CYBERACTU'

Le magazine du service « Protection des données » du Centre de gestion du Gard

octobre 2025

Cybersécurité et résilience

Ce que le projet de loi change pour les collectivités

Dossier page 18

Le point archives :
L'impact du projet de loi « résilience »

Les conseils du DPO :
L'utilisation de drones

Événement :
Colloque « cybersécurité et collectivité »

SERVICE PROTECTION DES DONNÉES

CENTRE DE GESTION
DU GARD

Contactez-nous

04 66 38 86 86
cdg30@cdg30.fr

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

Contactez-nous

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

Contactez-nous

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

Contactez-nous

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

SOMMAIRE

ÉDITO

Octobre 2025. Tandis que les menaces numériques se multiplient et que les collectivités territoriales deviennent des cibles de plus en plus fréquentes, un tournant législatif s'annonce : le projet de loi sur la résilience des infrastructures critiques place désormais les communes, même les plus petites, au cœur de la stratégie nationale de cybersécurité. Ce numéro de notre magazine s'inscrit pleinement dans cette actualité. Il propose un dossier central clair et opérationnel sur les nouvelles obligations à venir, les défis spécifiques des petites communes, et surtout les leviers d'action concrets pour se préparer sans se perdre dans la technicité. Car la sécurité numérique n'est pas qu'une affaire de spécialistes : elle concerne les élus, les agents, les partenaires, et les citoyens.

Pierre BONANNI – Ana VEGA

Sarah ROMAN

Contacts

Service « Protection des données »

☎ : 04 66 38 86 86

@ : dpd@cdg30.fr

CDG 30 CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD

PROJET DE LOI RÉSILIENCE : LE SEUIL DÉMOGRAPHIQUE, UNE FAUSSE FRONTIÈRE POUR LES COMMUNES ?

Alors que le projet de loi sur la résilience des infrastructures critiques poursuit son parcours parlementaire *(voir dossier page XX),* une question revient avec insistance dans les réunions d'élus et les échanges entre collectivités : Les petites communes seront-elles concernées par les nouvelles obligations de cybersécurité ?

La réponse officielle, pour l'instant, repose sur un chiffre : 30 000 habitants. Ce seuil, inscrit dans l'article 8 du projet de loi, délimite les collectivités considérées comme « *entités essentielles* » au sens de la directive NIS 2. En dessous, les obligations seraient allégées, voire différées. Mais cette frontière est loin d'être étanche…

Un amendement récent (n°000076, déposé le 4 septembre 2025) propose de supprimer ce seuil démographique, au motif qu'il ne reflète pas la réalité des risques. En effet, une commune de 2 000 habitants peut gérer un réseau d'eau potable, une cantine scolaire, un service périscolaire ou un état civil informatisé. Ces services sont tout aussi critiques que ceux d'une grande ville, et tout aussi exposés aux risques de cyberattaques. L'amendement souligne que la taille ne protège pas du risque, et que la cybersécurité doit s'appuyer sur les fonctions exercées, non sur le nombre d'habitants.

Même si le seuil reste inscrit dans le texte à ce jour, le gouvernement conserve la possibilité de désigner des communes comme « *entités essentielles* » par décret, en fonction de leurs activités. De plus, environ 1 500 collectivités ont déjà été identifiées comme concernées par les obligations de base liées à la directive NIS 2, sans condition de taille. En clair : les petites communes doivent se préparer, car elles pourraient être incluses dans le périmètre réglementaire dès 2026.

Affaire à suivre, donc…

VIDÉOSURVEILLANCE SCOLAIRE : CE QUE LES COLLECTIVITÉS DOIVENT SAVOIR

À l'heure où les collectivités territoriales cherchent à renforcer la sécurité dans les établissements scolaires, la tentation d'installer des caméras se fait de plus en plus fréquente. Mais entre vidéoprotection, vidéosurveillance et caméras dites « intelligentes », les règles sont strictes — et souvent méconnues. La CNIL vient justement de mettre à jour sa fiche pratique sur le sujet, et elle mérite toute l'attention des élus locaux.

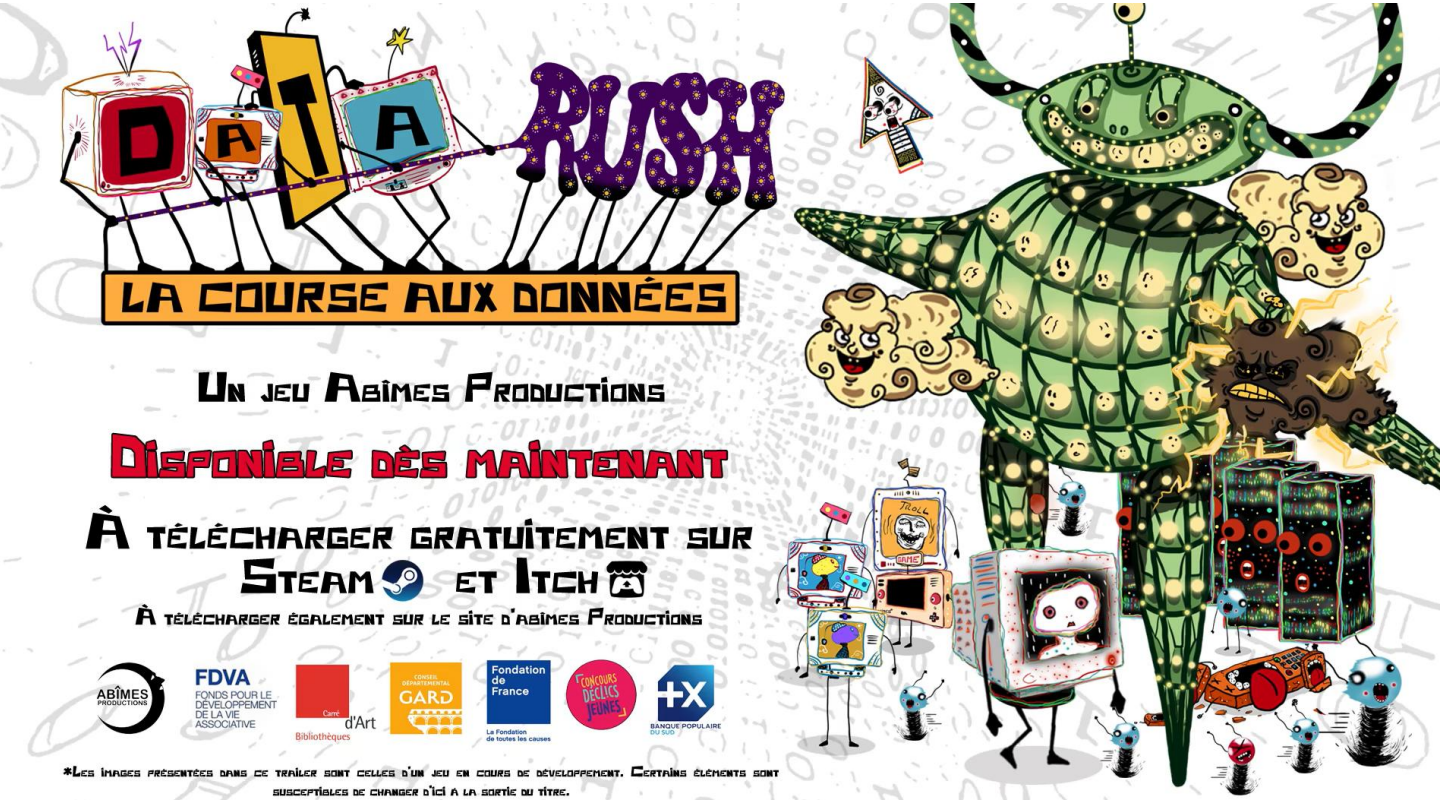
Prévenir les intrusions, les violences, les dégradations : les objectifs sont légitimes. Mais les dispositifs vidéo ne peuvent pas tout faire, et surtout, ils ne peuvent pas tout filmer. La CNIL rappelle que les caméras sont interdites dans les lieux de vie : salles de classe, cantine, cour de récréation, toilettes… sauf cas très exceptionnels. Filmer les abords de l'école ou les couloirs est possible, mais cela dépend du type de dispositif et du cadre juridique applicable.

