CYBERACTU'

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

Octobre 2023

Attention, sanctions !

Dossier page 12

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

Clémente aux débuts du RGPD, la CNIL a entamé ces dernières années un virage dans sa politique démontrant sa volonté d'accélérer la mise en application du RGPD en sanctionnant d'avantage tous les organismes n'en respectant pas les prescriptions.

De par sa nouvelle procédure simplifiée, dont nous fêterons bientôt le premier anniversaire, la CNIL sanctionne désormais bien plus rapidement et cible maintenant de plus petits organismes, tels que des cabinets de médecins ou même… une commune !

Face à la multiplication des plaintes dont le nombre augmente année après année, il devient aujourd'hui nécessaire de prendre conscience que la mise en œuvre du RGPD est un enjeu devenu majeur pour nos collectivités et établissements publics.

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

LES TEXTES RÉGLEMENTAIRES

Loi n°2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense

Cette loi, essentielle car présentant les orientations stratégiques en matière de défense pour les six prochaines années, vient renforcer la protection de la Nation dans le domaine de la cyberdéfense. Elle renforce, entre autres, les pouvoirs de l'ANSSI, l'agence nationale de sécurité des systèmes d'information, qui se voit accorder la possibilité de prescrire des mesures de filtrage de noms de domaine pour neutraliser les attaques informatiques. Elle pourra également obtenir la communication de certaines données techniques de cache de serveurs de systèmes de noms de domaines.

L'ANSSI doit désormais être impérativement informée en cas d'incident chez un éditeur de logiciel ou la découverte d'une vulnérabilité critique dans l'un de ses produits. Une alerte pourra ainsi être envoyée à tous les clients de l'éditeur de logiciel, dont les collectivités territoriales utilisatrices.

Décret n°2023-767 du 11 août 2023 relatif à la mise à disposition par les communes des données relatives à la dénomination des voies et à la numérotation des maisons et autres constructions

Ce décret, dont l'entrée en vigueur est fixée au 1er janvier 2024 (1er juin 2024 pour les communes de moins de 2 000 habitants), fixe les modalités de mise à disposition par les communes des données d'adressage sur leur territoire et devant alimenter la « base adresse nationale », elle-même définie par l'article R.321-5 du code des relations entre le public et l'administration et produite par l'Institut national de l'information géographique et forestière (IGN).

Il instaure des règles de publication par l'ensemble des communes de leurs données d'adressage, en prévoyant la fin de l'obligation de transmission de ces mêmes données aux services fiscaux. Les communes devront ainsi avoir réalisé la première mise à disposition de leurs données d'adressage à compter de la date d'entrée en vigueur du décret sur le site internet suivant :

www.adresse.data.gouv.fr

Les communes devront donc mettre à disposition :

- La dénomination de l'ensemble des voies, publiques et privées, lorsque ces dernières sont ouvertes à la circulation, ainsi que des lieux-dits
- La numérotation des maisons et autres constructions

Toute modification apportée à ces données doit être renseignée par la commune dans le délai d'un mois suivant la date de la décision de modification.

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

Dans la continuité de ses actions à destination des collectivités, **Cybermalveillance.gouv.fr** réalise une **enquête sur la maturité des collectivités** en termes de cybersécurité et a pour objectif d'améliorer la sécurisation numérique des collectivités locales.

Cette enquête est destinée aux collectivités de moins de 25 000 habitants et s'adresse prioritairement aux élus, aux agents des communes en charge de l'informatique, de la sécurité ainsi qu'aux DGS et secrétaire de mairie, ou tout agent ayant une visibilité sur ces sujets.

La **date limite** pour répondre à l'enquête est fixée au **15 octobre 2023** !

EN BREF

Conscient des enjeux essentiels liés à la cybersécurité, le CNFPT propose désormais une **formation à distance** sur la cybermalveillance et la cybersécurité.

Destinée à **l'ensemble des agents des collectivités territoriales**, et ce quel que soit leur niveau de responsabilité, leurs fonctions ou leur cadre d'emplois, cette « e-sensibilisation » a pour objectif de faire connaître l'état actuel des menaces cyber, faire comprendre leur fonctionnement et leurs conséquences.

Elle permet également de s'approprier les bonnes pratiques élémentaires pour se prémunir, tant pour la collectivité que pour l'agent lui-même dans un cadre privé, de tous les risques cyber. Elle vise également à favoriser la transmission et la sensibilisation sur ces thématiques dans la sphère personnelle et professionnelle de l'agent (famille, amis, collègues, relations hiérarchiques, administrés, etc.).

