CYBERACTU'

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

Janvier 2024

Bonnes résolutions : C'est le moment !

Dossier page 14

Et aussi

L'actualité de la protection des données, la vie du service, conseils du délégué à la protection des données, etc.

SERVICE PROTECTION DES DONNÉES · CENTRE DE GESTION DU GARD

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

CENTRE DE GESTION
DU GARD

Contactez-nous

04 66 38 86 86
cdg30@cdg30.fr

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

SOMMAIRE

ÉDITO

Le service « Protection des données » vous souhaite à toutes et à tous une merveilleuse année 2024. Puisse-t-elle être une année de bonheur et de réussite, tant sur le plan personnel que sur le plan professionnel.

Nous formulons également le vœu que cette année à venir soit celle de la prise de conscience dans l'importance de la protection des données et de la vie privée. Car derrière les noms et les numéros que nous traitons, il y a des vies, des familles dont l'intimité et le mode de vie sont menacés à chaque instant par des personnes à la moralité douteuse.

Nous espérons ainsi que cette année voit naître de bonnes résolutions destinées à protéger et à se protéger face aux criminels numériques.

Enfin, nous vous remercions pour cette année 2023 qui a été riche en échanges et en expériences, et formulons le vœu que l'année 2024 suive également cet exemple !

Pierre BONANNI – Ana VEGA

Sarah ROMAN

Contacts

Service « Protection des données »

☎ : 04 66 38 86 86

@ : dpd@cdg30.fr

SERVICE PROTECTION DES DONNÉES · CENTRE DE GESTION DU GARD

L'ACTUALITÉ DE LA PROTECTION DES DONNÉES

LES TEXTES RÉGLEMENTAIRES

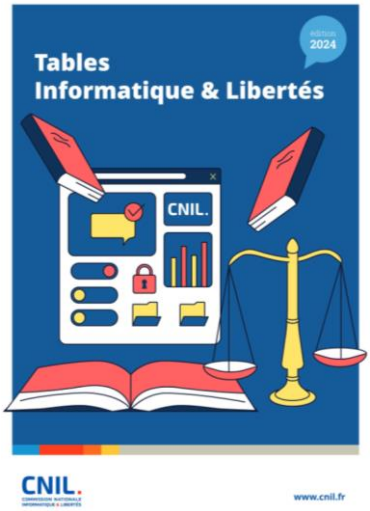
Règlement UE 2023/2841 du Parlement européen et du Conseil du 13 décembre 2023 établissant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans les institutions, organes et organismes de l'Union

Ce nouveau règlement européen intervient à moins d'un an de l'entrée en vigueur de la directive NIS-2, prévue pour le 18 octobre 2024, destinée à rehausser les exigences en matière de cybersécurité dans les secteurs essentiels. Il a pour objectif de renforcer la sécurité des systèmes d'information des différentes entités de l'Union qui entend ainsi montrer l'exemple en s'imposant à elle-même les règles prévues en matière de sécurité.

Décret n°2023-1027 du 7 novembre 2023 relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « Enquête harcèlement »

Ce texte prévoit que les élèves du CE2 à la terminale des écoles, collèges et lycées publics sont invités, au moins une fois par an, à renseigner un questionnaire non nominatif visant à évaluer s'ils sont susceptibles d'être victimes de harcèlement en milieu scolaire ou de cyberharcèlement, pour permettre aux directeurs d'école et aux chefs d'établissement d'adopter des mesures afin de prévenir ces situations. Le texte crée en conséquence le traitement à cette fin des données contenues dans les questionnaires.

EN BREF



Pour retrouver la première édition des Tables Informatique et Libertés, cliquez sur l'image ci-dessus

CNIL.

Publication des « Tables Informatique et Libertés » - 14 décembre 2023

Les Tables Informatique et Libertés sont un document inédit réunissant les décisions importantes de la CNIL et l'essentiel de la jurisprudence nationale et européenne suivant un classement thématique. La CNIL souhaite ainsi améliorer la diffusion de sa doctrine tout en permettant une meilleure prévisibilité de l'application du RGPD et de la loi Informatique et Libertés.

Publication du guide pratique pour les services de prévention et de santé au travail – 15 décembre 2023

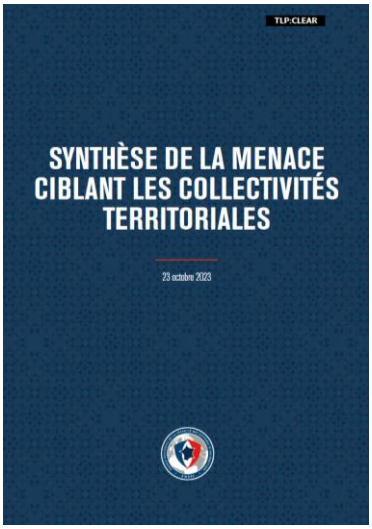
Afin d'accompagner les services de prévention et de santé au travail dans leur mise en conformité, la CNIL a élaboré un guide de sensibilisation au RGPD.

Jusqu'à présent, ces services ne disposaient pas d'outil permettant de les guider dans la mise en conformité de leurs pratiques alors qu'ils collectent de nombreuses données personnelles sensibles, notamment avec la constitution du dossier médical en santé au travail.

Ce guide est composé :

- d'un rappel des notions clés
- de 13 fiches thématiques
- de diverses annexes, notamment des modèles de fiches de registre des activités de traitement, un modèle de notice d'information à utiliser pour la gestion du dossier médical en santé au travail ainsi qu'un cahier des charges pour évaluer la conformité de ce dossier au RGPD.

Pour retrouver ce nouveau guide, cliquez sur l'image ci-dessus



Pour retrouver cette synthèse, cliquez sur l'image ci-dessus

ANSSI
Agence nationale
de la sécurité
des systèmes d'information

Publication de la synthèse de la menace ciblant les collectivités territoriales – 23 octobre 2023

Publiant régulièrement un état des lieux de la menace cyber, l'agence nationale de la sécurité des systèmes d'information (ANSSI) a fait paraître en cette fin d'année un panorama de la menace ciblant spécifiquement les collectivités territoriales.

Par ce document, l'ANSSI démontre pourquoi les collectivités sont aujourd'hui une cible de choix ainsi que les moyens principaux utilisés pour leur nuire.

Grâce à ce texte, il est ainsi aisé pour les collectivités de penser leur cyberdéfense en sensibilisant activement leurs collaborateurs et en prévoyant les mesures de sécurité nécessaires en privilégiant les domaines les plus à risques.

JOURNÉE MONDIALE

28 JANVIER 2024

« La sécurité des usages professionnels et personnels »

Nous sommes connectés au quotidien, ce n'est plus un secret. L'arrivée du numérique a amené la société à adapter ses usages. Le développement des technologies mobiles offre désormais la possibilité d'accéder aux informations personnelles et aux systèmes informatiques professionnels depuis presque n'importe où. Pour cette raison, il convient d'adapter nos pratiques afin de protéger tous les espaces de notre vie tant professionnelle comme privée.

C'est ainsi que le Centre de Gestion du Gard, à travers son Service « Protection des données », souhaite (pour continuer avec l'ambiance festive de fin d'année) rejoindre ce 28 janvier la fête européenne et mondiale de la Protection des données et inviter toutes ses collectivités partenaires à sensibiliser sur l'importance de la protection des données personnelles et du respect des libertés et droits fondamentaux, en particulier de la vie privée des administrés et des agents.

Sollicités régulièrement sur ces questions par nos collectivités, nous vous proposons 10 bonnes pratiques à adopter pour la sécurité de vos usages pro-perso.

1

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez.

A défaut, vous risquez qu'une personne malveillante vole votre mot de passe et accède à tous vos autres comptes et services (banque, messagerie, réseaux sociaux). Si vous utilisez ce même mot de passe pour accéder au système informatique de votre collectivité, vous la mettez en péril. En effet, le cybercriminel pourrait voler ou détruire ces informations.

2

Ne mélangez pas vos messageries professionnelle et personnelle.

Cela peut amener à faire des erreurs tel des erreurs de destinataires. En conséquence, vous pourrez envoyer des informations confidentielles de votre collectivité à vos contacts personnels qui pourraient en faire un mauvais usage. Ou, à l'inverse, vous pourrez voir un message trop personnel circuler dans votre environnement professionnel alors que vous ne le souhaiteriez pas.