Trois types de dispositifs sont ainsi à bien distinguer : la vidéoprotection, tout d'abord, qui concerne les abords extérieurs de l'établissement. Elle relève du Code de la sécurité intérieure et nécessite une autorisation préfectorale.

La vidéosurveillance, quant à elle, concerne les espaces intérieurs (halls, couloirs, accès). Elle relève du RGPD et de la loi Informatique et Libertés. Elle doit être proportionnée, justifiée, et ne pas porter atteinte à la vie privée. Enfin, les caméras « augmentées », qui sont celles avec reconnaissance de formes ou de comportements, sont interdites dans les établissements scolaires, faute de base légale. Ainsi, ce que les collectivités devront faire pour respecter la réglementation, suit un ensemble de recommandations édictées par la CNIL. La première chose à faire sera d'informer clairement les usagers, à savoir les élèves, leurs parents, et même le personnel de la présence des caméras, avec des affiches visibles et des explications adaptées.

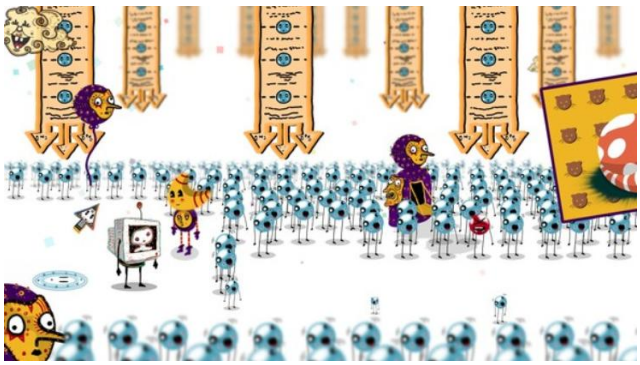
Il conviendra également de limiter l'accès aux images. Seules des personnes habilitées et formées peuvent consulter les enregistrements. Enfin, il ne faudra pas oublier les durées de conservation des images, qui sont de quelques jours en général, sauf procédure en cours. Il ne faudra pas oublier d'associer le délégué à la protection des données dès le début du projet.

Ce guide de la CNIL permet aux communes et intercommunalités de sécuriser leurs projets sans risquer de sanction, mais aussi d'éviter les erreurs fréquentes, comme filmer les cours ou installer des caméras sans autorisation. Il s'inscrit pleinement dans la logique de conformité RGPD et de prévention des risques, que les collectivités doivent désormais intégrer dans leur gestion quotidienne.



Data Rush : La course aux données est un jeu vidéo pédagogique dans lequel vous prenez les commandes d'un avatar personnalisable et vivrez une aventure mêlant mystère et humour au cœur des espaces numériques, à la recherche de vos données perdues.

Il a pour objectif d'apprendre à se protéger et à gérer ses données sur les espaces numériques tout en s'amusant. Le jeu fait s'alterner des phases d'exploration dans des niveaux réalisés et animés en 2D intégralement à la main, des interactions avec des personnages ainsi que des phases d'énigmes, des jeux pour tester ses connaissances et des puzzles.



Développé par l'association de conception et de production de projets culturels, artistiques et pédagogiques **Abîmes Productions**, ce jeu de sensibilisation est disponible **gratuitement** en téléchargement libre (*Free-to-play*).

Jeu disponible gratuitement sur

itch.io STEAM®

1912 : Naufrage du Titanic

Le Titanic n'aurait pas connu une fin aussi glaciale si son GPS avait été mis à jour.

À défaut de réécrire l'Histoire, prenez la vôtre en main...

Faites vos mises à jour régulièrement pour corriger les failles de sécurité.

CYBER MOIS

CYBERMOIS.GOUV.FR

Caméras dissimulées : la CNIL sanctionne La Samaritaine — un signal fort pour les collectivités

Le 12 septembre 2025, la CNIL a rendu publique une sanction de 200 000 € à l'encontre de La Samaritaine, célèbre enseigne parisienne, pour avoir utilisé des caméras dissimulées dans ses locaux. Cette décision rappelle fermement que la vidéosurveillance ne peut se faire en cachette et qu'elle doit respecter les droits fondamentaux des personnes filmées.

Que reproche la CNIL ? La Samaritaine avait installé des caméras dans des zones non accessibles au public (réserves, locaux techniques…), mais sans informer les salariés ni les prestataires. Ces caméras étaient dissimulées, et leur usage n'était ni justifié ni proportionné. La CNIL a relevé plusieurs manquements, notamment une absence d'information des personnes filmées, une surveillance excessive et injustifiée, un non-respect du principe de minimisation des données et un défaut de consultation du délégué à la protection des données.

