

CYBERACTU'

LE MAGAZINE DU SERVICE PROTECTION DES DONNÉES DU CENTRE DE GESTION DU GARD

SEPTEMBRE 2026



L'actualité :

Le Cyber mois

Fiche pratique :

L'hameçonnage

Archives :

Les archives des services éducatifs

Dossier page 10



Centre de gestion
de la fonction publique
territoriale du Gard

Rentrée 2026 : nouveaux projets et réflexes RGPD

SOMMAIRE

3 L'ACTUALITÉ DE LA PROTECTION DES DONNÉES

7 LES SANCTIONS RGPD DANS L'UE

9 CES COLLECTIVITÉS SE SONT FAIT ATTAQUER

10 LE DOSSIER

RENTÉE 2026 : RÉUSSIR SES NOUVEAUX PROJETS SANS OUBLIER
LE RGPD ET LA CYBER

13 FICHE RGPD : L'HAMEÇONNAGE

15 LE POINT ARCHIVES

Retrouvez toute l'actualité sur
notre **site internet** et nos
réseaux sociaux !



CyberActu' - n° 13 - Septembre 2026
Directeur de la publication : Fabrice Verdier
Responsable de la rédaction : Ana Vega Aguilar
Articles : Ana Vega Aguilar et Sarah Roman
Centre de gestion de la fonction publique territoriale
183 chemin du Mas Coquillard, 30900 Nîmes
Tous droits réservés sauf autorisation.
Pour contacter la rédaction :
☎ : 04 66 38 86 86
@ : dpd@cdg30.fr

LE CYBER MOIS EST DE RETOUR !

Du 1er au 31 octobre nous sommes #CyberEngagés

Nous vous invitons à sensibiliser vos administrés facilement grâce à la campagne nationale "Histoire de Cyber".

C'est très simple, on vous explique tout !

- ✓ **Qui ?** Les collectivités territoriales et établissements publics
- ✓ **Quoi ?** Sensibiliser les administrés grâce au Cybermois
- ✓ **Où ?** Trouvez toutes les ressources sur le site de cybermalveillance.gouv.fr
- ✓ **Quand ?** Tout le mois d'octobre
- ✓ **Comment ?** Postez sur votre site internet et votre réseau social préféré l'un des 6 conseils cyber illustrés accompagné de l'hashtag #CyberEngagés. 100% gratuit !
- ✓ **Pourquoi ?** Promouvoir les bons réflexes auprès de vos administrés et montrer l'engagement de votre collectivité.



PIXELS : DERNIER DELAI ÉCOULÉ

Le 14 juillet 2026 marquait la date limite de mise en conformité avec les obligations liées à l'utilisation des pixels

Nous l'évoquions déjà dans le CyberActu' précédant. Les pixels sont des traceurs intégrés aux messages électroniques. Selon les fonctionnalités activées, ils peuvent collecter différentes informations sur les destinataires.

Pour vous conformer à la réglementation, plusieurs actions sont à envisager :

- 1 Renseignez-vous auprès de votre fournisseur de messagerie électronique et de votre prestataire de newsletters afin d'identifier les pixels collectés par leurs solutions ;
- 2 Vérifiez si votre situation relève d'un cas d'exemption ;
- 3 Informez les usagers des données collectées via votre politique de confidentialité, notamment concernant l'utilisation des pixels dans les courriels ;
- 4 Ajoutez une mention d'information dans les formulaires d'inscription à votre newsletter afin de recueillir le consentement des nouveaux abonnés ;
- 5 Recueillez le consentement des abonnés déjà inscrits lorsque cela est nécessaire ;
- 6 Enfin, conservez des traces de la démarche

LES RENCONTRES INFORMATIQUE ET LIBERTÉS

Organisées par la CNIL le 29 septembre, ces rencontres présenteront 2 thématiques d'intérêt.



Les inscriptions sont complètes mais une rediffusion sera disponible sur le site de la CNIL.

Les lunettes connectées

Cette technologie ouvre la voie à de nouveaux usages au quotidien, mais aussi à de nouveaux risques pour la vie privée.

Les lunettes connectées feront l'objet d'un nouveau cadre de régulation qui permettra d'éclairer tout l'écosystème ainsi que les usagers.

Les sanctions RGPD

Le deuxième sujet sera : le rôle des sanctions RGPD, et les enjeux que cela relève pour les autorités de protection des données à l'échelle européenne et nationale.

Le service Protection des données y participera afin de vous faire un retour des échanges.

SENSIBILISER LES ÉLÈVES À LA PROTECTION DES DONNÉES

En 2026 la CNIL a contribué à sensibiliser 2500 élèves de CM2 (100 classes) aux enjeux du numérique et à la protection des données personnelles.