3

Ayez une utilisation responsable d'internet a votre travail.

L'utilisation d'une connexion internet professionnelle à des fins personnelles peut être tolérée, toutefois votre collectivité est en droit de contrôler l'utilisation de la connexion qu'elle met à votre disposition. N'utilisez donc pas votre connexion professionnelle pour des choses qui pour vous n'ont pas à être connues de votre collectivité.

4

Maîtrisez vos propos sur les réseaux sociaux.

Sur tous vos réseaux sociaux, verrouillez votre profil pour que tout ne soit pas public et avant de poster, demandez-vous toujours si ce que vous communiquez ne pourra pas vous porter préjudice ou à votre entreprise si vos propos étaient relayés par une personne malintentionnée.

DE LA PROTECTION DES DONNÉES

5

N'utilisez pas de services de stockage en ligne personnel à des fins professionnelles.

Ces services de stockage en ligne (Cloud) sont certes pratiques, mais d'un niveau de sécurité faible. Ceci pourrait mettre en danger votre collectivité si votre compte d'accès à ce service était piraté alors qu'il contenait des informations professionnelles.

6

Faites les mises à jour de sécurité de vos équipements.

Il est important d'installer les mises à jour sur vos moyens informatiques personnels et professionnels dès qu'elles sont publiées, elles corrigent les failles de sécurité qui pourraient être exploitées par des cybercriminels.

7

Utilisez une solution de sécurité contre les virus et autres attaques.

Utilisez une solution antivirus et tenez-la à jour. Il vous sera utile lorsque vous subirez des attaques par des virus, des rançongiciels, ou encore de l'hameçonnage.

8

N'installez des applications que depuis les sites ou magasins officiels.

Seuls les sites officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées par un virus. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, ne l'installez pas et choisissez-en une autre.

9

Méfiez-vous des supports USB.

Si vous trouvez ou on vous offre une clé USB partez du principe qu'elle est piégée. Ne la branchez jamais sur vos outils professionnels, vous pourriez ouvrir un accès à un cybercriminel. Utilisez une clé USB pour vos usages personnels et une autre pour vos usages professionnels afin d'éviter que la compromission de l'une ne puisse infecter l'autre.

10

Évitez les réseaux Wi-Fi publics ou inconnus.

Ces réseaux peuvent être contrôlés par des cyber-criminels, lesquels peuvent intercepter vos connexions et récupérer vos comptes d'accès et vos mots de passe personnels ou professionnels, vos messages ou même vos données de carte bancaire afin d'en faire un usage délictueux. Depuis un réseau Wi-Fi public ne transmettez jamais d'informations confidentielles.

Les décisions des autorités chargées de la protection des données

14 septembre 2023 : Italie – 10 000 €

La CNIL italienne a infligé une amende de 10 000 euros à la municipalité de San Severo. La commune avait **publié sur son site Internet un document contenant des données personnelles d'employés sans base légale valable**. Les données publiées concernaient la liste de 140 agents (nom, prénom, catégorie et situation économique, montant de la productivité reconnu).

28 septembre 2023 : Italie – 10 000 €

La CNIL italienne a infligé une amende de 50 000 euros à l'Autorité sanitaire locale du centre de la Toscane. Une personne a signalé que **des dossiers médicaux contenant des données sensibles sur les patients étaient toujours conservés** dans l'un des anciens bâtiments de l'établissement de santé, désormais accessibles au public.

28 septembre 2023 : Italie – 5 000 €

La CNIL italienne a infligé une amende de 5 000 euros au Ministère de l'Environnement et de la Sécurité Énergétique. Le responsable du traitement **avait publié sur son site Internet un document contenant de nombreuses données, notamment des données sur la santé des agents, sans base juridique valable**. Le document a été accessible au public pendant 16 jours.

26 octobre 2023 : Italie – 20 000 €

La Région de Lombardie a été lourdement sanctionnée pour avoir traité des données sans base légale. Ainsi, dans le cadre de la vente d'actions d'une société détenue par la Région, les données personnelles des employés de cette société ont été divulguées illégalement. Les employés ont ainsi découvert que, lorsqu'ils entraient leur nom et prénom dans un moteur de recherche, un lien apparaissait concernant le contrat de vente et lequel permettait d'accéder à des données relatives au revenu et à l'emploi des salariés de cette société.

02 novembre 2023 : Pays-Bas – 30 000 €

La CNIL néerlandaise a infligé une amende de 30 000 euros à la municipalité de Voorschoten. La municipalité avait **conservé les informations sur les déchets ménagers plus longtemps que nécessaire et n'avait pas suffisamment informé les habitants**.

En 2018 et 2019, la commune de Voorschoten a remplacé les poubelles des maisons et les conteneurs souterrains des appartements. Ces bacs étaient équipés de puces dont les numéros étaient liés à l'adresse d'une maison. L'objectif était d'augmenter la collecte sélective des déchets en limitant la quantité de déchets résiduels que les habitants pouvaient éliminer. Cependant, la municipalité a stocké trop longtemps les données de collecte des déchets des ménages. Par ailleurs, la commune n'a pas suffisamment informé les habitants sur l'utilisation de leurs données personnelles lors de la collecte des déchets.

07 novembre 2023 : Grèce – 5 000 €

Une commune grecque s'est vue infliger une sanction pour avoir publié les données personnelles d'une personne sur son site internet et **ne pas s'être conformée à la demande de suppression** formulée par ladite personne concernée, conformément à son droit reconnu par l'article 17 du RGPD.

09 novembre 2023 : France – Rappel à l'ordre

La CNIL a rappelé à l'ordre le ministère de la Transformation et de la Fonction publiques et le ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique pour avoir utilisé un fichier administratif contenant les coordonnées des agents publics à des fins de communication politique sur le projet de réforme des retraites. Or, en utilisant les adresses mail des agents publics, les ministères ont utilisé ces données de manière incompatible avec l'objet du fichier.

16 novembre 2023 : Espagne – 20 000 €

Un citoyen espagnol a porté plainte à l'encontre du parti politique asturien « *Foro Asturias* ».

Le parti est accusé d'avoir **transmis des données à caractère personnel de manière illégitime**. Ces données ont fait l'objet d'une publication dans la presse nationale sous la forme d'une photographie qui montre une quantité importante d'informations sur la personne concernée y compris son numéro de compte bancaire courant ainsi que des données professionnelles.

La CNIL espagnole a ainsi prononcé une amende de 20 000€ à l'encontre du parti pour avoir manqué au principe de confidentialité.

27 novembre 2023 : Norvège – 1 700 000 €

L'autorité norvégienne de protection des données a prononcé une sanction de 1 700 000 € à l'Agence norvégienne du travail et de la protection sociale (NAV).

Cette notification fait suite à une inspection au cours de laquelle l'autorité a constaté plusieurs écarts graves en termes de sécurité des informations dans les systèmes informatiques de la NAV. Un total de 12 violations au RGPD ont été identifiées regroupant des **défaillances dans la politique de gestion des accès, la tenue et le contrôle des journaux dans les solutions informatiques**. Aucun contrôle de l'utilisation des systèmes informatiques par les agents n'a été mis en place. Toutes ces raisons et afin d'avoir un effet dissuasif, ont motivé la CNIL norvégienne à opter pour une sanction d'un montant élevé.

28 NOVEMBRE 2023 : SUÈDE – 26 500 €

L'autorité suédoise de protection de la vie privée a déclaré que le conseil de l'enfance et de l'éducation de la municipalité d'Östersund **a manqué à son obligation** en vertu de l'article 35.1 du RGPD **de procéder à une analyse d'impact** avant que le service Google Workspace ne commence à être exploité dans 24 écoles de la Municipalité en 2020.

Google Workspace fournit un service pour l'enseignement et la communication entre les éducateurs et les étudiants. Sont ainsi concernées les données de presque 6000 étudiants et 1300 agents pour lesquelles l'impacte sur la vie privée n'avait pas été analysée préalablement à la mise en place du traitement de données.