Même si l'affaire concerne une entreprise privée, les collectivités territoriales sont directement concernées. Les agents, les prestataires, les élus peuvent être exposés à des dispositifs de surveillance dans les locaux techniques, les ateliers, les bureaux… Installer une caméra dans une salle de pause, un vestiaire ou un bureau sans informer les personnes est illégal, même si l'intention est sécuritaire. Les communes doivent associer leur DPD à tout projet de vidéosurveillance, et s'assurer que les dispositifs sont visibles, justifiés et proportionnés.

Moralité : si vous devez filmer, mieux vaut une caméra bien visible qu'un scénario digne de Mission Impossible… surtout quand la CNIL joue le rôle du spectateur vigilant !

Fraude au virement de la paie : une menace discrète mais bien réelle

La CNIL a récemment mis en lumière un type de fraude encore trop méconnu : l'usurpation d'identité visant à détourner les virements de salaire. Dans le cas présenté, un salarié découvre qu'il n'a pas été payé. L'entreprise réalise alors qu'un faux courriel, imitant son adresse, a demandé un changement de RIB. Le salaire a été versé sur un compte frauduleux, et d'autres agents ont été ciblés de la même manière. Ce scénario, malheureusement de plus en plus courant, révèle une faille dans les procédures internes de gestion des données personnelles et des flux financiers. Il ne s'agit pas seulement d'un vol, mais d'une violation de données qui engage la responsabilité de l'employeur. La CNIL rappelle que ce type d'incident doit être traité avec rigueur : enquête rapide, information des personnes concernées, et notification si nécessaire. Pour les collectivités territoriales, ce cas est un signal d'alerte. Les services RH, souvent en sous-effectif, doivent redoubler de vigilance face aux courriels suspects et sécuriser les procédures de modification de coordonnées bancaires. La prévention passe par la sensibilisation, la traçabilité et l'implication du délégué à la protection des données dès qu'un doute survient. La fraude au virement de la paie n'est pas une fatalité. C'est un risque que l'on peut contenir, à condition de ne pas le sous-estimer.

Le délégué à la protection des données, un coût ou un levier économique pour les collectivités ?

Longtemps perçu comme une contrainte administrative liée au RGPD, le délégué à la protection des données (ou DPO, de son sigle anglophone *Data Privacy Officer*) s'impose aujourd'hui comme un acteur stratégique, y compris dans les collectivités territoriales. La CNIL, dans son analyse publiée en juillet 2025, démontre que le DPO ne se limite pas à la conformité : il peut générer des bénéfices économiques tangibles pour les organisations.

Une fonction qui réduit les risques… et les coûts

Le premier apport du DPO est évident : il permet d'éviter les sanctions. En anticipant les risques, en encadrant les traitements de données et en sensibilisant les agents, il réduit les probabilités de violation du RGPD. Or, les amendes peuvent être lourdes, même pour les collectivités. Mais au-delà de la sanction, le DPO agit comme un réducteur de coûts indirects : il limite les pertes de temps liées aux incidents, les tensions internes, les erreurs de communication ou les recours des usagers.

Un rôle d'optimisation des pratiques

Le DPO ne se contente pas de dire « non ». Il aide à structurer les projets, à clarifier les responsabilités, à documenter les processus. En cela, il participe à une meilleure gouvernance de l'information. Dans les collectivités, cela se traduit par des gains de temps pour les agents, une meilleure traçabilité des décisions, et une réduction des doublons ou des traitements inutiles.

Par exemple, un DPO qui accompagne la mise en place d'un portail citoyen ou d'un logiciel RH peut éviter des choix techniques coûteux ou non conformes. Il devient alors un facilitateur de projets, et non un frein.

Un vecteur de confiance et de transparence

Dans un contexte de défiance de plus en plus poussé envers les institutions, le DPO incarne une démarche éthique. Il rassure les usagers, valorise les agents, et renforce la légitimité de l'action publique.

Cette confiance peut avoir des effets économiques indirects : meilleure adhésion aux démarches en ligne, réduction des litiges, amélioration de la qualité de service. Pour les élus, le DPO est aussi un atout politique : il montre que la collectivité prend au sérieux les droits des citoyens et la sécurité de leurs données.

Un investissement des plus rentable

La CNIL souligne que les bénéfices du DPO dépassent largement son coût, surtout lorsqu'il est mutualisé. Dans les petites collectivités, le recours à un DPO partagé via le centre de gestion permet de bénéficier de son expertise sans alourdir les charges. C'est une forme d'intelligence collective, qui renforce la résilience des territoires.

En somme, le DPO n'est pas un simple garant du RGPD. Il est un acteur de performance, de prévention et de confiance. Pour les collectivités, il représente une opportunité de professionnaliser la gestion des données, de sécuriser les projets numériques, et de renforcer le lien avec les citoyens ■

Une commune sanctionnée par la CNIL : un signal fort pour les collectivités territoriales

Le 11 septembre 2025, la CNIL a prononcé une sanction de 10 000 euros à l'encontre d'une commune française, dans le cadre d'une procédure simplifiée. Si le nom de la collectivité n'a pas été rendu public, les motifs de la sanction sont clairs et instructifs pour l'ensemble du secteur public local.

Deux infractions majeures au Règlement général sur la protection des données (RGPD) ont été constatées. Ainsi, la commune conservait des données relevant des « *catégories particulières* » (santé, opinions, etc.) au-delà des durées nécessaires à leur finalité. De plus, et bien que pourtant obligatoire pour tout responsable de traitement, le registre de traitements n'était pas tenu, privant la collectivité d'une vision claire de ses obligations et de ses pratiques.

Cette décision rappelle que les collectivités territoriales ne sont pas exemptes des exigences du RGPD. Même en l'absence de plainte ou de violation spectaculaire, des manquements structurels peuvent entraîner des sanctions financières et ternir l'image d'une administration locale.