Libre accès aux ressources

Toutes les ressources utilisées sont en ligne afin de permettre aux enseignants de reproduire ce projet pédagogique dans leurs écoles.

Le contenu

Les séances ont une durée d'une heure et sont articulées en 4 étapes : une introduction, une mise en activité, des échanges sur les activités et enfin une évaluation individuelle.

Lisez la note complète et récupérez les outils ici : [Sensibiliser les élèves à la protection des données](#)

Les enseignants peuvent prolonger les échanges avec les élèves, grâce aux fiches de préparation mises à leur disposition. Les thématiques centrales sont : l'IA, les mots de passe, l'hameçonnage et les bonnes pratiques sur Internet.

Le service Protection des données vous accompagne dans la mise en œuvre de ces projets pédagogiques.

MUNISSEZ VOS BIBLIOTHEQUES DE RESSOURCES RGPD



L'agence de la vie privée

La CNIL a publié le 2ème tome de leur manga "L'Agence Privacy" à destination des jeunes et des parents. Après le succès de leur premier tome, les aventures continuent. Ces lectures abordent les risques numériques pour la vie privée.

Les acteurs de l'éducation numérique peuvent faire la demande pour obtenir un exemplaire en format papier en écrivant à educnum@cnil.fr

LES ACTIONS DU SERVICE PROTECTION DES DONNÉES

L'organisation des Cyber Cafés

La sensibilisation n'est jamais de trop. Nous le répétons souvent lors de nos rendez-vous. Et pour une fois, on peut dire que les cordonniers ne sont PAS les plus mal chaussés !

En effet, depuis déjà deux ans, le Centre de gestion a mis en place un projet en interne : les Cyber Cafés.



Ces réunions hebdomadaires ont pour objectif de sensibiliser les agents du CDG30, tous services confondus, aux enjeux de la protection des données et de la cybersécurité. Comme leur nom l'indique, le café et les biscuits sont toujours au rendez-vous !

Il ne s'agit pas d'un cours, mais bien d'un moment d'échange où tous les agents sont sur un pied d'égalité pour réfléchir ensemble aux risques cyber et aux bons réflexes à adopter.

Les actions du service en interne :
La sensibilisation permanente de nos agents !

D'une durée de 30 minutes en matinée et organisés en groupes de 10 personnes maximum, les Cyber Cafés permettent à chacun de participer. Les 15 premières minutes sont consacrées à la découverte du sujet du jour, puis les 15 suivantes laissent place au jeu. Répartis en petits groupes, les agents travaillent sur une activité pédagogique et, très vite, l'esprit de compétition prend le dessus !



SENSIBILISATION DES CLASSES CM1 ET CM2 AUX RISQUES D'UTILISER L'IA

En juin 2026, le service Protection des données est intervenu auprès d'une centaine d'élèves de CM1 et CM2 dans le cadre du programme de sensibilisation conçu par une mairie.

L'objectif était d'accompagner les enfants dans leurs premiers usages du numérique en les sensibilisant aux données personnelles, aux opportunités offertes par Internet et l'intelligence artificielle, mais également aux risques liés à leur utilisation.

Les échanges, très interactifs, ont permis aux élèves de mieux comprendre ce qu'est une identité numérique et pourquoi il est important de protéger ses informations personnelles.

Chaque séance alternait présentation, discussions et activités ludiques. Après une introduction sur les usages du numérique et de l'IA, les élèves découvraient les notions essentielles de protection des données, les bons réflexes à adopter en ligne et participaient à un défi en équipe.

Les retours d'expérience, très positifs de la part des élèves et des équipes pédagogiques, confirment l'intérêt de poursuivre ces actions de sensibilisation dès le plus jeune âge.



LES ACTIONS DE NOS COLLECTIVITÉS

Bellegarde : Une démarche à suivre !

Dans le cadre de notre bilan de rentrée, nous avons souhaité mettre en lumière la commune de Bellegarde, adhérente à notre service.

Des actions structurantes

En un peu plus de deux ans, la commune a réalisé un travail conséquent : désignation d'un délégué à la protection des données pour la commune et le CCAS, réalisation d'audits de sécurité, cartographie et registre des traitements, recensement des sous-traitants.

Côté organisationnel, ils ont réalisé les analyses d'impact sur plusieurs traitements sensibles, sensibilisation des agents et mise en place de documents structurants tels que la charte informatique.

Un travail collaboratif

Le tout a été possible grâce à un travail collaboratif. Tout d'abord, grâce à la volonté politique de sécuriser la mairie sur les plans informatique et juridique.