06 DÉCEMBRE 2023 : ISLANDE – 85 100 € CUMULÉS

Les communes islandaises de Kópavogur, Hafnarfjörður, Garðabær, Reykjavik et Reykjanesbær ont été sanctionnées de plusieurs amendes pour un montant cumulé de 85 100 €.

Les communes avaient ainsi utilisé le système Google Education sans respecter suffisamment les règles de protection des données. En particulier, ces villes n'avaient pas rempli leurs obligations en sélectionnant Google comme sous-traitant et **le contrat de sous-traitance** avec Google **n'était pas conforme aux exigences en matière de protection des données**.

De plus, les villes n'avaient pas veillé à ce que les données des étudiants **ne soient pas traitées à des fins autres que celles spécifiées préalablement**. En outre, la **durée de conservation n'a pas été jugée appropriée mais plutôt trop longue**.

Une attention particulière a été accordée par la CNIL islandaise à la protection des données sensibles des enfants. Bien qu'aucun dommage démontrable n'ait eu lieu, il a été critiqué que chaque ville n'ait pas suffisamment encadré le transfert sécurisé des données vers les États-Unis. Cependant, il a été noté que les villes ont coopéré de manière transparente avec l'autorité de protection des données et ont depuis révisé leurs pratiques en matière de protection des données.

12 décembre 2023 : France – 5 000 €

Nous en avions déjà parlé dans notre numéro du mois d'octobre 2023, mais la CNIL avait sanctionné pour la première fois en février dernier une commune dont le nom n'avait pas été révélé pour **ne pas avoir désigné de délégué à la protection des données**.

La commune, qui avait en outre reçu une injonction de se mettre en conformité sous un délai de trois mois, n'en a pourtant rien fait et n'a toujours ni désigné de délégué, ni répondu à la CNIL. L'autorité de contrôle a ainsi décidé d'initier une nouvelle procédure de sanction, cette fois-ci publique.

Ainsi, la **commune de Kourou** (Guyane) s'est vue infligée une nouvelle sanction de 5 000 € assortie d'une nouvelle injonction de se mettre en conformité dans un délai de deux mois. Cette sanction est par ailleurs assortie d'une astreinte de 150 € par jour de retard.

La CNIL a par ailleurs renforcé cette sanction par deux moyens : **d'une part en la rendant publique**, et d'autre part en ordonnant à la commune **d'afficher pendant quatre jours un message d'information à destination des usagers sur son site web**.

Lien vers le communiqué de la CNIL :

CNIL.

22 décembre 2023 : France – Amende

Dans le cadre de sa procédure simplifiée (*Voir Cyberactu' – octobre 2023*), la CNIL a infligé une amende envers une nouvelle commune, dont ni le nom, ni le montant de l'amende n'ont été révélés.

Il apparaît cependant que l'autorité de contrôle a constaté un défaut majeur de sécurité des données des administrés, notamment en ce qui concernait les **précautions minimales en matière de robustesse et de stockage des mots de passe**.

Si le montant de l'amende n'a pas été révélé, la CNIL rappelle cependant qu'une sanction avait été infligée envers une entreprise privée pour des faits similaires le 28 juillet 2020, prononçant à cette occasion une amende de 250 000 € ainsi qu'une injonction de se mettre en conformité assortie d'une astreinte de 250 € par jour de retard.

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Assemblée nationale
18 novembre 2023

Ozoire-la-Ferrière
09 décembre 2023

CC Les Portes Briardes
09 décembre 2023

CC du Pays du Neubourg
1er décembre 2023

Ministère du Travail (Plateforme « La bonne alternance »)
1er décembre 2023

EHPAD de Marigny-Le-Lozon
23 octobre 2023

Ministère de l'Education nationale (Plateforme du SNU)
05 décembre 2023

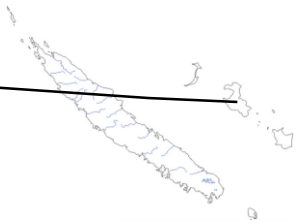
Département du Loiret
11 novembre 2023

Syndicat interdépartemental pour l'assainissement de l'agglomération parisienne
19 novembre 2023

SDIS 64
12 octobre 2023

Mairie et CA du Puy-en-Velay
17 octobre 2023

Province des Îles Loyauté
08 décembre 2023



** Sur les trois derniers mois*

BONNES RÉSOLUTIONS : C'EST LE MOMENT !

« *Bien mal acquis ne profite jamais* », disait l'adage que nos aïeux avaient la joie d'apprendre lors de leur leçon de morale par un instituteur sévère et à la punition facile.

Pour autant, à toujours mettre en avant les échecs, les accidents et les sanctions, l'on en oublierait presque que le respect des règles, quant à lui, profite ! Lequel de nos aïeux ne nous a jamais raconté sa fierté de ramener à ses parents le bon point distribué par son instituteur parce qu'il avait parfaitement su réciter sa leçon ? Quel malade n'a jamais été reconnaissant envers son médecin pour lui avoir préconisé et recommandé de suivre le bon traitement ?

Car oui, on ne le répètera jamais assez : le respect des règles paie ! Surtout dans le monde de la protection des données…

Car, hélas, la question n'est pas de savoir si l'on va être attaqué un jour, mais plutôt de savoir quand et avec quels moyens !

Paralysée en décembre 2020 par une cyberattaque, la ville de Bayonne a ainsi investi pas moins de 50 000 € par an pour s'offrir la protection d'un nouveau logiciel dédié à la lutte contre les cybermenaces.

Hôtel de Ville de Bayonne (Source : bayonne.fr)

Interrogé à l'époque par France Bleu, Olivier Alleman, conseiller municipal de Bayonne délégué à la Ville numérique, rapportait entre 250 et 350 attaques par jour ! Il est donc plus qu'évident qu'au moment ou nous écrivons ces lignes, comme au moment ou vous les lirez, un grand nombre d'attaques ciblent votre propre système d'information.

Mais alors, pourquoi le site internet de la Ville de Bayonne est-il toujours en ligne à ce jour ? Comment ses services arrivent-t-ils encore à éditer tous les actes liés à leurs missions de service public malgré ces centaines d'attaques quotidiennes ? La réponse est simple : l'application de mesures de protection élémentaires.

SAUVEGARDE EST MÈRE DE SÛRETÉ

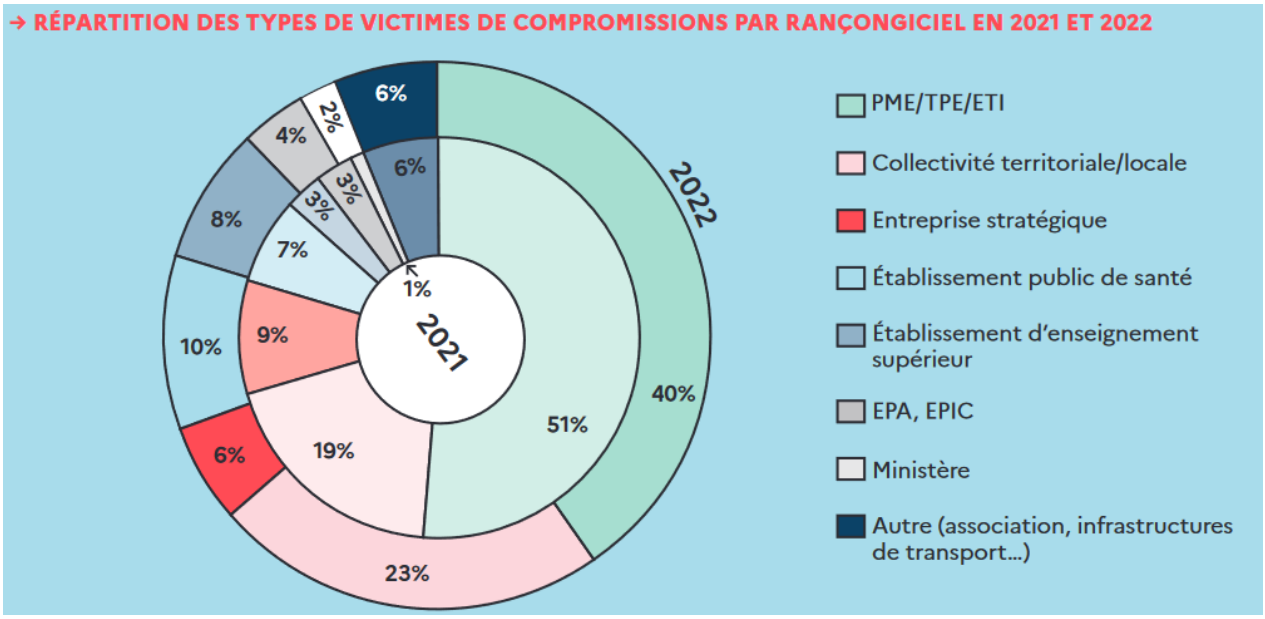
Prenons l'exemple de Marie-Amélie, secrétaire générale d'une petite commune fictive. Nous sommes lundi. Après deux jours de repos auprès de sa famille, la secrétaire arrive, par ce froid matin de janvier. Posant sa tasse

