant des mineurs).

C'est pourquoi, face au nombre croissant de cyberattaques, la CNIL a décidé, en 2025, de faire de la cybersécurité des collectivités territoriales l'une de ses thématiques annuelles de contrôle.

Plusieurs collectivités territoriales, acteurs publics, ainsi que leurs prestataires, ont ainsi été contrôlés, afin de vérifier que les mesures de sécurité, techniques, organisationnelles et physiques, mises en œuvre pour protéger les données des administrés étaient suffisantes.

Les contrôles ont révélé plusieurs manquements au RGPD et à la loi Informatique et Libertés, entraînant dix sanctions financières dans le cadre de la procédure simplifiée.

Les manquements sanctionnés

Des manquements à la sécurité (article 32 du RGPD)

Les manquements relevés témoignent de la diversité des failles pouvant affecter la sécurité d'un système d'information.

Il a notamment été constaté que :

les modalités d'authentification permettant aux agents des collectivités de se connecter à distance (notamment en télétravail) n'étaient pas suffisamment robustes, en particulier pour ceux disposant de privilèges élevés (absence d'authentification multifacteur pour les administrateurs) ;

certains prestataires extérieurs (par exemple, des éditeurs de logiciels) pouvaient accéder au réseau des collectivités de manière permanente, sans y être autorisés au cas par cas, ou via des comptes partagés entre plusieurs salariés ;

les mesures déployées afin de détecter les comportements anormaux étaient inefficaces (journalisation incomplète ou absence d'exploitation en temps réel ou à court terme des journaux) ;

le cloisonnement du réseau était insuffisant, ce qui pouvait étendre l'impact d'une violation à plusieurs segments du réseau ;

certains systèmes d'exploitation utilisés par des serveurs étaient obsolètes : ils n'étaient plus maintenus à jour par leur éditeur et ne bénéficiaient donc pas des correctifs de sécurité adéquats ;

certains mots de passe utilisés étaient insuffisamment robustes, transmis en clair aux usagers ou stockés dans des conditions ne permettant pas de garantir leur confidentialité.

L'ensemble de ces manquements exposaient les données, parfois sensibles, des administrés à des risques de perte de confidentialité. Certaines des collectivités contrôlées ont d'ailleurs subi une ou plusieurs violations de données, qui auraient pu être évitées si les mesures adéquates avaient été prises.

Plusieurs décisions relèvent également que les systèmes d'information des collectivités, utilisés notamment pour échanger en ligne avec les administrés, ne faisaient pas l'objet d'une homologation de sécurité avant leur mise en service, alors que le référentiel général de sécurité (RGS) l'exige. Cette homologation, rendue obligatoire, permet aux autorités administratives d'assurer la mise en conformité de leur système d'information.

Un manquement à l'obligation d'effectuer une analyse d'impact (article 90 de la loi Informatique et Libertés)

Plusieurs collectivités ont été sanctionnées pour ne pas avoir réalisé d'analyse d'impact (AIPD) préalablement à la mise en œuvre des systèmes de vidéoprotection installés sur la voie publique, qui constituent « une surveillance systématique à grande échelle d'une zone accessible au public ».

Les sanctions prononcées

Des amendes allant de 3 000 € à 20 000 € (maximum légal pour ce type de procédure) ont été prononcées. Ces montants tiennent notamment compte du nombre de manquements relevés et de leur gravité, des catégories de données traitées (données de mineurs, coordonnées bancaires, etc.), du budget de chacune des collectivités et du nombre de personnes concernées. Ils tiennent également comptent des mesures prises pour se mettre en conformité.

La CNIL, qui consacre en 2026 la moitié de ses contrôles et actions répressives à la sécurité des données, poursuivra ses vérifications afin de s'assurer que les données, parfois sensibles, des administrés sont traitées dans des conditions de sécurité satisfaisantes par les collectivités territoriales et leurs prestataires. D'autres procédures sont actuellement en cours et pourraient mener, en cas de manquements, à des sanctions, des mises en demeure ou des rappels aux obligations.

En parallèle, la CNIL poursuit ses actions de sensibilisation et d'accompagnement des collectivités territoriales en matière de cybersécurité. Cette double action de contrôle et d'accompagnement s'inscrira également dans la préparation de l'entrée en application de la directive NIS2, en cours de transposition, qui met à la charge notamment des collectivités territoriales de nouvelles exigences en matière de sécurité informatique.

Texte de référence

Article 32 du RGPD (sécurité)

Article 90 de la loi Informatique et Libertés (AIPD)