Mais aussi grâce à la participation de tous les services de la mairie. Pilotés par la référente Informatique et Libertés de la mairie, tous les agents ont participé à chaque étape de la démarche de mise en conformité afin d'atteindre le niveau actuel.

Certes, la mise en conformité a vocation à être permanente et des mises à jour sont nécessaires chaque année, une fois les règles communiquées et les bons réflexes adoptés, le maillon le plus faible, l'humain, se transforme en force.

Les avantages

Chaque étape franchie contribue à renforcer la sécurité juridique et opérationnelle de la collectivité, tout en améliorant la protection des données des usagers et des agents.

Le RGPD sert aussi à prendre de la hauteur vis-à-vis du travail que l'on réalise parfois presque en mode automatique. Il permet de rendre les procédures plus efficaces, de tracer les actions, de se protéger en cas de contentieux et d'être maître de son organisation.

L'exemple de Bellegarde montre qu'avec de la méthode et de la persévérance, les collectivités peuvent progresser significativement dans la maîtrise de leurs traitements de données.



CES COLLECTIVITÉS ONT ÉTÉ RAPPELÉES À L'ORDRE...

Durant le dernier trimestre, la scène à l'échelle européenne met en évidence les causes de sanctions infligées par les autorités de contrôle de la protection des données personnelles. Attention, collectivités, restez vigilantes sur les points suivants : courriel d'un ex-collaborateur non supprimé, manquement à l'obligation de transparence envers ses employés, des mesures techniques et organisationnelles insuffisantes pour garantir la sécurité des informations et manquement de notification de violation des données.

 FRANCE

FUITE DE DONNÉES DE SANTÉ : 700 000 PERSONNES CONCERNÉES

Au cours de l'été 2025, un attaquant est parvenu à se connecter au dossier patient informatisé (DPI), un dossier informatique contenant l'ensemble des données des patients de l'Hôpital privé de la Loire. Au total plus de 700 000 personnes affectées, y compris les patients et leurs tiers de confiance.

À la suite des contrôles menés par la CNIL, une amende de 500 000 € a été prononcée à l'encontre de l'hôpital.

Les manquements sanctionnés

D'abord, un manquement à l'obligation d'assurer la sécurité des données personnelles. La procédure d'authentification des médecins libéraux n'était pas robuste : absence de VPN et de moyen d'authentification multi facteur.

Politique d'habilitation inadéquate

Le secret médical n'était pas assuré par une séparation des droits entre l'équipe des soins et les autres équipes. Ce qui a donné libre accès à l'attaquant.

L'hôpital n'avait pas pris des mesures permettant de détecter une activité suspecte au sein du DPI en temps réel et de déclencher le cas échéant un mécanisme d'alerte.

Dans ces conditions, l'attaquant a pu explorer le DPI de l'hôpital durant plusieurs jours et extraire un volume très important de données, sans que cette activité anormale soit détectée.

Enfin, un manquement à l'obligation d'informer les personnes concernées par la violation de données (article 34 du RGPD) vis-à-vis des tiers de confiance.

LES POINTS DE VIGILANCE

- ✓ Vérifiez qu'une politique d'habilitation a été appliquée permettant l'accès aux données selon différents niveaux de confidentialité;
- ✓ Vérifiez que tout accès distant à une application hébergeant des données de santé passe par un VPN et une authentification à deux facteurs;
- ✓ Vérifiez que le système de journalisation est présent

LE CONSEIL DU DPO

Pour sécuriser vos systèmes il est indispensable de :

Savoir qui accède à quoi, depuis où et avec quel moyen d'authentification

BELGIQUE

Manquement à l'obligation de transparence envers ses employés

En Belgique, une société a été contrainte de payer le montant de 83 000 €. Les motifs sont l'enregistrement et écoute d'appels téléphoniques avec les clients à des fins de contrôle du service et de formation du personnel, sans avoir informé au préalable les employés de ces enregistrements. La société a également été sanctionnée pour l'insuffisance de base légale pour le traitement des données, durées de conservation trop longues et absence d'analyse d'impact.

Défaut d'effacement de l'adresse électronique d'un ex-collaborateur

L'autorité de contrôle belge a infligé une amende de 177 000 € à l'encontre d'une société parce que cette dernière n'avait pas effacé l'adresse électronique d'un ancien salarié après son départ.

POLOGNE

Mesures techniques et organisationnelles insuffisantes

L'autorité polonaise de protection des données a infligé une amende de 23 540 € au ministre de la Justice. Ce dernier n'a pas mis en œuvre les mesures adéquates pour garantir la sécurité des données, ce qui a permis à des personnes d'obtenir des données personnelles de magistrats. Ces données ont ensuite été publiées dans le cadre du scandale dit « de la haine », au cours duquel les données de magistrats ayant exprimé des opinions jugées indésirables ont été divulguées, les exposant ainsi à des attaques diffamatoires.