de café bien chaud près de son clavier, elle allume son écran qu'elle se contente d'éteindre le soir quand elle s'en va. Après tout, c'est moins contraignant que de devoir éteindre cette chose qui met un temps infini à s'allumer et sur lequel il faut en plus saisir un mot de passe long et complexe que son prestataire informatique lui a imposé… Pas encore très bien réveillée, Marie-Amélie met quelques secondes avant de prendre conscience que, cette fois-ci, quelque chose ne va pas : au lieu de la photo de son petit-fils en arrière plan de son écran, c'est au contraire un fond noir qui s'affiche. Les icones des dossiers semblent différents et les textes affichés sont illisibles. Tous les fichiers semblent avoir été renommés par un chat ayant marché au hasard sur le clavier. Marie-Amélie comprend alors que l'impensable c'était produit en son absence : la Mairie avait été victime d'une cyberattaque…

Après une rapide vérification du prestataire informatique de la commune, le verdict est sans appel : l'intégralité des fichiers informatiques de la Mairie sont perdus. En entendant la triste nouvelle, Marie-Amélie se sent défaillir. Des années de travail ont été perdus. Cela va lui prendre des mois pour reconstituer de quoi assurer un service minimal !

Alors que les larmes lui viennent aux yeux, un large sourire se dessine sur le visage de son informaticien : les sauvegardes ont fonctionné. La secrétaire ne comprend pas tout de suite ce que cela signifie. Son prestataire lui explique alors la teneur de ce miracle : les sauvegardes qu'il a programmé (« *et qui ont coûté cher* », pensa Marie-Amélie) ont sauvé l'intégralité des données. Il ne lui faudra que quelques heures pour relancer l'activité de la commune. En entendant la nouvelle, la secrétaire se met à pleurer de joie… Car oui, comme le montre cet exemple fictif, la sauvegarde régulière est la mesure essentielle à la protection des données d'une collectivité ou d'un établissement public. Une telle mesure permet, en cas de défaillance, de conserver l'ensemble du travail accompli et de relancer l'activité de la collectivité en peu de temps. C'est ainsi que la Mairie de Bayonne, dans son malheur survenu en décembre 2020, a pu reprendre une activité normale en un week-end !

C'est également ce qui a sauvé l'activité de la Mairie de Morlaix, attaquée le 21 septembre dernier. Malgré un très bon niveau de sécurité, une cyberattaque a réussi à faire tomber deux des trois serveurs de la commune qui a été sauvée grâce à ses sauvegardes quotidiennes. Jean-Paul Vermot, Maire de Morlaix, sensible à la cause de la sécurité numérique, s'y attendait et avait ainsi pris toutes les mesures pour protéger sa collectivité des criminels numériques. Les collectivités sont en effet de plus en plus ciblées par les cyberattaques, notamment les rançongiciels qui se développent



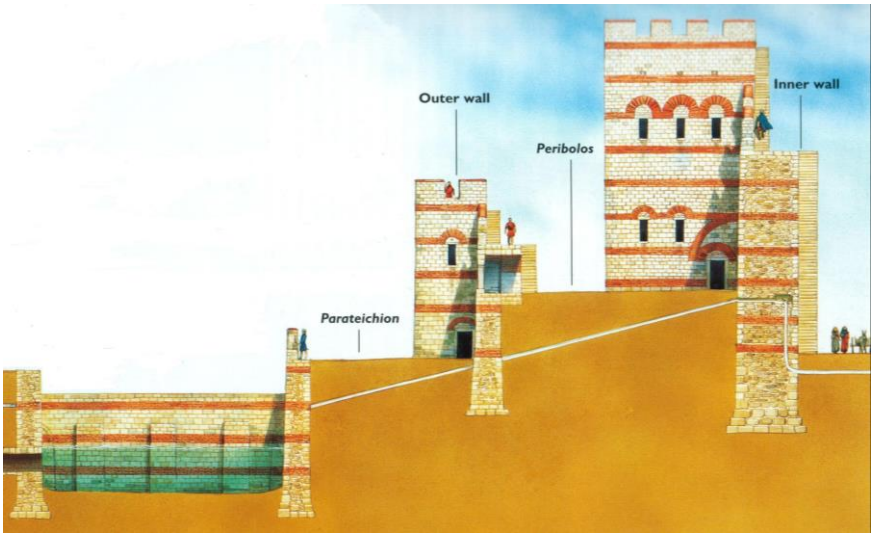
Source : Panorama de la cybermenace 2022 – Agence nationale de sécurité des systèmes d'information

de plus en plus ces dernières années. Hélas, comme le montre cette attaque, même avec toutes les mesures de protection du monde, un cybercriminel particulièrement doué peut arriver à s'introduire partout. La seule mesure de protection efficace reste la sauvegarde en amont, qui permet de restaurer l'intégralité de ce qui peut être perdu dans une attaque.

Mieux vaut prévenir que guérir

Pour autant, sauvegarder ses données ne suffit pas à assurer sa sécurité numérique ! Combien de collectivités ont vu leur support de sauvegarde être lui-même compromis lors d'une attaque ! Certains criminels n'hésitent d'ailleurs pas à cibler en priorité les sauvegardes, conscients de leur valeur, en installant un programme qui ne s'activera qu'une fois sauvegardé avec le reste des données. Oui, la cybersécurité prend parfois des allures de conflit militaire, avec ses armes et ses stratégies.

C'est d'ailleurs sous cet angle que nous présenterons ce que les spécialistes de la cybersécurité dénomment « la défense en profondeur ». Derrière ce terme technique se cache la pensée selon laquelle il ne sert à rien de tenter d'empêcher un assaillant de franchir les défenses du système d'information à tous prix, puisque celui qui y mettra les moyens pourra y parvenir. La défense en profondeur a, en réalité, pour but de retarder l'assaillant à tel point qu'il finira pas se détourner de sa cible pour en attaquer une autre.



Coupe de la muraille de Théodose, défendant Constantinople (aujourd'hui, Istanbul)

Afin d'illustrer cette théorie, prenons un exemple historique : le siège de Constantinople en 1453. La capitale de l'Empire byzantin, assiégée par une armée de 100 000 ottomans, ne pouvait compter que sur 7 000 hommes pour se défendre. Et malgré ce, la ville a réussi à tenir face à l'assaillant pendant près de deux mois sans que la muraille ne soit prise. Comment est-ce possible ?

Il faut savoir que Constantinople était alors sans doute la ville la mieux défendue au monde. Sa muraille présentait en effet un nombre impressionnant de lignes de défense successives qui garantissaient chacune la sécurité de la ville si l'une de ces lignes de défense venait à tomber. Le fossé venait à tomber ? Le mur extérieur était là pour interdire l'entrée de la cité aux ottomans. Le mur extérieur était pris ? Le mur intérieur surmontant un second fossé laissait aux archers byzantins le soin de repousser les assaillants.

Car c'est cela, la défense en profondeur : une succession de mesures de sécurité destinées à ralentir l'ennemi. Si notre exemple se base sur la défense d'une ville au XV^{ème} siècle, la logique reste aujourd'hui la même pour la cyberdéfense. Les murailles physiques ont simplement été remplacées par de nouvelles murailles numériques. Fini les fossés, bonjour les pare-feu ! Terminé les herses et les murs, remplacés par les mots de passe et les antivirus !