Étant dispensée par le CNFPT, cette formation **entre en compte** dans le décompte des jours au titre de la **formation de professionnalisation** tout au long de la carrière.

Pour vous inscrire, rendez-vous sur :

cnfpt.fr

E-sensibilisation à la cybermalveillance et à la cybersécurité

code du stage : SX0SC

ZOOM sur une décision essentielle

Au mois de septembre 2023, le « Garant de la protection des données personnelles » (GPDP), l'équivalent italien de la CNIL, a rendu publique une sanction sur le sujet de la vidéoprotection sur la voie publique.

Les communes françaises, de plus en plus équipées de tels dispositifs, sont tenues de respecter les obligations légales et règlementaires en la matière. Nous vous proposons une étude de cas qui vous permettra d'identifier l'ensemble des mesures à prendre en compte pour la mise en place d'un système de Vidéo protection en France.

Un administré de la commune de Modica (Sicile) a déposé plainte contre la commune pour une utilisation abusive des caméras sur des zones destinées au dépôt des déchets. La collectivité avait pourtant confié à un prestataire privé l'installation de caméras, ainsi que la collecte et l'analyse des vidéos enregistrées.

De plus, la commune, et en accord avec la Police municipale, qui ne disposait pas en interne des moyens pour traiter les données collectées, avait accepté de nommer la société en tant qu'auxiliaire de la police judiciaire.

Par la suite d'un contrôle réalisé par l'autorité de contrôle, celle-ci a constaté les points suivants :

- Les clauses contractuelles encadrant la protection des données n'avaient pas été correctement déterminées
- La société n'avait pas été correctement désignée en tant que sous-traitant
- La société ne disposait pas du droit de mettre en place un tel traitement
- La société avait mis en œuvre un traitement de données personnelles qui ne respectait pas les principes de licéité, d'exactitude et de transparence

L'autorité de contrôle a conclu que le traitement des données en question, effectué par l'entreprise pour le compte de la mairie, a été effectué sans un encadrement clair du rôle de la société en qualité de sous-traitant, conformément à l'article 28 du RGPD. En effet, l'acte de nomination de la société comme « auxiliaire de police judiciaire » ne satisfait pas aux caractéristiques d'un acte juridique visant à encadrer la relation avec le responsable de traitement. La CNIL italienne a ainsi prononcé une sanction administrative de 5 000 €, assortie de sanctions complémentaires, vis-à-vis de la société.

Cependant, si un tel cas s'était présenté en France, c'est la collectivité qui aurait été sanctionnée. Mais alors, pourquoi ?

Il est ainsi essentiel de noter qu'en France, au regard des règles posées par le code de la sécurité intérieure (loi française), seules les collectivités peuvent filmer la voie publique*. Ni les entreprises, ni les établissements publics ne le peuvent. Ils peuvent néanmoins filmer les abords immédiats de leurs bâtiments et installations dans les lieux susceptibles d'être exposés à des actes de terrorisme.

Les particuliers, pour leur part, ne peuvent filmer que l'intérieur de leur propriété.

Ainsi, si un tel cas s'était présenté dans une des collectivités françaises, ce serait la commune, en tant que « Responsable de traitement » qui aurait subi la sanction, ainsi que la « mauvaise publicité » qui en aurait découlé.

De plus, la collectivité pourrait voir ses relations partenariales endommagées par un défaut de confiance, désormais amoindri du fait d'une image écornée.

**à ne pas confondre avec la notion de « lieu ouvert au public », qui peut être un lieu privé, tel qu'un commerce ou des parties communes d'un immeuble, et peut très bien disposer d'un tel système de vidéoprotection.*

La vidéoprotection en France

Il est essentiel de noter qu'en France la vidéoprotection, en plus d'être encadrée par la loi « Informatique et Libertés », loi française pour la protection des données personnelles modifiée afin d'être conforme avec les textes européens, le RGPD et la directive « Police-Justice », relève d'un statut particulier prévu par l'article L257-2, et le Titre V du Code de la Sécurité Intérieure (CSI). Pour pouvoir mettre en place ce dispositif il est nécessaire que le traitement remplisse des conditions cumulatives qui seront abordées par la suite.

Mais avant d'éclaircir ces conditions, il faudra définir ce qu'est un dispositif de vidéoprotection selon ledit code ainsi que vis-à-vis des autres dispositifs d'enregistrement d'images.