Maire sanctionné par un défaut de notification de violation de données

L'autorité polonaise de protection des données a sanctionné le maire de Myślenice d'une amende de 1 790 € à la suite d'une violation de données. Celle-ci résulte de la publication accidentelle, par un employé, d'une liste non anonymisée de signataires d'une pétition. Le responsable du traitement n'ayant pas déclaré l'incident à l'autorité compétente, une sanction a été prononcée.

ROUMANIE

Défaut de contrôle des droits d'accès

L'autorité de contrôle de protection des données roumaine a infligé une amende de 5 000 € à la Poste Nationale par la suite à une fuite de données qui a eu pour conséquence la destruction d'envois postaux contenant de données personnelles.



CES COLLECTIVITÉS SE SONT FAIT ATTAQUER...



Mairie de Sixt-sur-Aff

La base de données d'un site internet a été compromise, ainsi qu'un accès administrateur.

Mairie de Camiers

Une fuite de données est revendiquée par le groupe ransomware Kairos.

Mairie de Quiberon

Système d'information impacté et certains services ont été perturbés.

Mairie de Marcq-en-Barœul

Les données de 5700 usagers exposées par une fuite de données. La ville a subi une intrusion de leur site internet.

Police municipale - La Tremblade

Fuite de données : données et panneau d'administration revendiqués sur un forum cybercriminel.

Mairie de Perreux-sur-Marne

Le portail municipal permettant aux habitants d'accéder aux démarches administratives en ligne est compromis. Risque de fuite de données.

Mairie d'Eyguieres

Une attaque informatique met hors service tout le système informatique et menace de nombreuses données administratives et personnelles.

Police municipale - Gradignan

Le logiciel de la police municipale a fait l'objet d'une attaque. La Ville appelle à la vigilance.

Police municipale - Le Pontet

La Mairie a été victime d'un incident de cybersécurité ayant affecté les fichiers d'opérations courantes de la Police Municipale. Un export frauduleux de données a été réalisé.

...SEREZ-VOUS LES PROCHAINES VICTIMES?

Rentrée 2026 : réussir ses nouveaux projets sans oublier le RGPD et la cyber

La rentrée est toujours une période stratégique pour les collectivités territoriales et les établissements publics. Après la pause estivale, les projets redémarrent et les équipes se réorganisent. Cette phase de relance est aussi l'occasion de remettre la protection des données personnelles et la cybersécurité au cœur des priorités.

Une révision nécessaire des accès et des habilitations

L'été est souvent synonyme de mouvements de personnel : départs, recrutements, mutations, remplacements ou réorganisations internes.

Chaque changement doit conduire à une vérification des habilitations d'accès aux outils numériques, aux applications métiers et aux données personnelles.

Quelques questions essentielles doivent être systématiquement posées

- ✓ Les comptes des agents ayant quitté la collectivité ont-ils été désactivés ?
- ✓ Les nouveaux arrivants disposent-ils uniquement des droits nécessaires à leurs missions ?
- ✓ Les habilitations accordées sont-elles documentées ?

Cette gestion rigoureuse des droits constitue l'un des premiers remparts contre les fuites de données et les cyberattaques.

De nouvelles obligations

La rentrée est souvent le moment choisi pour lancer de nouveaux outils et services numériques :

- nouveaux logiciels ;
- portail famille ;
- application citoyenne ;
- démarches en ligne ;
- système de réservation ;
- gestion dématérialisée des demandes ;
- nouveaux outils RH.

Avant toute mise en œuvre d'un nouveau projet impliquant des données personnelles, il convient de suivre ces étapes :

1. identifier les données collectées ;
2. vérifier leur nécessité ;
3. définir une durée de conservation ;
4. identifier les personnes ayant accès aux données ;
5. informer clairement les usagers.

Le délégué à la protection des données doit être associé à ces réflexions.

Rappeler les règles internes

Le début d'année administrative constitue un moment idéal pour communiquer ou actualiser les documents de référence de la collectivité :

- ✓ règlement intérieur ;
- ✓ charte informatique ;
- ✓ procédures de gestion des incidents ;
- ✓ bonnes pratiques relatives aux données personnelles.

Ces documents permettent de formaliser les règles applicables et de rappeler les responsabilités de chacun. Ils doivent être facilement accessibles aux agents et faire l'objet d'une présentation lors de l'accueil des nouveaux arrivants.

Inscriptions aux services municipaux

La rentrée correspond à une période particulièrement intense pour les inscriptions :

- ✓ nouveaux arrivants ;
- ✓ PCS ;
- ✓ écoles ;
- ✓ restauration scolaire ;
- ✓ accueils périscolaires ;
- ✓ centres de loisirs ;
- ✓ activités sportives ;
- ✓ médiathèques ;
- ✓ transports scolaires.