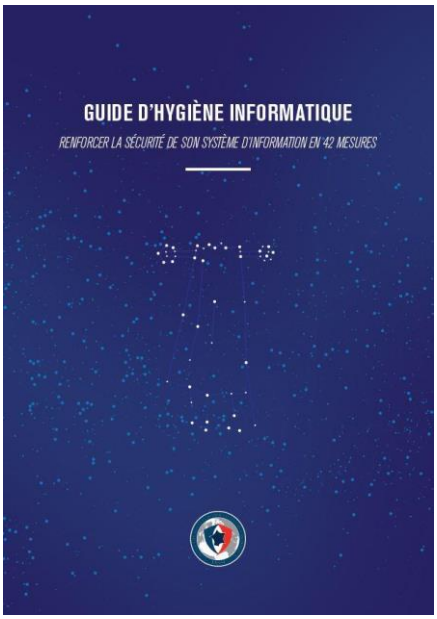
Comme dit précédemment, l'objectif d'une telle défense est de retarder suffisamment l'assaillant pour que celui-ci ne se détourne vers des cibles plus faciles. Car la cybercriminalité aujourd'hui suit souvent une logique financière, et une attaque trop longue ou nécessitant de trop gros moyens ne devient plus assez rentable.

Il est donc aujourd'hui relativement aisé de se protéger. Rappelons nous de l'exemple de la Mairie de Bayonne, qui parvenait à repousser entre 250 et 350 attaques par jour ! Appliquer les règles d'hygiène

numérique est donc aujourd'hui un indispensable pour s'assurer d'une relative tranquillité dans notre activité quotidienne.

Mais quelles sont-elles ces règles d'hygiène numérique ?

Heureusement, l'ANSSI a publié de nombreux guides destinés à comprendre et à mettre en place ces règles simples et parfois oubliées.



Guide d'hygiène informatique - ANSSI

Les principales mesures restent très simples : mettre à jour son infrastructure, réaliser des sauvegardes régulières, sécuriser son poste de travail, ou encore mettre en place un mot de passe robuste et conforme aux exigences de l'ANSSI.

Une complexité apparente

La terminologie de ces mesures peut évidemment faire peur. Pourtant, les mesures minimales de sécurité sont très simples à mettre en œuvre, et les guides destinés aux débutants sont de plus en plus nombreux. Mais le plus sûr est encore d'avoir affaire à un professionnel en la matière, qu'il s'agisse de votre responsable informatique ou d'un prestataire extérieur, qui saura paramétrer le système d'information de la collectivité.

Il est évident que l'application de ces mesures de sécurité est parfois contraignante. Qui n'a jamais soufflé du nez en devant saisir une suite de chiffres et de lettres (sans oublier les caractères spéciaux !) d'une longueur à faire pâlir les plus patients d'entres-nous ? Pour autant, ces mesures ne sont pas préconisées pour rien.

Lorsque le 1er octobre 1979 est décidé de l'obligation du port de la ceinture de sécurité au volant, une partie des conducteurs de l'époque avaient également été outrés de cette entrave à leur liberté. Pourtant, plus de 40 ans après, il ne viendrait plus à l'idée de personne de censé de se passer de cette mesure de sécurité élémentaire. Il est donc évident que si les mesures de sécurité informatique sont encore aujourd'hui vues comme des contraintes, celles-ci rentreront également dans les mœurs au fur et à mesure que les utilisateurs en comprendront l'utilité et en acquerront l'automatisme.

Il ne faut donc pas avoir peur d'en imposer l'application dans un premier temps pour permettre même aux plus récalcitrants d'acquérir cet automatisme, tout en accompagnant ces nouvelles mesures par une sensibilisation de chaque instant.

La sécurité, avant tout une affaire de sensibilisation ?

Car c'est bien de la sensibilisation de chacun que naitra notre sécurité collective. Il ne sert à rien d'imposer les meilleures mesures de sécurité techniques si une erreur d'origine humaine vient en compromettre l'efficacité.

Reprenons notre exemple du siège de Constantinople. Malgré les éloges que nous avons portés sur les défenses de la cité au début de notre dossier, les amateurs d'Histoire auront cependant compris que, si cette cité s'appelle aujourd'hui Istanbul, c'est bien parce que malgré ses hautes murailles, la ville a fini par tomber. Mais, Ô surprise, ce n'est pas suite à la prise de la muraille…

En effet, deux éléments sont responsables de la chute de la ville face aux troupes ottomanes. Tout d'abord, les défenseurs ont laissé une poterne (une petite porte) ouverte, ce qui a permis l'intrusion de soldats ottomans. D'autre part, au même moment, Giovanni Giustiniani, principal général byzantin, était blessé et évacué du champ de bataille, semant la panique chez les défenseurs qui ont vu, au même moment, la bannière ennemie flotter au dessus de la petite porte qui venait d'être découverte. Ces deux éléments conjugués ont ainsi entraîné la

chute de la cité sans que les murailles ne tombent face aux canons ottomans.

Cet exemple est ici à mettre en parallèle avec ce qui pourrait se passer demain malgré toutes les mesures de sécurité installées sur un système d'information : une simple erreur humaine peut entraîner la compromission de tout un système. Une pièce jointe infectée sur laquelle on clique, un mot de passe mal choisi ou noté sur un post-it collé sur l'écran, un mail envoyé par erreur à la mauvaise personne… L'erreur humaine est aujourd'hui la menace principale pour un système d'information.

Mais plus que l'erreur humaine, c'est toute l'ingénierie sociale qui peut servir d'arme à un attaquant expérimenté. En posant les bonnes questions et en manipulant son interlocuteur, un attaquant peut extorquer les informations nécessaires pour parfaire son attaque. Il est donc essentiel que chacun et chacune soit sensibilisé à la cause de la protection des données afin d'éviter toute erreur qui risquerait d'entraîner des conséquences dramatiques.

Sécurité et sensibilisation, les meilleures résolutions

Parce que la cybersécurité dépend avant tout de son organisation, il est essentiel de mettre en place un plan destiné à sécuriser sa collectivité et son système d'information. Cela peut passer par des actions de sensibilisation et la mise en place de mesures plus techniques. Mais il est important que ce plan soit adapté aux besoins et à la taille de la collectivité ainsi qu'à son fonctionnement afin que tous, agents comme élus, puissent se sentir impliqués et concernés par sa réalisation.

Enfin, il est également à noter que, pour faire face à la menace croissante des cyberattaques, l'Union européenne a décidé d'imposer de nouvelles règles en matière de sécurité des systèmes d'information via le vote et l'entrée en vigueur de la directive NIS-2 (pour « *Network and Information Security* » version 2). Les États membres ont ainsi jusqu'au 18 octobre 2024 pour voter la transposition de ladite directive qui va venir imposer aux collectivités de nouvelles mesures dont le détail sera connu en début d'année.

Alors, pour la nouvelle année qui commence, et si la cybersécurité faisait partie de nos bonnes résolutions ? ■

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention
en sécurité numérique

Adieu les courriels malveillants, je passe par voie aérienne.

FACE AUX RISQUES CYBER VOUS N'ÊTES PAS SEUL.

De vraies solutions existent.

Conseils, assistance et mise en relation, avec des professionnels
en cybersécurité sur Cybermalveillance.gouv.fr

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

TOUS ENSEMBLE
PRUDENCE SUR INTERNET

EN LIGNE, AS-TU LES BONS RÉFLEXES ?

QUIZ **Réponds aux questions ci-dessous, et compte combien tu as de :**

△ : .....
◇ : .....
○ : .....

1 Pendant une partie de jeu en ligne, Samouraï_du_69 veut discuter avec toi. C'est un joueur que tu ne connais pas.

△ Tu l'ignores, car tu ne parles jamais à des inconnus !

◇ Tu lui écris : « On se connaît ? »

○ Vous discutez pendant toute la partie, il est trop sympa ! Tu lui racontes ta vie !

2 Tu as très envie de t'inscrire sur le réseau social Tacotac pour mettre des vidéos en ligne. Mais dans le formulaire à remplir, il faut avoir plus de 13 ans !

◇ Tu vas en discuter avec tes parents : on ne sait jamais, ils seront peut-être d'accord pour te créer un compte !