Tout d'abord, une différence est à faire entre la vidéoprotection et la vidéosurveillance. Le premier système se limite aux enregistrements vidéo portant sur les espaces de la voie publique (rue, route…) et aux lieux ouverts au public (gare, mairie, commerce…), tandis que le système de vidéosurveillance relève de l'enregistrement des espaces privés ou ne recevant pas de public (des dispositifs qui filment des lieux de travail non ouverts au public.).

Par ailleurs, il faut également différencier les systèmes dits « classiques », ne faisant qu'enregistrer des images, et les systèmes « augmentés », dont les fonctionnalités sont plus larges, tels qu'un décompte des personnes (sans reconnaissance de l'identité de la personne).

Enfin, il existe des systèmes dits « biométriques », répondant à deux critères. Premièrement, la finalité du dispositif doit être l'identification d'une personne. Ensuite, la catégorie des données traitées correspond à des données dites biométriques dont une caractéristique physique, physiologique ou comportementale. Il peut s'agir, par exemple, des caméras individuelles des services de police municipale. En outre, une caméra « augmentée » ne remplira aucun de ces deux critères ou remplira seulement un des deux.

Prenons le dispositif LAPI (lecture automatisée de plaques d'immatriculation) adopté davantage par les mairies françaises en tant que mesure de sécurité face aux infractions à la réglementation du stationnement. Une analyse de l'outil permet de déterminer qu'il s'agit d'une caméra « augmentée ». En effet, ce dispositif n'a pas comme objectif d'identifier ou d'authentifier de manière unique une personne. De plus, il ne traite pas des données qui correspondent à une caractéristique physique, physiologique ou comportementale.

Face à une réglementation complexe, notre service vous propose de retrouver nos fiches Pratiques RGPD sur notre site internet qui vous permettront de tout savoir sur la mise en conformité de votre collectivité :

Pour retrouver nos fiches, cliquez ici !

Les décisions des autorités chargées de la protection des données

31 janvier 2019 : Injonction

Pour la première fois depuis l'entrée en vigueur du RGPD, la CNIL s'est attaquée au domaine des administrations publiques en sanctionnant un établissement public national à caractère administratif pour « **défaut de sécurité des données personnelles** ».

Ayant, en 2019, une volonté d'accompagner les administrations vers la mise en conformité, cet établissement public n'avait alors pas fait l'objet de sanction financière, mais avait simplement été sanctionné d'une **injonction sous astreinte**.

03 septembre 2020 : Rappel à l'ordre

Toujours dans une volonté d'accompagner la mise en conformité des administrations, la CNIL a simplement **rappelé à l'ordre** le Rectorat de l'Académie de Normandie, ainsi que la Députée de la 4ème circonscription de la Manche, pour avoir utilisé le fichier national des lycéens « OCEAN » dédié à la gestion des examens et concours scolaires dans le but d'adresser des courriers de félicitations aux lauréats du baccalauréat de l'année 2019. La CNIL a ainsi estimé qu'il s'agissait là d'un **traitement de données illicite**, faute de base légale.

12 janvier 2021 : Rappel à l'ordre

Premier Ministère à faire l'objet de l'attention de la CNIL depuis l'entrée en vigueur du RGPD, le Ministère de l'Intérieur a fait l'objet d'un **rappel à l'ordre** du fait de l'usage par les forces de Police et de Gendarmerie de drones dans le but de vérifier le respect des mesures de confinement, mais aussi dans le cadre de leurs missions de police judiciaire (reconnaissance avant interpellation, surveillance de trafic de stupéfiant, etc.) ou de maintien de l'ordre (surveillance des manifestations, gestion des contrôles routiers, etc.).

La CNIL a ainsi estimé que le traitement mis en œuvre était **illicite faute de base légale**, et qu'il souffrait également d'un **défaut d'information des personnes concernées** par le traitement de leurs images. La CNIL a également mis en avant l'absence de réalisation par le Ministère d'une étude d'impact, préalable à la mise en œuvre des traitements de données sensibles.

24 septembre 2021 : Rappel à l'ordre

Peu de temps après un premier rappel à l'ordre, le Ministère de l'Intérieur a fait l'objet d'un second **rappel à l'ordre assorti d'une injonction de se mettre en conformité** pour sa mauvaise gestion du fichier automatisé des empreintes digitales.

La CNIL a en effet constaté cinq manquements, à savoir une **utilisation de données illicites car non prévues par les textes**, une **durée de conservation excessive**, la **conservation de données de personnes ne devant pas être concernées** par le traitement des données, une **sécurité insuffisante** et **l'absence d'information** des personnes concernées.