Chaque formulaire, papier ou numérique, doit comporter une information claire sur le traitement des données personnelles.

Cette mention d'information doit notamment préciser :

- ✓ l'identité du responsable du traitement ;
- ✓ les finalités poursuivies ;
- ✓ la base juridique ;
- ✓ les destinataires ;
- ✓ la durée de conservation ;
- ✓ les droits des personnes ;
- ✓ les coordonnées du DPO.

Une information insuffisante demeure l'un des manquements les plus fréquemment observés lors des contrôles.

Accueillir les nouveaux habitants

De nombreuses communes organisent des cérémonies ou événements destinés à accueillir les nouveaux habitants.

Ces moments conviviaux sont souvent relayés sur les réseaux sociaux, le site internet communal ou les supports de communication institutionnels.

Attention toutefois au respect du droit à l'image.

Avant toute publication de photographies permettant d'identifier des personnes, il convient de vérifier la base juridique appropriée et, lorsque cela est nécessaire, de recueillir les autorisations correspondantes.

Vigilance renforcée sur les données des enfants

Les données relatives aux enfants bénéficient d'une attention particulière au regard du RGPD.

Les collectivités doivent veiller à :

- ✓ collecter uniquement les informations nécessaires ;
- ✓ sécuriser les dossiers scolaires ;
- ✓ encadrer les échanges avec les établissements partenaires ;
- ✓ limiter l'accès aux personnes habilitées ;
- ✓ sensibiliser les personnels concernés.

Les listes d'élèves, informations médicales, données relatives aux repas ou aux activités périscolaires nécessitent un niveau de vigilance élevé.

Encadrer les échanges avec les partenaires

La rentrée s'accompagne également de nombreux échanges de données avec les organismes publics partenaires. Ces transmissions doivent être juridiquement encadrées.

Lorsqu'un partage de données est mis en œuvre, il est recommandé de formaliser une convention précisant :

- les finalités du partage ;
- les responsabilités respectives ;
- les catégories de données transmises ;
- les mesures de sécurité ;
- les modalités d'exercice des droits des personnes.

Une convention bien rédigée sécurise les pratiques et réduit les risques juridiques.

Vidéoprotection : mettre à jour son analyse d'impact

De nombreuses collectivités poursuivent le développement de leurs dispositifs de vidéoprotection.

Cette analyse doit notamment être réévaluée lorsque :

- de nouvelles caméras sont installées ;
- le périmètre de surveillance est étendu ;
- les modalités techniques évoluent ;
- de nouveaux usages sont envisagés.

Les collectivités adhérentes au service Protection des données bénéficient d'un accompagnement et de modèles adaptés pour réaliser ou actualiser cette analyse.

La sensibilisation

Les incidents de cybersécurité résultent souvent d'erreurs humaines. La rentrée constitue donc le moment idéal pour organiser une session de sensibilisation à destination :

- ✓ des agents ;
- ✓ des encadrants ;
- ✓ des élus ;
- ✓ des nouveaux arrivants.

Une simple piqûre de rappel annuelle permet souvent d'éviter des incidents majeurs.

Là encore, les agents du CDG assurent cette mission.

Faire de la conformité un réflexe

La rentrée est synonyme de nouveaux départs, de nouveaux projets et d'ambitions renouvelées pour les territoires. C'est aussi une occasion privilégiée de remettre la protection des données personnelles et la cybersécurité au cœur des pratiques de la collectivité.

Quelques heures consacrées à la vérification des accès, à la sensibilisation des équipes et à la mise à jour des procédures peuvent éviter des incidents coûteux, renforcer la confiance des administrés et contribuer à une administration plus performante, plus résiliente et plus respectueuse des droits des citoyens.

Nous vous proposons une liste de contrôle afin de ne rien oublier !



Check-list de rentrée RGPD et cybersécurité

Avant de lancer la nouvelle année administrative, vérifiez les points suivants :

- ☐ Désactiver les comptes des anciens agents et élus.
- ☐ Mettre à jour les habilitations et les accès aux applications métiers.
- ☐ Vérifier l'actualité du registre des traitements.
- ☐ Contrôler les mentions d'information présentes sur tous les formulaires.
- ☐ Mettre à jour la charte informatique et les procédures internes.
- ☐ Encadrer les échanges de données par des conventions adaptées.
- ☐ Réexaminer les dispositifs de vidéoprotection et leurs analyses d'impact.
- ☐ Sensibiliser les élus aux obligations de protection des données.
- ☐ Organiser un exercice ou une communication sur les bonnes pratiques cyber.
- ☐ Vérifier les sauvegardes et les procédures de reprise d'activité.
- ☐ Contrôler les publications sur les réseaux sociaux et le respect du droit à l'image.
- ☐ S'assurer que les nouveaux projets numériques intègrent les exigences du RGPD dès leur conception.