○ Tu mets la date de naissance de ton papa, il a largement plus de 13 ans !

△ Tu te dis : « Dommage, il va falloir attendre ! »

3 Pour accéder à une appli, tu dois te créer un mot de passe...

◇ Tu choisis le mot de passe compliqué que tu mets partout.

△ Tu mélanges majuscules, minuscules, chiffres et ponctuation.

○ Tu mets 1234.

4 Pour débloquer un accessoire pour ton personnage dans le jeu, il faut payer...

○ Ta maman a enregistré sa carte bleue dans son téléphone, ça va être simple.

△ Tant pis pour eux, ils n'auront pas ton argent !

◇ Tu demandes à ton papa qu'il te l'offre pour ton anniversaire.

5 La grande sœur de ta copine est sur Tacotac. Dans sa dernière vidéo, elle montre comment elle se maquille...

△ Tu ne l'as pas vue, car tu n'as pas Tacotac.

○ Tu mets un smiley qui vomit en commentaire.

◇ Tu likes, ça lui fera plaisir !

6 À l'anniversaire de Tom, tu as pris des photos et des vidéos de tous les invités.

○ En rentrant, tu les publies sur ton profil en mode public en taguant tes amis.

◇ Tu crées un groupe fermé pour partager ces photos.

△ Tu envoies à chacun par e-mail les photos et les vidéos sur lesquelles il apparaît.

7 L'appli de jeu que tu veux installer te demande d'indiquer ton adresse.

◇ Tu inventes une adresse bidon.

△ À quoi peut bien leur servir ton adresse ? Tu désinstalles l'appli.

○ Toi, ce que tu veux, c'est jouer ! Tu remplis et tu cliques sur « OK » !

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

TOUS ENSEMBLE
PRUDENCE SUR INTERNET

8 Quand tu regardes des vidéos en ligne :

△ Tu règles les paramètres pour que les vidéos ne s'enchaînent pas automatiquement.

○ Tu adores, parce que les vidéos s'enchaînent sans que tu choisisses.

◇ Tu as vu une vidéo horrible qui t'a dégoûté(e), tu en parles à tes parents pour qu'ils modifient les réglages.

9 Quand tu accèdes à un site web :

◇ Tu refuses tous les cookies, sauf ceux qui t'empêchent d'accéder aux pages qui t'intéressent.

△ Tu refuses tous les cookies puis tu effaces l'historique.

○ Tu cliques sur « Accepter » dès qu'on te le demande, sinon, ça t'énerve, ça bloque !

Fais passer le test à tes parents ! Sont-ils vraiment prudents ?

Tu as un maximum de...

△ Bravo ! En ligne, tu as les bons réflexes !

Sur Internet, tu es très prudent(e) et très conscient(e) qu'il y a des risques. On dirait que tu as suivi nos conseils... super ! N'hésite pas à montrer nos vidéos et à expliquer ta façon de faire à ton entourage, tu rendras service à beaucoup de monde !

◇ Pas mal, mais tu peux encore t'améliorer !

En ligne, c'est un peu comme dans la vraie vie. Peut-être que tu ne rentres pas encore tout(e) seul(e) de l'école à pied et que tu ne prends pas le train sans être accompagné(e), mais ça va venir ! Derrière l'écran, c'est pareil : continue à être prudent(e) et demande conseil dès que tu as un doute. Regarde à nouveau nos vidéos, tu vas découvrir des choses qui t'avaient échappé.

○ Tu as encore des progrès à faire...

Toi, à tous les coups, tu plongeais dans le grand bassin de la piscine sans savoir nager ! En ligne, tu ne fais pas attention à ce que tu fais. C'est dangereux pour toi, pour tes ami(e)s, pour tes parents. Internet, c'est un monde passionnant et excitant, mais il faut que tu sois plus prudent(e). Pour ça, regarde à nouveau les vidéos et reprends toutes les questions du jeu !

Découvre tous les conseils de la CNIL en te rendant, seul(e) ou avec tes parents, sur cnil.fr/fr/education

Illustrations : Alexandre Franc. Texte : Anne Bideault. Réalisé par Bayard Media Développement.

Gestion et conservation des archives : les bonnes pratiques

« *Les **archives** sont l'ensemble des **documents**, y compris les **données**, quels que soient leur **date**, leur **lieu de conservation**, leur **forme** et leur **support**, produits ou reçus par toute personne physique ou morale, et par tout service ou organisme public ou privé, **dans l'exercice de leur activité*** »

Code du Patrimoine, article L.211-1, modifié par loi n°2016-925 du 7 juillet 2016 - art. 59

Ainsi, quel que soit le service public, les documents produits sont des archives publiques.

Les conserver, les protéger et les valoriser permet de sauvegarder l'histoire de votre collectivité, autant d'un point de vue juridique qu'historique.

Prenant ces éléments en compte, voici quelques conseils à suivre pour, dans un premier temps, **constituer un dossier à archiver :**

- Ouvrir un dossier pour toute nouvelle affaire.
- Le mettre en ordre grâce à des chemises et sous chemises de couleurs neutres et constituer si possible un dossier qui n'excède pas 10 cm d'épaisseur (le scinder si besoin).
- L'identifier avec un titre précis (objet, résumé du contenu) et une date (date d'ouverture, de clôture, année).
- Bannir les éléments nocifs pour la conservation des documents : les objets métalliques (trombones, agrafes), les élastiques, la colle, le ruban adhésif, ainsi que les fiches plastiques.
- Éliminer les pièces sans valeur historique ou administrative : doubles et copies inutiles, post-it, brouillons, documentation.
- Conditionner les dossiers dans des boites archives conformes et de taille adaptée aux dossiers.

Attention !

concernant les actes administratifs (délibérations, arrêtés et procès-verbaux), ces derniers doivent être reliés en suivant la réglementation en vigueur.

Ensuite, **lors du rangement en salle archives ou dans un espace de stockage**, il convient de respecter quelques règles pour créer un espace optimisé et sécurisé :

- Ranger vos boites de manière thématique pour vous y retrouver, sans surcharger les étagères. N'oubliez pas que le poids de 20 boites d'archives est d'environ 100 kg !
- Afin d'assurer une bonne conservation des documents, l'espace choisit doit être sécurisé et désencombré de tout objet autre. Il ne doit pas subir de variations importantes de température ni d'hygrométrie. Il faut éviter l'éclairage naturel et prévoir un éclairage artificiel de max 200 lux. Les rayonnages doivent être métalliques, ils sont plus résistants et n'attirent pas les insectes xylophages. Penser également à la résistance au sol qui doit être suffisante (900kg/m2). Et concernant la sécurité incendie, il vous faut un dispositif d'alarme et des extincteurs sans additifs.

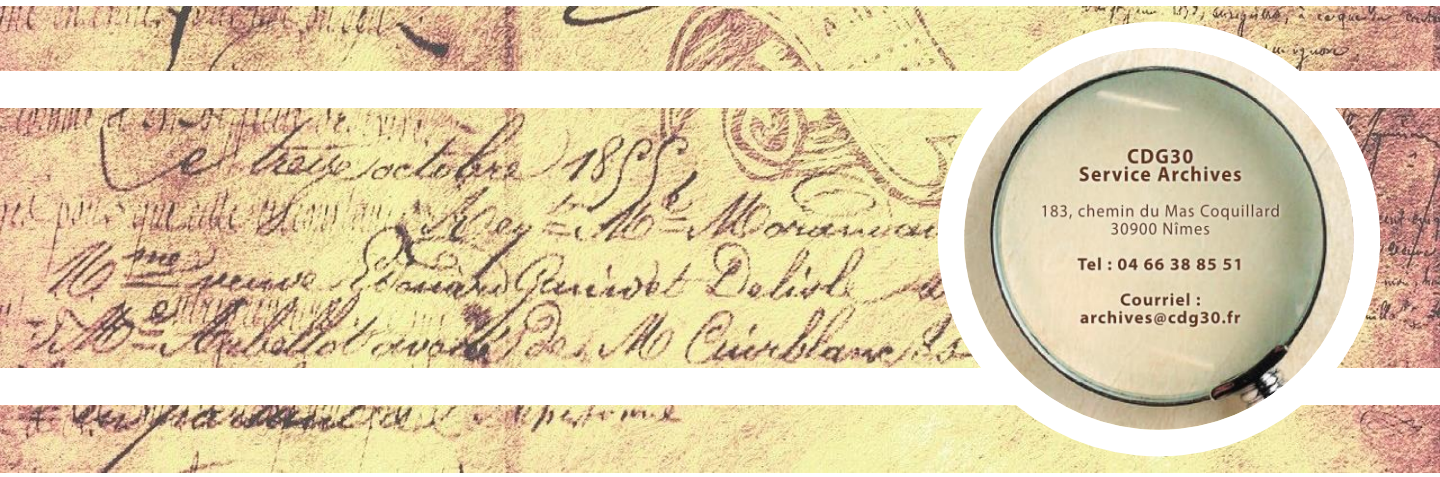
À savoir, pour l'aménagement de votre local, des subventions peuvent être attribuées par les Archives Départementales