29 OCTOBRE 2021 : 400 000 €

Pour sa première (lourde) sanction pécuniaire à viser un établissement public, la CNIL a pris pour cible la RATP après avoir constaté que plusieurs centres d'autobus avaient décompté le nombre de jours de grève des agents dans un fichier utilisé pour préparer les choix de promotion.

La RATP a ainsi manqué à ses obligations de **minimisation des données** en ne traitant pas que les données strictement nécessaires à l'évaluation de ses agents. La CNIL a, en outre, relevé un défaut de **sécurité des données** traitées ainsi qu'un **défaut de durées de conservation**. Pour ces faits, la CNIL a sanctionné la RATP d'une amende administrative de **400 000 €**.

29 DÉCEMBRE 2022: 10 000 €

Première administration publique à faire les frais de la nouvelle procédure simplifiée* de sanction de la CNIL, une université, dont le nom n'a pas été communiqué (conformément aux règles de cette procédure), s'est vue infliger une **amende de 10 000 €** pour ne pas avoir respecté le principe de limitation des finalités de traitements en utilisant des données à des fins non prévues par la réglementation.

** voir dossier en page 12*

08 FÉVRIER 2023 : 5 000 €

Pour la première fois depuis la mise en application du RGPD, la CNIL a décidé d'infliger une sanction envers une collectivité territoriale ! De par sa procédure simplifiée, l'autorité de contrôle a ainsi infligé une **amende de 5 000 € assortie d'une injonction** envers une commune, dont le nom n'a pas été communiqué, pour ne pas… **avoir simplement désigné de délégué à la protection des données**.

La CNIL a relevé en ouvre un défaut de coopération de la commune pendant toute la procédure de contrôle, ce qui a permis d'accélérer sa décision.

NÉCROLOGIE

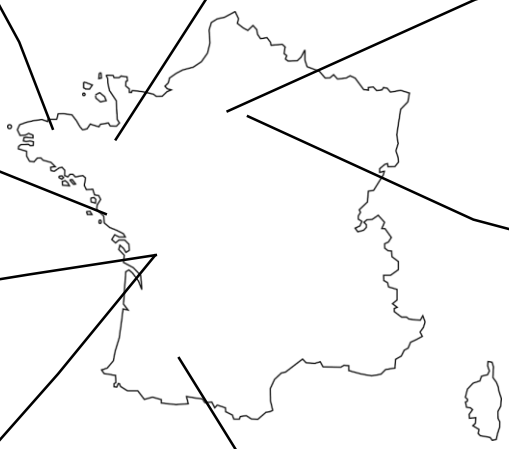
LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Mairie de Betton
1er septembre 2023

Mairie de Sartrouville
17 août 2023

Mairie de Morlaix
21 septembre 2023

Mairie de Remouillé
19 juillet 2023



Mairie de Chevilly Larue
27 juillet 2023

CA du Grand Angoulême
24 juillet 2023

Mairie de Angoulême
24 juillet 2023

Mairie de Agen
05 juillet 2023

** Sur les trois derniers mois*

ATTENTION, SANCTIONS !

« *Ce n'est point par la rigueur des supplices que l'on prévient le plus sûrement les crimes, c'est par la certitude de la punition* » disait en son temps Cesare Beccaria, principal théoricien de la notion moderne de droit pénal. Cette philosophie pourrait aujourd'hui être prêtée à la CNIL, autorité française en charge de veiller au respect des règles relatives à la protection des données, tant sa nouvelle procédure de sanction simplifiée vient apporter une nouvelle dimension à son action répressive.

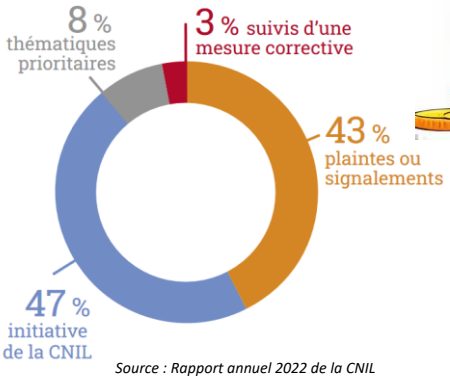
Il n'est pas de réglementation sans sanction pour celui qui l'outrepasse. Cela semble aller de soi. C'est pourquoi le RGPD prévoit, par son article 83, des sanctions devant être « effectives, proportionnées et dissuasives », et pouvant aller du simple rappel à l'ordre jusqu'à la très lourde sanction financière pour un montant maximal de 20 million d'euros ! Pour les entreprises privées, ce montant maximal peut même être alourdi jusqu'à 4% du chiffre d'affaire mondial.