L'HAMEÇONNAGE



MÉTHODE

L'hameçonnage (ou phishing) est un SMS ou courriel frauduleux destinés à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour une personne de confiance. Ces techniques d'arnaque aux SMS évoluent constamment.

BUT RECHERCHÉ

- Dérober des informations personnelles ou professionnelles (informations d'identité, coordonnées, mots de passe, codes de validation, données bancaires...) pour en faire un usage frauduleux ;
- Infecter un équipement par un virus pour en prendre le contrôle.

COMMENT RÉAGIR ?

- Ne répondez pas au message, ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes d'un message suspect ou provenant d'un émetteur inconnu ;
- Au moindre doute, vérifiez l'information directement auprès de l'organisme ou de la personne qui vous sollicite.

SI VOUS ÊTES VICTIME

- ▶ En cas de doute, **CONTACTEZ DIRECTEMENT L'ORGANISME CONCERNÉ** pour confirmer le message ou l'appel que vous avez reçu.
- ▶ Si vous avez communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte bancaire, **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier.
- ▶ Si vous avez communiqué un mot de passe, **CHANGEZ LE IMMÉDIATEMENT** ainsi que sur tous les autres sites ou services sur lesquels vous l'utilisiez.
- ▶ **CONSERVEZ LES PREUVES** et, en particulier, le message d'hameçonnage reçu.
- ▶ Si vous avez reçu un message douteux sans y répondre, **SIGNALEZ-LE À SIGNAL SPAM (SIGNAL-SPAM.FR)**.
- ▶ Vous pouvez également **SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE À PHISHING INITIATIVE (PHISHINGINITIATIVE.FR)** qui en fera fermer l'accès.
- ▶ En fonction du préjudice subi (débits frauduleux, usurpation d'identité...) **DÉPOSEZ PLAINTÉ** au commissariat de police ou à la gendarmerie ou écrivez au procureur de la République dont vous dépendez en fournissant toutes les preuves en votre possession.



ASTUCES POUR DETECTER UNE TENTATIVE D'HAMEÇONNAGE

- 1 Une alerte de votre logiciel de messagerie ou de votre antivirus
- 2 Un message d'un service, d'un organisme ou d'une entreprise dont vous n'êtes pas client ou utilisateur
- 3 Un nom ou une adresse d'expéditeur inhabituel, incohérent voire fantaisiste
- 4 Un objet de message succinct ou alarmiste
- 5 Une apparence suspecte (mauvaise mise en forme ou logo), une absence ou des erreurs dans la personnalisation
- 6 Un message aguicheur, inquiétant ou bien une demande inhabituelle
- 7 Des fautes de français surprenantes
- 8 Une incitation à cliquer sur un lien ou ouvrir une pièce-jointe
- 9 Un appel provenant d'un numéro de téléphone inconnu ou masqué

MESURES PRÉVENTIVES

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

Utilisez des mots de passes différents et complexes pour chaque site et application afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres-forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

Si le site le permet, vérifiez les date et heure de dernière connexion à votre compte afin de repérer si des accès illégitimes ont été réalisés.

Si le site vous le permet, activez la double authentification pour sécuriser vos accès.

Tour d'horizon des archives des services éducatifs : écoles, crèches, restauration, périscolaire et transports

Les archives produites par les communes et les EPCI, dans le cadre de leurs compétences scolaires, périscolaires, de restauration, de petite enfance et/ou de transport scolaire, ne doivent pas être confondues avec les archives de scolarité et de pédagogie produites par l'Éducation nationale.

Les archives scolaires : un intérêt administratif, juridique et historique

Écoles maternelles et primaires

Les archives produites par les collectivités dans le domaine des écoles maternelles et élémentaires concernent notamment les inscriptions et dérogations scolaires, les bâtiments scolaires, les personnels territoriaux et les services associés. Au-delà de leur utilité administrative, elles constituent un témoignage précieux de l'évolution de la vie scolaire, des effectifs et des politiques éducatives locales.

Crèches et petite enfance

Les structures de la petite enfance produisent des archives liées à l'accueil des enfants, au suivi administratif des familles et au respect des obligations réglementaires. Ces documents, souvent sensibles au regard des données personnelles qu'ils contiennent, permettent également de retracer l'évolution des modes d'accueil et des besoins des familles sur le territoire.