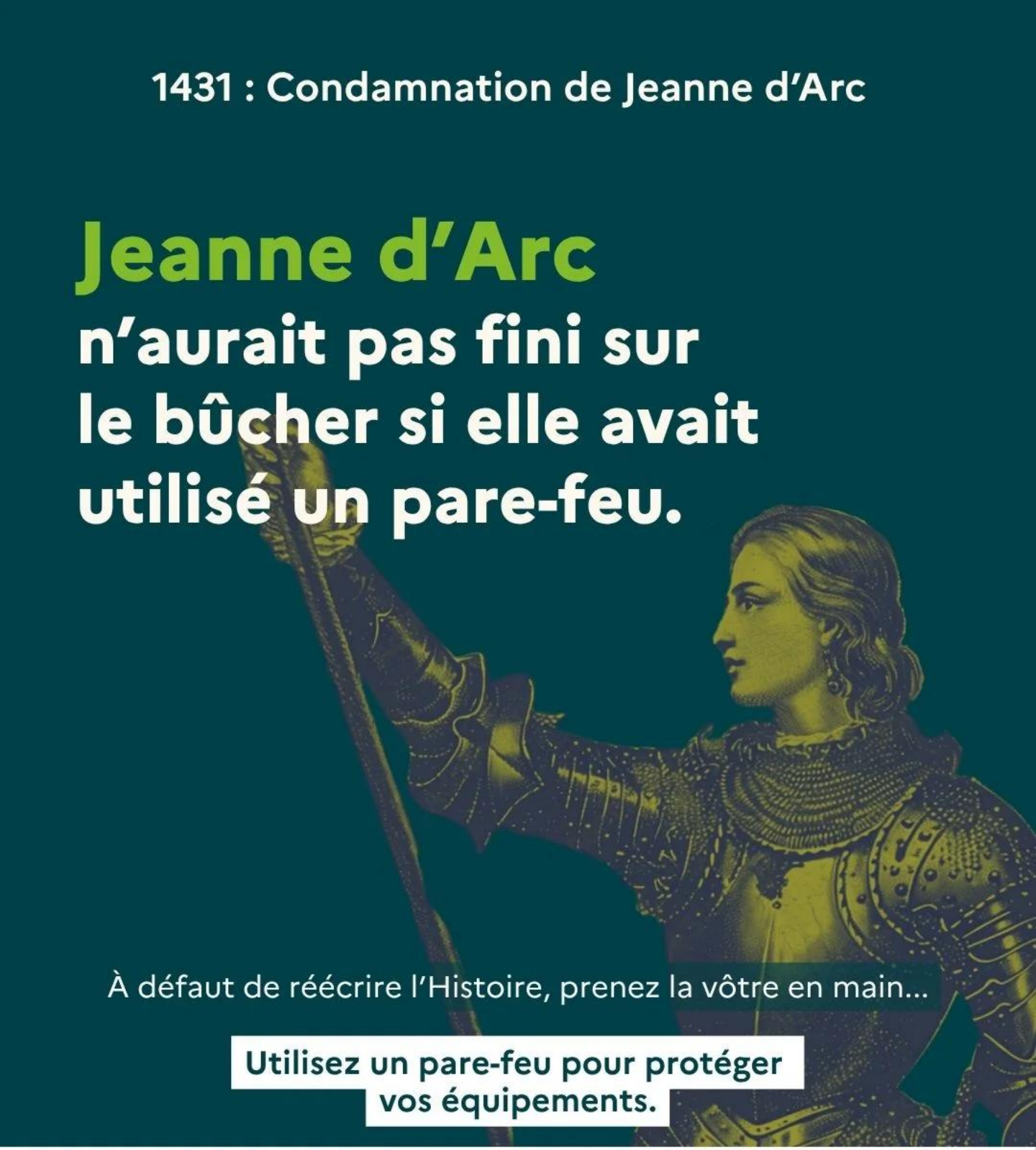
Elle souligne également l'importance de mettre en place une gouvernance des données claire et documentée, mais aussi de sensibiliser les agents au respect de la durée de conservation et de la finalité des traitements. Il est également essentiel de maintenir un registre de traitements à jour, véritable outil de pilotage et de conformité.

Cette affaire peut servir de cas d'école pour renforcer les pratiques locales. Il est essentiel de mener régulièrement un audit interne des durées de conservation et des traitements sensibles (voir même des traitements ordinaires) afin d'assurer une mise à jour du registre de traitements, avec un accompagnement des services. Enfin, la formation ciblée des agents sur les risques liés à la conservation excessive doit être assurée, notamment avec l'appui du délégué à la protection des données et un archiviste pour sécuriser les pratiques de la collectivité.

La conformité RGPD n'est pas une contrainte administrative, mais une garantie de confiance envers les citoyens. Chaque commune, quelle que soit sa taille, a les moyens d'agir.

1431 : Condamnation de Jeanne d'Arc

Jeanne d'Arc n'aurait pas fini sur le bûcher si elle avait utilisé un pare-feu.



À défaut de réécrire l'Histoire, prenez la vôtre en main...

Utilisez un pare-feu pour protéger vos équipements.

CYBER MOIS

CYBERMOIS.GOUV.FR

Les décisions des autorités chargées de la protection des données

11 septembre 2025 : France – 10 000 €

Le 11 septembre 2025, la CNIL a sanctionné une commune française à hauteur de 10 000 euros pour des manquements au RGPD. En cause : la conservation excessive de données sensibles et l'absence de registre des activités de traitement. Cette procédure simplifiée rappelle que les obligations en matière de protection des données concernent toutes les collectivités, quelle que soit leur taille. Cette décision, bien que peu médiatisée, constitue un signal fort pour les administrations locales. Elle invite à renforcer la gouvernance des données et à outiller les agents pour une conformité durable. 👉 *Retrouvez l'analyse complète et les pistes d'action en page 8 du magazine.*

04 août 2025 : Italie – 10 000 €

La CNIL italienne a examiné le dispositif mis en place par la Ville de Venise pour gérer une taxe d'accès à la ville et aux îles de la lagune, en alternative à la taxe de séjour. L'enquête a porté sur les modalités de collecte et de traitement des données personnelles des personnes exemptées ou exclues du paiement. Or, il a été relevé plusieurs violations du RGPD, notamment en matière de minimisation des données, de proportionnalité, de conservation, et de conception respectueuse de la vie privée.

04 août 2025 : Pologne – 7 700 €

L'autorité polonaise de protection des données a infligé une amende de 7 700 euros à un établissement de santé à Pyskowice après le vol du véhicule personnel d'un médecin contenant des dossiers médicaux non sécurisés de huit patients. L'enquête a révélé que l'analyse des risques menée par l'établissement était incomplète et que les procédures de protection des données ne prenaient pas en compte les situations de traitement en dehors des locaux, notamment lors des visites à domicile. Bien que des alertes internes aient été émises dès 2017, aucune mesure concrète n'avait été mise en œuvre avant l'incident. Ce n'est qu'après le vol que l'établissement a mis à jour sa politique de sécurité, formé son personnel et fourni des mallettes verrouillables pour le transport des documents médicaux.