Pour aller plus loin : quelques étapes pour un archivage de qualité

- Créer un répertoire thématique et chronologique de vos dossiers, en y mentionnant les intitulés de chaque dossier et leurs dates extrêmes.
- Identifier les archives définitives et les archives éliminables à terme grâce à un tableau de gestion de vos documents se référant aux circulaires de tri et de conservation des archives publiques.
- Rédiger une fois par an, un bordereau des archives pouvant être éliminées puis soumettez le au visa de la Direction des Archives Départementales.
- Après validation de votre bordereau par celle-ci, vous pourrez entamer la procédure pour l'élimination en interne ou avec un prestataire extérieur certifié.

Ces étapes réalisées, vous assurerez l'identification et la conservation de vos archives en optimisant votre temps de recherche et votre espace de stockage dans le respect de la réglementation en vigueur.

Plus d'infos sur l'espace « Archives » du site internet cdg30.fr



LE BON GESTE

LA BONNE TENUE DE LA LISTE ÉLECTORALE

Les communes ont la charge de constituer et de tenir à jour les listes électorale. En cette année d'élections européennes, notre service a souhaité vous aider à constituer la liste électorale de votre commune dans les règles de l'art, tout en assurant une communication et une transmission des informations présentes sur ladite liste conforme au RGPD.

LA RECOMMANDATION DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

NE COLLECTER QUE LES DONNÉES NÉCESSAIRES

Inscriptions sur la liste électorale	
Type de données pertinentes	**Comment les collecter ?**
Identité et coordonnées de l'électeur Nom, prénom, sexe, date et lieu de naissance, adresse, téléphone, mail Type et motif de demande d'inscription (déménagement, etc.)	Ces données sont nécessaires pour traiter les demandes d'inscription et vérifier que les administrés remplissent bien les conditions pour être électeurs. Elles peuvent être demandées via une copie de la carte d'identité ou un justificatif de domicile

Transmission de la liste électorale	
Type de données pertinentes	**Comment les collecter ?**
Identité et coordonnées du demandeur Nom, prénom, date et lieu de naissance, adresse	Ces données sont nécessaires pour vérifier que le demandeur dispose bien de la qualité pour accéder à la liste électorale. Une copie de sa carte d'identité peut lui être demandée. Le demandeur devra en outre fournir une **attestation sur l'honneur à ne pas faire un usage commercial de la liste électorale**. La commune peut lui demander des précisions sur l'usage qui en sera faite, même si cette demande ne doit pas être systématique.

Attention : collecte particulière pour la radiation de la liste électorale

Pour identifier les électeurs à radier de la liste électorale, les communes doivent se fier à **un faisceau d'indices prouvant que l'administré ne remplit plus les conditions d'inscription sur la liste électorale communale**.

Cela passe notamment par les retours de courriers de propagande ou de carte électorale sur lesquels sont apposés la mention « N'habite pas à l'adresse indiquée », ou encore par une consultation des fichiers liés à la fiscalité locale.

Il peut être difficile d'identifier les électeurs à radier, et ladite radiation ne peut être prononcée qu'après **avoir notifié à l'électeur cette décision de radiation assortie d'un délai de 15 jours pour présenter ses observations**.

De plus, il est essentiel de garder à l'esprit que les témoignages des autres administrés ne peuvent pas constituer un faisceau d'indices et ne sauraient être collectés ni conservés comme preuve justifiant la radiation.

INFORMER CORRECTEMENT LES PERSONNES DE L'UTILISATION DE LEURS DONNÉES

Concernant **l'inscription sur les listes électorales**, la mention d'information est inscrite directement sur l'outil proposé par les services de l'État (formulaire CERFA ou démarche en ligne).

Cependant, une mention d'information pourra être mise en place pour les notifications de radiation transmises aux administrés dont le faisceau d'indices laisse à supposer qu'ils ne remplissent plus les conditions d'inscription.

De plus, une mention d'information particulière sera à adopter par la commune concernant **les demandes de transmission de la liste électorale**. Celle-ci devra être fournie à l'administré lors de sa demande, soit par voie d'affichage (par exemple, à l'accueil de la commune), soit sur le formulaire collectant les données de la demande si la commune en a créé un.

Retrouvez en page suivante nos exemples de mentions d'information dédiées

Exemples de mentions d'information

Mention d'information notification de la radiation de la liste électorale
Les données personnelles que vous nous communiquez seront utilisées dans le seul but de contrôler la validité de votre inscription sur la liste électorale, conformément aux dispositions des articles L9 à L15-1 du code électoral et ne seront traitées que par les services de la Mairie de **[X]**, représentés par son Maire, en tant que responsable de traitements. Les données ne seront pas utilisées à des fins sortant du cadre de cette vérification. Vos informations personnelles seront conservées pendant une durée de 3 ans, conformément aux recommandations de l'instruction DAF/DPACI/RES/2009/018 du 28 août 2009. Vous disposez d'un droit d'accès, d'interrogation et de rectification qui vous permet, le cas échéant, de faire rectifier, compléter, mettre à jour, verrouiller ou effacer les données personnelles vous concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Pour exercer vos droits Informatique et Libertés et pour toute information sur ce dispositif, contactez nos services à l'adresse [**adresse mail]**, ou par voie postale à l'adresse suivante : [**Adresse postale]** Si vous estimez, après nous avoir contactés, que vos droits Informatique et Libertés ne sont pas respectés ou que le dispositif de contrôle d'accès n'est pas conforme aux règles de protection des données, vous pouvez adresser une réclamation à la CNIL.

Mention d'information transmission de la liste électorale
Les données personnelles que vous nous communiquez seront utilisées dans le seul but de répondre à votre demande de transmission d'un extrait de la liste électorale, conformément aux dispositions de l'article L37 du code électoral et ne seront traitées que par les services de la Mairie de **[X]**, représentés par son Maire, en tant que responsable de traitements. Les données ne seront pas utilisées à des fins sortant du cadre de cette demande. Vos informations personnelles seront conservées pendant une durée de 3 ans, conformément aux recommandations de l'instruction DAF/DPACI/RES/2009/018 du 28 août 2009. Vous disposez d'un droit d'accès, d'interrogation et de rectification qui vous permet, le cas échéant, de faire rectifier, compléter, mettre à jour, verrouiller ou effacer les données personnelles vous concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation est interdite. Pour exercer vos droits Informatique et Libertés et pour toute information sur ce dispositif, contactez nos services à l'adresse [**adresse mail]**, ou par voie postale à l'adresse suivante : [**Adresse postale]** Si vous estimez, après nous avoir contactés, que vos droits Informatique et Libertés ne sont pas respectés ou que le dispositif de contrôle d'accès n'est pas conforme aux règles de protection des données, vous pouvez adresser une réclamation à la CNIL.

UTILISER LES DONNÉES CONFORMÉMENT À LA RÉGLEMENTATION

LA COMMUNICATION POLITIQUE

Ni le code électoral, ni la réglementation relative à la protection des données personnelles ne s'opposent à ce qu'un Maire (comme un tiers) utilise la liste en période électorale. Cependant, dans un soucis d'égalité entre les candidats (et plus largement, d'égalité entre demandeurs), le « Maire candidat » doit **s'imposer strictement les mêmes règles** que pour n'importe quel demandeur.