Au niveau européen, depuis l'entrée en application du RGPD, les amendes prononcées par les autorités de protection des données sur la base de ce texte dépassent le montant total de 2,5 milliards d'euros. En France, sur la seule année 2022, ce ne sont pas moins de 101 millions d'euros répartis en seulement 21 sanctions qui ont été infligées.

A ce jour, pour l'année 2023, ce ne sont pas moins de 45 927 500 euros qui ont été totalisés pour seulement 14 sanctions.

Et parmi elles, et ce pour la première fois en France depuis l'entrée en vigueur du RGPD, **une commune**…

L'origine des contrôles



Source : Rapport annuel 2022 de la CNIL

LES PLAINTES SONT LES ARMES DES VICTIMES

Proverbe oriental

Mais comment en arrive-t-on à une sanction pour non-respect du RGPD ? Car si la logique de sanction en cas d'infraction est simple à comprendre, la chaîne répressive de la CNIL l'est un peu moins, celle-ci étant dérogatoire vis-à-vis de la procédure pénale. Il est par ailleurs à noter que des sanctions pénales sont également prévues par la loi Informatique et Libertés du 06 janvier 1978. Mais nous y reviendrons…

Tout part en premier lieu d'un signalement vis-à-vis d'un manquement aux règles concernant la protection des données. Ce signalement peut avoir plusieurs origines. La principale : la plainte. Il s'agit du signalement par les usagers d'un manquement à la protection et/ou au bon traitement de leurs données effectué directement auprès de la CNIL via leur site internet. La facilité déconcertante de déposer une telle plainte dans une époque de plus en plus procédurière laisse à penser une explosion des contrôles dans les années à venir.

Mais il ne s'agit pas de la seule voie de signalement des manquements auprès de l'autorité de contrôle. Les enquêtes de la presse, de plus en plus attaché au domaine de l'utilisation des données personnelles, sont également l'un des outils utilisés par la CNIL qui va profiter de cette remontée de faits pour procéder à des contrôles. Et lorsqu'il ne s'agit pas de la presse, ce sont les autres autorités de contrôle des pays européens qui peuvent, dans le cadre de la coopération entre autorités européennes, dénoncer des faits illicites lorsqu'elles en ont connaissance.

Et enfin, la CNIL elle-même peut s'autosaisir. Chaque année, l'autorité de contrôle présente ses thématiques prioritaires, des sujets à fort enjeux pour le public, afin d'orienter sa politique de contrôle. La CNIL peut ainsi décider de contrôler tout organisme envers lequel elle exprime des doutes quant au bon traitement des données utilisées.

A titre d'information, les thématiques prioritaires pour l'année 2023 sont « *l'utilisation du fichier des incidents de remboursement de crédit aux particuliers* », « *l'accès au dossier patient informatisé au sein des établissements de santé* », mais surtout « *l'utilisation de caméras augmentées*[1] *par les acteurs publics* ».

345
CONTRÔLES DONT :

143
sur place

128
en ligne

43
sur pièces

31
sur audition

Auxquels s'ajoutent l'analyse de
45 signalements
relatifs à des violations de données

TOUTE RÉGLEMENTATION EXIGE CONTRÔLE

Dès lors qu'un manquement est signalé à la CNIL, celle-ci va pouvoir engager une procédure de contrôle. Ce contrôle n'est pas forcément réalisé sur place. En fonction

Source : Rapport annuel 2022 de la CNIL

1 – Attention, une caméra dite « augmentée » n'est pas une caméra utilisant la reconnaissance faciale ! Une simple caméra comptant le nombre de passants ou une caméra permettant la lecture automatisée des plaques d'immatriculation, de plus en plus fréquentes dans nos collectivités, sont considérées comme des caméras augmentées !

des besoins, la CNIL va ainsi pouvoir demander des documents ou poser des questions écrites au responsable de traitements lors de ce que l'on va appeler un « contrôle sur pièces ». Elle peut enfin convoquer les acteurs concernés dans les traitements de données ou procéder à un contrôle en ligne dès lors que les manquements sont visibles à distance.