04 août 2025 : Italie – 10 000 €

La CNIL italienne a infligé une amende de 10 000 euros à l'ordre des professions de soins infirmiers de Viterbe. Le responsable du traitement a subi une fuite de données en raison de mesures techniques et organisationnelles insuffisantes pour garantir la sécurité des données.

16 juillet 2025 : Roumanie – 4 000 €

La CNIL roumaine a infligé une amende à l'homme politique et ancien candidat à l'élection présidentielle Côlin Georgescu. Le candidat n'a pas informé les personnes concernées sur son site web du traitement de leurs données et de la manière dont elles pourraient exercer leurs droits

10 JUILLET 2025 : ITALIE – 10 000 €

La CNIL italienne a infligé une amende de 10 000 euros à l'école maternelle « *La Combricola Dei Birichini Di Betty* ». L'autorité territoriale n'acceptait les nouveaux enfants que si ses parents consentaient à ce qu'ils puissent prendre et utiliser des photos d'eux à des fins de communication. Il en est résulté un affichage excessif d'images pour enfants sur Internet, qui ne sont pas conformes aux principes de base du RGPD

10 JUILLET 2025 : ITALIE – 4 000 €

La CNIL italienne a infligé une amende de 4 000 euros à un institut de formation de Monopoli. Le responsable de traitement a en effet publié une liste indiquant le nom des élèves handicapés sur son site Web sans base juridique suffisante

10 JUILLET 2025 : ITALIE – 8 000 €

La CNIL italienne a infligé une amende de 8 000 euros à l'Università degli Studi di Cassino e del Lazio Meridionale. Le responsable du traitement n'a pas supprimé l'adresse électronique d'un ancien employé dans un délai raisonnable et n'a pas non plus répondu de manière adéquate à la demande de l'ancien employé de supprimer ses données

10 JUILLET 2025 : ITALIE – 3 000 €

La CNIL italienne a infligé une amende de 3 000 euros à la commune de Conversano pour ne pas avoir correctement réalisé une analyse d'impact sur la vie privée.

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

ARS de Normandie
08 septembre 2025

ARS des Hauts-de-France
08 septembre 2025

ARS du Pays de la Loire
08 septembre 2025

Muséum national d'histoire naturelle
14 août 2025

Mairie de Poitiers
29 août 2025

Communauté urbaine du Grand Poitiers
29 août 2025

France Travail
Juillet 2025

CNFPT
Juillet 2025

Département de l'Aude
21 août 2025

Centre d'Urgence Cyber
0 800 71 13 13
Numéro gratuit
Cyber'Occ délivre un service gratuit d'assistance, en cas de cyber-incident, aux TPE, PME, ETI, collectivités et associations d'Occitanie.
csirt@cyberocc.fr

** Sur les trois derniers mois*

CDG 30

COLLOQUE

NOUS SOMMES #CYBERENGAGÉS
CYBER MOIS
01 OCT – 31 OCT
ÉDITION 2025

Jeudi 23 octobre 2025
à L'Ombrière Pays d'Uzès
de 9h à 16h

COLLECTIVITÉS ET CYBERSÉCURITÉ

PROTÉGER LES DONNÉES PUBLIQUES

Une journée d'interventions
et ateliers pour renforcer la sécurité
numérique des collectivités

>>>>>

GRATUIT SUR INSCRIPTION EN LIGNE SUR CDG30.FR

AVEC LA PARTICIPATION DU CIG GRANDE COURONNE ET DE LA GENDARMERIE.
ORGANISÉ PAR LE CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD.

>>>>> PROGRAMME

8h30 **Accueil café**

9h00 **Ouverture**

Fabrice Verdier, président du Centre de gestion de la fonction publique territoriale du Gard

9h15 - 12h30 **Interventions**

- L'exfiltration et la commercialisation des données dans les collectivités
- La gestion des cyberattaques : retour d'expérience du CIG de Versailles
- Cyber Gend & élus locaux : construire une cybersécurité partagée ; avec la Gendarmerie nationale
- Manager la sécurité : les étapes techniques et humaines

12h30 **Pause buffet déjeunatoire**

14h00 **Table ronde**

L'impact de l'application des mesures de sécurité au sein des collectivités

Avec la participation de plusieurs collectivités et établissements publics du Gard

15h00 et 15h30 **Sessions d'ateliers : *1 ou 2 atelier(s) à choisir lors de l'inscription***

- Atelier 1 : la gestion de la liste électorale à l'approche des élections
- Atelier 2 : Collectivités & IA : le futur commence ici
- Atelier 3 : Savoir anticiper pour se prémunir

16h00 **Fin**

>>>>> Informations pratiques

Gratuit
Sur inscription obligatoire en ligne sur cdg30.fr

L'Ombrière Pays d'Uzès
3, place de la Croix des Palmiers
30700 Uzès

Parking gratuit du côté du stade du Refuge (route de Nîmes).

CYBERSÉCURITÉ ET RÉSILIENCE : CE QUE LE PROJET DE LOI CHANGE POUR LES PETITES COLLECTIVITÉS

Les cybermenaces ne connaissent ni frontières ni tailles de commune. En 2025, les petites collectivités territoriales sont devenues des cibles privilégiées pour les attaques informatiques, souvent faute de moyens suffisants pour se protéger efficacement. Face à cette réalité, le gouvernement français engage une réforme d'ampleur avec le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

L'Assemblée Nationale, actuellement en discussion du projet de loi

Ce texte, en cours d'examen à l'Assemblée nationale, vise à transposer plusieurs directives européennes, dont NIS 2 (Network and Information Système Security n°2 – que l'on peut traduire par « Sécurité des réseaux et de l'information ») et REC (Résilience des entités critiques), et à imposer de nouvelles obligations aux entités publiques, y compris pour les collectivités.

Désignation d'un référent en cybersécurité, documentation des incidents, audits réguliers : autant de mesures qui pourraient bouleverser les pratiques locales dès 2026. Mais comment les petites communes peuvent-elles anticiper ces changements sans sombrer sous la complexité réglementaire ? Ce dossier décrypte les enjeux du projet de loi, identifie les impacts concrets pour les collectivités de proximité, et propose des leviers d'action adaptés à leurs réalités.

Un texte stratégique à portée européenne

Le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité ne s'inscrit pas dans une dynamique franco-française : il est directement issu d'un cadre européen ambitieux visant à renforcer la sécurité numérique des États membres.