Il doit ainsi faire une demande en qualité de candidat, attester de ne pas réutiliser les données à des fins commerciales, voir même prendre en charge le coût de la copie des données (si la commune fait payer la communication comme la règlementation le permet).

LA COMMUNICATION MUNICIPALE

Le Maire dispose de la possibilité d'utiliser les données issues de la liste électorale à des fins de communication municipale, sous réserve d'informer convenablement les personnes concernées dans les mentions d'information et/ou la politique de confidentialité générale de la commune.

Par ailleurs, si les usagers ne peuvent s'opposer à leur inscription sur la liste électorale (article L9 du code électoral), ils disposent de la possibilité de s'opposer à l'utilisation de leurs données dans un but de communication municipale et doivent en conséquence disposer de la possibilité de s'opposer à figurer dans le fichier de communication ainsi établi par la commune.

Il est possible, à cette fin, **d'opérer un tri des personnes** sur la liste électorale (en fonction de l'âge, du lieu de résidence, etc.). Cependant, les tris opérés sur la consonance des noms qui sont susceptibles de faire apparaître les origines raciales, ethniques ou les appartenances religieuses, réelles ou supposées, des personnes concernées sont en revanche interdits compte tenu des risques de discrimination qu'ils comportent (article 226-19 du code pénal).

LA RÉUTILISATION COMMERCIALE DES DONNÉES

Le code électoral permet à tout électeur, tout candidat et tout parti ou groupement politique de prendre communication et copie de la liste électorale**, à condition de s'engager à ne pas en faire un usage commercial** (utilisation par une agence de publicité, par une entreprise commerciale ou par un agent immobilier en vue de démarches de prospection, par exemple).

A ce titre, même lorsque l'électeur prend l'engagement de ne pas faire un tel usage de la liste, la commune peut demander des précisions sur l'usage que la personne entend faire de la liste électorale, s'il y a des raisons sérieuses de craindre un usage commercial.

Transmettre les données uniquement aux tiers et personnes autorisés

Les tiers à qui la transmission des données est <u>obligatoire</u>

Les données doivent être impérativement transmises :

- À **l'INSEE**, dès lors qu'une inscription ou une radiation du répertoire électoral unique intervient. En cas de modification, la Mairie doit en informer l'INSEE dans un délai de 7 jours.
- A la **commission de contrôle** chargée de s'assurer de la régularité de la liste électorale et de statuer sur les recours administratifs formés par les électeurs.

Les tiers à qui la transmission des données est <u>possible</u>

Les données peuvent être transmises :

- Aux **candidats aux élections** à des fins de communication politique et sous réserve de respect des modalités régissant la communication des documents administratifs
- Aux **services de la Mairie** en charge de la communication institutionnelle, notamment à des fins d'information des administrés (voir page précédente), reconnue comme intérêt légitime du responsable de traitement (le Maire).
- A **toute personne** qui en ferait la demande, à condition de s'engager à ne pas en faire un usage commercial.

*Notre service **<u>recommande</u>** par ailleurs d'inscrire toute demande dans un registre, afin d'assurer une traçabilité des demandes et de prévenir tout possible contentieux, y compris lorsqu'il n'a pas été donné de suite favorable à la demande !*

CONSERVER LES DONNÉES PENDANT UNE DURÉE CONFORME À LA RÉGLEMENTATION

Document	Durée de conservation	Sort final
• Liste électorale générale	3 ans	Conservation définitive
• Listes électorales par bureau de vote • Demandes d'inscription sur la liste • Dossiers de radiation		Destruction (après accord des archives départementales)

Source : Instruction DAF/DPACI/RES/2009/018 du 28 août 2009

Bon à savoir

Certains traitements de données nécessitent la réalisation d'une **analyse d'impact relative à la protection des données** (AIPD). Il s'agit d'un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, dès lors que le traitement est *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées*.

Cependant, dans le cas de la gestion de la liste électorale, et sous réserve que le traitement ait été mis en œuvre dans les conditions décrites dans cette fiche, alors l'AIPD **ne sera pas requise**.

Source : Délibération n°2019-118 du 12 septembre 2019 portant adoption de la liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

FRANCE RELANCE

Vous demanderiez à votre garagiste de vérifier votre dentition ?

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr

Face aux risques cyber, faites confiance à un véritable expert.

Pour votre sécurité numérique, faites-vous accompagner par des professionnels labellisés ExpertCyber.

Rendez-vous sur : securisation.cybermalveillance.gouv.fr

HOROSCOPE DE L'ANNÉE 2024

Découvrez ce que vous réservent les cieux pour cette nouvelle année 2024. Nuages, horizon bleu et ensoleillé, nuit étoilée ou coup de foudre… Votre signe vous dit tout !

BELIER

Ne soyez pas trop impulsif et réfléchissez avant de cliquer sur un lien ou d'ouvrir une pièce jointe. Vous pourriez être victime d'un phishing ou d'un rançongiciel !

TAUREAU

Ne soyez pas trop matérialiste, et ne vous laissez pas séduire par des offres trop belles pour être vraies. Vous pourriez être victime d'une arnaque ou d'un vol de données bancaires. Pensez à ne télécharger vos applications que sur les sites de prestataires reconnus et de confiance.

GEMEAUX

Vous pourriez avoir la tentation de vous disperser. Choisissez donc des mots de passe forts et uniques pour chaque site ou application, faute de quoi une usurpation d'identité ou un accès non autorisé à vos comptes n'est pas à exclure.

CANCER

L'émotivité vous gagne en cette année 2024, ce qui est normal pour un signe dominé par la Lune. Vous aurez tendance à vous confier, mais soyez méfiants envers les inconnus sur internet. Le chantage n'est, hélas, jamais bien loin.

LION

Tel le félin majestueux, vous pouvez vous montrer parfois trop orgueilleux et avoir tendance à vous exposer sur les réseaux sociaux. Prenez donc garde à l'image que vous souhaitez renvoyer et aux informations sur votre vie privée qui pourraient vous échapper…

VIERGE

L'année 2024 pourrait commencer sur les chapeaux de roues pour vous les Vierges, tandis que l'impact de Mercure se fait sentir. Le stress vous gagne, alors n'hésitez pas à faire des pauses régulières pour vous détendre. Pensez à vous renseigner sur le droit à la déconnexion.

BALANCE

L'indécision vous guette, vous les Balances. Choisissez des paramètres de confidentialité adaptés à vos besoins. N'hésitez pas à vous faire aider par un prestataire afin de vous éviter toute violation de données, mais gardez à l'esprit que votre prestataire devra également vous montrer patte blanche. Pensez donc à lui présenter une clause de confidentialité avant toute intervention.

SCORPION

Cette nouvelle année sera calme en apparence, mais le regard avisé de Pluton à l'arrivée de l'hiver pourrait vous jouer des tours. Attention aux connexions non sécurisées, tels que les réseaux Wi-Fi publics, car qui s'y frotte s'y pique !

SAGITTAIRE

Ne soyez pas trop imprudent, vous les Sagittaires, alors que cette année se place sous le signe des voyages et du télétravail. Utilisez un VPN et une connexion sécurisée lorsque vous voyagez ou travaillez à distance. Vous pourriez être victime d'un piratage ou d'une interception de vos communications.

CAPRICORNE

La rigidité est de mise en ce début d'année, tandis que votre attention se relâche suite à des fêtes animées. Restez à l'affut des nouvelles technologies et des nouvelles menaces. Ne laissez pas l'obsolescence s'installer et réalisez dès que possible toutes vos mises à jour.

VERSEAU

Attention aux mauvaises rencontres en ligne, pour vous les Verseaux. D'attitude rebelle, vous pourriez ne pas voir venir l'abus de confiance et vous faire détrousser vos données personnelles à votre insu. Restez donc sur vos gardes et demandez toutes les garanties nécessaires à vos interlocuteurs avant de leur confier vos secrets.

POISSONS

Gouvernés par Neptune, votre mémoire pourrait bien vous jouer des tours une fois le printemps venu. N'hésitez pas à multiplier les sauvegardes et à en contrôler la fiabilité régulièrement. Pour plus de sécurité, déportez-en une vers un lieu distinct. Ainsi, vous serez parés à toutes les éventualités.