Périscolaire et accueils de loisirs

Les activités périscolaires et les accueils de loisirs génèrent des archives relatives à l'organisation des activités, à l'encadrement des mineurs et aux relations avec les familles. Elles témoignent de l'évolution des services proposés aux enfants et de l'action éducative menée par les collectivités en complément du temps scolaire.

Restauration scolaire

Les archives de restauration scolaire concernent le fonctionnement du service, la gestion des usagers, les aspects financiers ainsi que les obligations sanitaires. Elles illustrent également les évolutions des pratiques alimentaires, des normes sanitaires et des politiques publiques en matière de restauration collective.

Transport scolaire

Les archives du transport scolaire retracent l'organisation des déplacements des élèves, les relations avec les familles et les transporteurs ainsi que l'évolution des modes de gestion du service. Elles présentent un intérêt particulier pour comprendre :

- les transformations de la carte scolaire,
- les regroupements pédagogiques intercommunaux et
- l'aménagement des territoires ruraux.

Qu'elles concernent les écoles, les crèches, la restauration scolaire, le périscolaire ou le transport, les archives produites par les communes et les EPCI témoignent de compétences essentielles au service de la population. Leur bonne gestion, depuis leur production jusqu'à leur élimination réglementaire ou leur conservation définitive, contribue à la fois à la sécurité juridique de la collectivité et à la préservation de la mémoire locale.

Une archive inattendue : le menu de cantine

Les menus de cantine font partie de ces documents qui paraissent anodins, mais dont l'intérêt historique est réel. Leur conservation (selon les règles de tri applicables) permet de suivre l'évolution des pratiques alimentaires, de l'éducation nutritionnelle et des politiques publiques en faveur des enfants. À l'image des archives scolaires du XIX^e siècle, ils constituent des témoins précieux de la vie quotidienne et de l'histoire locale.



Le menu scolaire est un document qui présente les repas proposés aux élèves pendant la semaine. Il est généralement affiché dans les écoles et les cantines. Le menu du 03 au 07 juin 2024 est le suivant :

LUNDI 03 JUIN	MARSI 04 JUIN	MERCREDI 05 JUIN	JEUDI 06 JUIN	VENREDI 07 JUIN
Salade de tomates	Carottes râpées vinaigrette	Concombre à la crème	Salade verte et miel	Bonnes herbes
Œuf de dinde sauté curry	Pâtis à la bûche (beurre)	Poisson blanc au citron	Œuflette aux fines herbes	Pâtis de cake saucisson
Œuf	Œuf	Œuf	Œuf	Œuf
Fromage blanc	Emmental râpé	Vapeur de légumes	Œuf	Œuf
Fruit de saison (orange)	Compote de pommes	Cake maison au chocolat	Fruit de saison (orange)	Fruit de saison (orange)

Menu adapté aux besoins d'accompagnement. Les repas sont préparés sur place par l'équipe de restauration.

Tableau récapitulatif des producteurs des archives et de leurs compétences

Archives publiques et protection des données : trouver le juste équilibre

Les archives scolaires, périscolaires ou liées à la petite enfance contiennent de nombreuses données à caractère personnel concernant les enfants, leurs représentants légaux ou encore les agents des collectivités.

À ce titre, la gestion de ces archives publiques doit concilier les obligations du Règlement général sur la protection des données (RGPD) et celles du Code du patrimoine.

Le RGPD impose de ne pas conserver les données au-delà de ce qui est nécessaire à la finalité du traitement. Toutefois, lorsqu'elles constituent des archives publiques, certaines informations doivent être conservées pendant des durées parfois longues afin de répondre à des obligations administratives, juridiques, probatoires ou historiques.

Ainsi, les tableaux de gestion constituent un outil essentiel de mise en conformité.

DOMAINES	PRODUCTEURS	EXEMPLES DE DOCUMENTS
Gestion des écoles communales	Commune	Inscriptions et dérogations scolaires (dossiers d'inscription, listes d'élèves, dérogation), bâtiments scolaires (travaux, entretien, contrôles de sécurité), équipements et fournitures (inventaires, commandes, factures), relations avec les écoles et les familles (courriers, supports de communication)
Gestion des services scolaires et périscolaires	Commune ou syndicat scolaire	Restauration scolaire (inscriptions, menus, tarifs, facturation, marchés de fourniture de repas), garderie et activités périscolaires (dossiers d'inscription, listes de présence, programmes d'activités), transports scolaires (circuits, horaires, listes d'élèves, conventions avec les transporteurs), règlements et correspondance avec les familles
Organisation intercommunale de la scolarisation	Communes organisées en RPI (regroupement pédagogique intercommunal)	Répartition des classes et des élèves entre les communes, suivi et prévisions des effectifs, échanges avec l'Éducation nationale, organisation des services mutualisés : restauration, garderie, activités périscolaires et transport scolaire
Enseignement et suivi de la scolarité	Éducation nationale	Suivi des élèves (dossiers scolaires, fiches de renseignements, registres matricules, registres et listes d'appel), évaluation (livrets scolaires, bulletins, résultats), orientation et passage de classe, projets d'école, cahiers de textes, supports pédagogiques, comptes rendus des conseils d'école ou de classe, enquêtes et statistiques scolaires.