Trois directives adoptées par l'UE en décembre 2022 constituent le socle de cette réforme. Tout d'abord, la directive NIS 2 (*Network and Information Security n°2*), qui élargit considérablement le périmètre des entités qui seront concernées par les obligations de cybersécurité, en intégrant les collectivités territoriales, les établissements publics et les opérateurs de services essentiels.

Ensuite, vient REC (*Resilience of Critical Entities*). Elle impose aux États membres de garantir la continuité des services critiques en cas de crise, qu'elle soit cyber, climatique ou géopolitique.

Enfin, la directive DORA (*Digital Operational Resilience Act*) qui, bien que centrée sur le secteur financier, complète

le dispositif en encadrant la résilience numérique des infrastructures pouvant être interconnectées.

Le projet de loi actuellement examiné à l'Assemblée nationale vise donc à anticiper cette échéance, en adaptant les obligations aux réalités du terrain français. Ce texte marque un tournant : il reconnaît que les collectivités territoriales, même les plus petites, sont des maillons essentiels de la chaîne de sécurité nationale. En gérant des services comme l'eau potable, l'état civil, les écoles ou les déchets, elles deviennent des acteurs critiques dont la vulnérabilité peut entraîner des conséquences systémiques. En intégrant les communes dans le périmètre des entités jugées « essentielles » ou même « importantes », le législateur envoie un signal fort : la cybersécurité n'est plus une option, mais une responsabilité partagée, du niveau national jusqu'au plus local.

Les nouvelles obligations pour les collectivités

Le projet de loi prévoit plusieurs nouvelles règles pour aider les communes à mieux se protéger contre les attaques informatiques. Même si certaines communes fournissent déjà des efforts, ces règles deviendront bientôt obligatoires pour toutes celles qui gèrent des services importants pour les habitants :

Mettre en place des protections de base

Chaque commune devra installer des outils simples mais efficaces pour sécuriser ses ordinateurs :

- Séparer les accès entre les différents services (exemple : ne pas mélanger les accès de la cantine avec ceux de l'état civil)
- Utiliser des mots de passe solides et bien gérer les droits d'accès
- Faire les mises à jour régulièrement pour éviter les failles
- Surveiller les alertes et les anomalies (par exemple, une connexion inhabituelle)

Ces mesures doivent être notées et suivies dans le temps.

Tenir un registre des incidents

Si un problème survient (comme un virus ou une tentative de piratage), la commune devra le noter dans un registre :

- Ce qui s'est passé
- Quand et comment cela a été découvert
- Ce qui a été fait pour y répondre

Ce registre permettra de mieux comprendre les risques et d'améliorer les réactions en cas de nouvelle attaque.

Faire vérifier régulièrement ses pratiques

Des contrôles devront être réalisés par des professionnels agréés pour vérifier que la commune respecte bien les règles. Ces contrôles permettront :

- De repérer les points faibles
- De proposer des améliorations
- De rassurer les élus et les habitants sur la sécurité des services.

Désigner un référent cybersécurité

Chaque commune devra nommer une personne chargée de suivre les questions de sécurité informatique. Cette personne pourra être :

- Un agent de la commune
- Un référent mutualisé via le centre de gestion ou l'intercommunalité

Son rôle sera de :

- Veiller à ce que les règles soient appliquées
- Aider les agents et les élus à comprendre les bons réflexes
- Être le point de contact en cas de problème.

Ces nouvelles obligations ne visent pas à compliquer la vie des communes, mais à les aider à mieux se défendre face aux risques numériques. Pour les petites collectivités, cela peut sembler ambitieux, mais des solutions existent pour mutualiser les efforts et s'appuyer sur des partenaires compétents.

Les défis spécifiques des petites communes

Si le projet de loi vise à renforcer la sécurité numérique de toutes les collectivités, les petites communes sont confrontées à des difficultés particulières. Manque de moyens, faible technicité, isolement… autant de réalités qui rendent l'application des nouvelles règles plus complexe.

Dans une petite mairie, le secrétariat gère à la fois l'état civil, les élections, la comptabilité, les demandes d'urbanisme… Il est rare qu'un agent soit dédié à la maintenance informatique ou à la cybersécurité. Résultat : les risques sont souvent mal identifiés, et les bonnes pratiques peu appliquées faute de temps ou de formation. Beaucoup de communes utilisent des logiciels métiers installés depuis plusieurs années, sans mises à jour régulières. Les mots de passe sont parfois partagés entre agents, et les sauvegardes ne sont pas automatiques. Ces failles techniques peuvent être exploitées par des attaquants, même sans grande expertise. Le RGPD, les registres de traitement, la gestion des incidents… Ces notions restent floues pour de nombreux élus et agents. Pourtant, une mauvaise gestion des données ou une négligence en matière de sécurité peut engager la responsabilité de la commune.

Les petites communes ont parfois l'impression d'être livrées à elles-mêmes. Les textes sont complexes, les ressources rares, et les interlocuteurs techniques peu accessibles. Ce sentiment peut freiner l'action, alors même que des solutions existent. Heureusement, des leviers permettent de surmonter ces défis.

Des leviers d'actions adaptés aux petites collectivités

Face aux nouvelles obligations du projet de loi, les petites communes peuvent se sentir dépassées. Pourtant, il existe des solutions concrètes et accessibles pour se mettre en conformité sans alourdir la charge de travail ni exploser les budgets.

Plutôt que d'agir seules, les communes peuvent s'appuyer sur plusieurs structures destinées à les accompagner. Ainsi, les centres de gestion (CDG) sont souvent dotés d'un service RGPD mutualisé. Et certains éditent même des magazines très intéressants sur le sujet de la protection des données où ils aiment se lancer des fleurs en écrivant leurs articles 😉

De même, les syndicats intercommunaux ou les GIP peuvent proposer des outils et des aides spécifiques. Enfin, les EPCI peuvent porter des projets communs dans le domaine du numérique.

Mutualiser permet de partager les coûts, de bénéficier d'experts, et de gagner du temps.

Mais au-delà de la mutualisation, la collectivité peut aussi agir par elle-même sans attendre un support extérieur. Parce que la plupart des cyberattaques comptent sur le manque de vigilance des utilisateurs, la formation et la sensibilisation restent des impératifs. La cybersécurité n'est pas qu'une affaire de techniciens. Chaque agent, chaque élu peut adopter des réflexes simples, à la portée de tous, tel que ne pas cliquer sur des liens suspects, ne pas partager ses mots de passe,

➔ *Suite page 20*

Retrouvez de nombreux outils disponibles gratuitement sur :

cdg30.fr

cybermalveillance.gouv.fr

Checklist des questions à se poser pour se préparer à l'entrée en vigueur de la loi

Sécurité informatique

- ☐ Les ordinateurs et logiciels sont mis à jour régulièrement
- ☐ Les mots de passe sont robustes et non partagés entre agents
- ☐ Les accès aux dossiers sont bien séparés selon les services
- ☐ Une sauvegarde automatique des données est en place

Organisation et suivi

- ☐ Un registre des incidents informatiques est tenu à jour
- ☐ Un référent cybersécurité est désigné
- ☐ Les agents ont été sensibilisés aux bons réflexes
- ☐ Les services critiques ont été identifiés

Conformité RGPD

- ☐ Un registre des traitements de données personnelles est disponible
- ☐ Les mentions légales sont intégrées dans les formulaires
- ☐ Les demandes d'accès aux données sont traitées correctement
- ☐ Un délégué à la protection des données a été désigné

Ressources

- ☐ Je connais les contacts utiles : CNIL, Cybermalveillance, ANSSI, etc.
- ☐ Je sais où trouver des modèles et guides pratiques
- ☐ Je prévois une action locale pour le mois européen de la cybersécurité

ou encore sauvegarder régulièrement ses documents. Des formations en ligne gratuites existent, et des ateliers locaux peuvent être organisés avec l'aide du CDG.

Ces leviers permettent aux petites communes de prendre part à la dynamique nationale de cybersécurité, sans se sentir exclues ou dépassées. L'enjeu est collectif : protéger les services publics, les données des habitants et la confiance dans l'action locale.

Calendrier et étapes clés

Le projet de loi sur la résilience des infrastructures critiques suit une procédure accélérée, ce qui signifie que les changements vont arriver vite. Ainsi, le texte est actuellement discuté à l'Assemblée nationale. Il devrait être adopté d'ici la fin de l'année. Des ajustements sont possibles, mais les grandes lignes sont déjà connues. Début 2026, son entrée en vigueur progressive est ainsi prévue. Les obligations ne tomberont pas toutes d'un coup. Un calendrier sera fixé par décret pour chaque type d'entité. Les communes auront plusieurs mois pour se mettre en conformité.

Toutefois, même sans attendre les textes définitifs, il est utile de commencer à identifier les services critiques : eau, état civil, périscolaire, voirie… Il est essentiel de réfléchir d'ores-et déjà à désigner un référent cybersécurité et à en prévoir la formation pour être prêt le moment venu. Par ailleurs, il peut être utile de tenir un registre des incidents (même simple) tout en espérant ne jamais avoir à s'en servir.

Le service « Protection des données » lors d'une matinée d'information sur la sécurité et la protection des collectivités auprès de la communauté de communes de Cèze Cévennes

Enfin, en ce mois d'octobre 2025, mois européen de la cybersécurité, c'est le moment idéal pour lancer une action locale visant à sensibiliser le personnel, les élus, et de manière plus globale, l'ensemble des usagers de nos services publics. Il peut ainsi être utile d'organiser des réunions d'information, des ateliers, ou encore une campagne d'affichage dans les locaux communaux.

En anticipant dès maintenant, même modestement, les communes montrent qu'elles prennent au sérieux la sécurité des données et des services publics. C'est aussi une manière de rassurer les habitants et de valoriser le rôle des élus dans la protection du quotidien.

La cybersécurité n'est plus une affaire réservée aux grandes villes ou aux experts informatiques. Avec le projet de loi sur la résilience des infrastructures critiques, les petites communes entrent pleinement dans le périmètre des entités à protéger. Ce n'est pas une contrainte, mais une reconnaissance : celle du rôle essentiel qu'elles jouent dans la vie quotidienne des citoyens.

Plutôt que de subir les obligations à venir, les collectivités peuvent prendre les devants : mutualiser les compétences, s'appuyer sur les partenaires publics, adopter des outils simples et sensibiliser leurs équipes. Chaque action compte, même modeste, pour renforcer la sécurité des services publics et la confiance des habitants. À l'heure où les menaces numériques se multiplient, la résilience locale devient un enjeu national. Et c'est en agissant dès maintenant, avec pragmatisme et solidarité, que les communes pourront transformer cette réforme en opportunité ■

NE CRAIGNEZ PLUS LES CYBERCRIMINELS

REJOIGNEZ-NOUS LORS DU COLLOQUE

COLLECTIVITÉS ET CYBERSÉCURITÉ
PROTÉGER LES DONNÉES PUBLIQUES

COLLOQUE ORGANISÉ PAR LE CDG30

Jeudi 23 octobre 2025
à L'Ombrière Pays d'Uzès

Archives et cybersécurité : ce que le projet de loi « résilience des infrastructures critiques » change pour les collectivités

Le projet de loi sur la résilience des infrastructures critiques, actuellement en cours d'examen au Parlement (*voir dossier page 16*), vise à renforcer la sécurité des entités publiques face aux menaces numériques croissantes. Les collectivités territoriales, même de petite taille, sont progressivement intégrées dans le périmètre des obligations, notamment en matière de cybersécurité, continuité de service et gestion des risques.

Dans ce cadre, les archives — qu'elles soient papier ou numériques — jouent un rôle fondamental. Elles ne sont pas seulement un outil de mémoire ou de preuve : elles constituent une infrastructure critique invisible, indispensable à la traçabilité des décisions, à la protection des droits des usagers et à la continuité administrative en cas d'incident.

Si le texte ne mentionne pas explicitement les archives, il impose aux collectivités une logique de sécurisation globale des systèmes d'information. Cela inclut les **plateformes d'archivage électronique**, les **procédures de conservation**, les **accès aux documents sensibles**, et les **plans de reprise d'activité**. En somme, les archives deviennent un maillon stratégique de la résilience locale. Leur compromission pourrait entraîner des pertes irréversibles, des atteintes aux droits des usagers ou des blocages administratifs majeurs.

Le projet de loi impose aux collectivités identifiées comme « entités essentielles » ou « importantes » de renforcer leur cybersécurité, ce qui inclut la protection des accès aux archives numériques (authentification, traçabilité, cloisonnement), mais également la mise en place de sauvegardes régulières et de plans de reprise d'activité incluant les fonds archivés.