Ils définissent, pour chaque catégorie de documents, une durée de conservation justifiée et prévoient, à l'issue de cette période, soit leur élimination réglementaire, soit leur conservation définitive lorsqu'ils présentent un intérêt historique ou patrimonial.

Les documents contenant des données personnelles, tels que les dossiers d'inscription scolaire, les listes de fréquentation des services périscolaires, les dossiers d'accueil en crèche ou encore certaines pièces relatives au transport scolaire, ne peuvent pas être détruits au seul motif qu'ils ne sont plus utiles à la gestion quotidienne du service.

Leur sort est déterminé conformément aux durées de conservation et aux règles de tri applicables aux archives publiques.

Toutefois, la conservation d'un document ne signifie pas qu'il est librement accessible. L'accès à ces archives doit être limité aux seules personnes habilitées pendant toute leur durée de conservation.

Les archives publiques contenant des données personnelles sont soumises aux règles de communicabilité prévues par le Code du patrimoine.

Ces délais de communicabilité visent précisément à concilier le droit d'accès aux archives et la protection de la vie privée des personnes concernées.

Pour connaître les durées de conservation, les règles de tri et le sort final applicables à ces documents, il convient de se reporter au tableau de gestion des affaires scolaires mis à disposition par les Archives départementales du Gard.

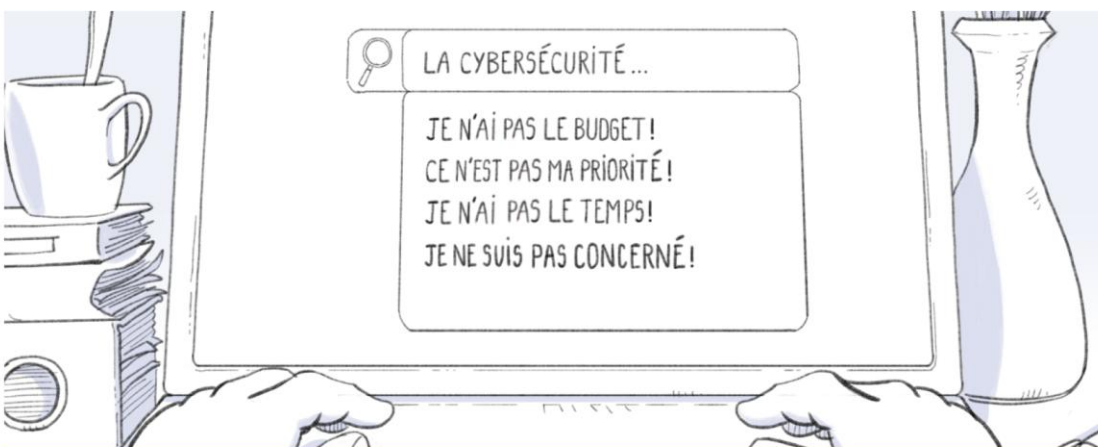
N'oubliez pas que toute élimination d'archives publiques est soumise au visa préalable des Archives départementales. À ce titre, un bordereau d'élimination doit être transmis pour validation avant toute destruction matérielle des documents.

Une bonne gestion des archives participe pleinement à la conformité RGPD : elle permet à la fois d'éviter la conservation injustifiée de données, de respecter les obligations légales de conservation et de garantir une protection adaptée des informations personnelles tout au long de leur cycle de vie.

Les conseils de l'archiviste

- ✓ Une archive publique contenant des données personnelles ne doit pas être systématiquement détruite dès qu'elle n'est plus utilisée par le service. Chaque archive possède une durée de conservation pour des raisons administratives, juridiques et/ou historiques.
- ✓ Les archives sont librement communicables sous réserve des délais prévus pour protéger la vie privée. Ainsi les documents contenant des données personnelles sont soumis à des délais de communicabilité strictement encadrés.
- ✓ L'élimination d'archives publiques est toujours soumise à l'accord préalable des Archives Départementales de la collectivité concernée.





**SE LIBÉRER DE SES PRÉJUGÉS,
C'EST ASSURER SA CYBERSÉCURITÉ**

Rendez-vous sur
cybermalveillance.gouv.fr