L'identification des documents sensibles ou stratégiques dans les cartographies des risques et l'intégration des archives dans les audits de sécurité et les protocoles de gestion de crise sont également des mesures à adopter. Les collectivités devront également veiller à ce que les solutions d'archivage utilisées soient conformes aux exigences du RGPD et du Code du patrimoine, notamment en matière de durée de conservation, de droit d'accès et de sécurisation des données personnelles.

En somme, les archives ne sont plus seulement un enjeu patrimonial ou réglementaire : elles deviennent un élément de résilience opérationnelle, au même titre que les systèmes de gestion des états civils, des finances ou des ressources humaines.

Face aux nouvelles exigences de cybersécurité, les collectivités doivent intégrer les archives dans leur stratégie de résilience. Cela ne nécessite pas forcément des moyens techniques lourds, mais une approche structurée et collaborative.

1 Sécuriser les accès

Les agents habilités doivent disposer d'identifiants personnels, et les connexions aux systèmes d'archivage doivent être tracées. Il est essentiel de cloisonner les accès selon les fonctions, pour éviter les manipulations involontaires ou malveillantes.

2 Assurer la sécurisation du système d'archivage électronique

Ensuite, il faut s'assurer que les solutions d'archivage électronique utilisées sont conformes aux normes en vigueur, notamment celles du SIAF (Service interministériel des Archives de France) et du RGPD. Cela implique des sauvegardes régulières, une documentation claire des procédures, et une capacité à restaurer les données en cas d'incident.

3 Associer les référents

Le délégué à la protection des données et le référent cybersécurité doivent être associés à toute réflexion sur les archives, qu'il s'agisse de numérisation, de conservation ou de destruction. Leur expertise permet d'anticiper les risques et de garantir la conformité.

4 Sensibiliser les agents

Enfin, les agents doivent être sensibilisés : comprendre pourquoi certaines données doivent être protégées, comment manipuler les documents numériques, et quoi faire en cas de doute ou d'incident. Une fiche réflexe ou une formation courte peut suffire à créer une culture de vigilance.

DRONES ET RESPECT DE LA VIE PRIVÉE

Cadre légal

- Code des transports et le code de l'aviation civile
- Code pénal : articles 226-1 à 226-7: atteinte à la vie privée
- Code pénal : articles 226-8 à 226-9 : atteinte à la représentation de la personne
- RGPD

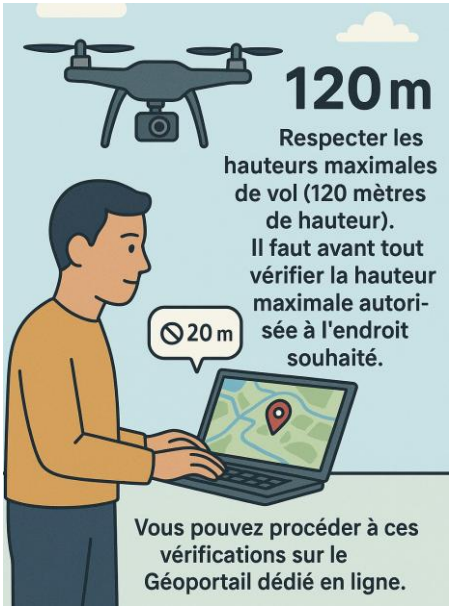
Qu'est ce que c'est ?

Un drone est défini comme un aéronef sans équipage à bord (Unmanned Aircraft Systems UAS). Terminologie retenue par la réglementation européenne pour désigner un aéronef télépiloté, un drone ou un aéromodèle. Il s'agit d'un appareil capable de s'élever ou de circuler dans les airs qui ne transporte pas des passagers, commandé à distance par un télépilote ou complètement autonome.

Règles à suivre pour toute utilisation d'un drone

1.

2.



3.

CLIQUEZ ICI

géo

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES

dpd@cdg30.fr
04 66 38 86 86

4.

5.

6.

7.

8.

Souscrire une assurance responsabilité civile spécifique.
La responsaabilité du télépilote peut être engagée en cas de dommages causés aux autres drones, aux personnes et aux biens.

9.

Ne pas survoler de sites sensibles ou protégés (centrales nucléaires, terrains militaires, réserves naturelles...).
Respecter les restrictions : l'utilisation d'un drone peut être interdite dans certaines zones, le site Géoportail permet de connaitre

Obligations liées à l'exploitation du drone

- ✓ Selon le type de drone l'enregistrement auprès de la Direction Générale de l'Aviation Civile (DGAC) et la formation du pilote sont nécessaires.
- ✓ Le télépilote ne peut pas se trouver à bord d'un véhicule en déplacement.

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

Obligations liées au RGPD

FINALITÉ	DONNÉES PERSONNELLES	DUA	SORT FINAL
Captation d'événements publics ou cérémonies à des fins de communication ou promotion	Images et vidéos captées utilisées dans la production audiovisuelle finale	1 an	Tri ou conservation (si la captation a une valeur patrimoniale ou historique, elle peut être conservée définitivement).

Attention : toute élimination doit faire l'objet d'un visa préalable des Archives départementales.

- L'opérateur doit réaliser une analyse d'impact relative à la protection des données si le traitement présente des risques élevés.
- Tenir un registre des activités de traitement.
- Mettre en place des mesures techniques et organisationnelles pour assurer la sécurité des données.

Sanctions

RGPD	
La CNIL dispose d'un pouvoir de sanction qui peut aller jusqu'à 20 millions d'euros.	
Code Pénal	
L'atteinte à la vie privée (article 226-1)	Punie d'un an d'emprisonnement et de 45 000 € d'amende.
La mise en danger de la vie d'autrui (article 223-1)	Punie d'un an d'emprisonnement et de 15 000 € d'amende.
L'intrusion dans une zone d'interdiction de survol	Punie de six mois d'emprisonnement et de 15 000 € d'amende.
Direction Générale de l'Aviation Civile	
Suspension ou retrait de l'autorisation d'exploitation	
Amendes administratives jusqu'à 750 € pour une personne physique et 3 750 € pour une personne morale.	

SOURCES :

- https://www.ecologie.gouv.fr/politiques-publiques/exploitation-drones-categorie-ouverte
- https://www.ecologie.gouv.fr/sites/default/files/documents/Guide_categorie_Specifique_0.pdf

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

LE SERVICE
PROTECTION
DES DONNÉES

s'engage pendant le CYBERMOIS

NOUS SOMMES #CYBERENGAGÉS
CYBER MOIS
01 OCT — 31 OCT
ÉDITION 2025

Du 1er au 31 octobre 2025

En savoir plus sur **Cybermois.gouv.fr**