La CNIL va ainsi pouvoir demander des documents ou poser des questions écrites au responsable de traitements lors de ce que l'on va appeler un « contrôle sur pièces ». Elle peut également convoquer les acteurs concernés dans les traitements de données ou procéder à un contrôle en ligne dès lors que les manquements sont visibles à distance.

Mais le contrôle le plus complet, et aussi le plus redouté, est le contrôle dit « sur place ». Très souvent organisé de manière surprise, et ce afin d'éviter toute dissimulation de faits répréhensibles, ces contrôles permettent aux auditeurs de la CNIL un accès aux traitements de données, et notamment aux moyens utilisés et aux mesures de sécurité mises en place.

Les agents de la CNIL peuvent ainsi contrôler TOUS les traitements de données et avoir accès à TOUTES les données traitées. Ils peuvent accéder à tous les locaux et demander à accéder à tous les outils de traitements de données pour en contrôler la conformité. Oui, le contrôle peut aller très loin.

La suite de la procédure va cependant dépendre de ce que les agents de l'autorité de contrôle française vont constater lors du contrôle, qui ne signifie pas forcément une sanction. En effet, si la CNIL constate que tout va bien, ou que seuls quelques manquements mineurs sont présents, elle peut décider de clôturer la procédure et adresser un courrier au responsable de traitements assorti d'une ou plusieurs recommandations.

Si, en revanche, des irrégularités d'importance sont constatées, la CNIL va pouvoir enclencher sa procédure répressive. Une fois encore, l'on fait face à plusieurs possibilités…

« Comment se passe un contrôle de la CNIL ? »

publié sur cnil.fr

Vite fait, bien fait !

Si la CNIL dispose bien du pouvoir de sanction, elle est néanmoins responsable de l'accompagnement et de la sensibilisation des acteurs de la protection des données. Elle ne va pas avoir pour objectif de simplement réprimer les différents manquements. L'objectif reste de s'assurer que les données des citoyens restent bien protégées et soient traitées dans les règles de l'art.

C'est pourquoi elle va, sauf irrégularité très importante, procéder tout d'abord à une mise en demeure, en adressant au responsable de traitements une liste de points très précis à respecter pour pouvoir échapper à une sanction. Cette mise en demeure a ainsi pour principal objectif d'imposer rapidement au responsable de traitements récalcitrant ou négligeant l'application du RGPD.

Cette mise en demeure n'est hélas pas toujours suivie d'effets. Certains restent sourds aux diverses injonctions de la CNIL qui va alors devoir sévir et sanctionner l'organisme.

C'est ce qui arrive encore aujourd'hui trop souvent, de nombreuses sanctions étant prises, entre autres, pour « défaut de coopération avec l'autorité de contrôle ».

C'est pourquoi la CNIL a décidé de passer à la vitesse supérieure en matière de sanctions. Dans son plan stratégique pour la période 2022-2024, l'autorité de contrôle française entend ainsi « *accroître l'efficacité de l'action répressive* » afin d'assurer « *l'effectivité des droits des personnes et la conformité des organismes au RGPD* ».

Ainsi, dès la fin de l'année 2022, la CNIL a mis en place une nouvelle procédure de sanction dite « simplifiée », réservée aux affaires « *ne présentant pas de difficulté particulière* ». Cela peut ainsi être le cas au regard d'une jurisprudence établie du fait d'une précédente décision de sanction « ordinaire », ou encore du fait de la simplicité de la ou des questions qu'elle présente à trancher.

Cette procédure, prévue par l'article 22-1 de la loi Informatique et Libertés, permet ainsi à la CNIL de sanctionner beaucoup plus rapidement un organisme, qui bénéficie néanmoins de la possibilité de formuler des observations écrites. Si cette procédure ne permet pas à la CNIL de communiquer l'identité de l'organisme mis en cause, trois mesures dissuasives sont prévues :

- Un rappel à l'ordre
- Une injonction de se mettre en conformité, y compris sous astreinte d'un montant maximal de 100 euros par jour de retard
- Une amende d'un montant maximal de **20 000 euros**

C'est ainsi que, outre les grosses prises de la CNIL via les sanctions ordinaires, de nouveaux organismes, de moindre importance et pensant sans doute échapper aux sanctions, se sont retrouvés pris dans les filets de l'autorité de contrôle qui en a sérieusement resserré les mailles. C'est ainsi un médecin qui a ouvert le bal en étant sanctionné pour non respect du droit d'accès et un défaut de coopération avec la CNIL par une amende de 5 000 euros et une injonction sous astreinte.

Depuis, plusieurs médecins, de petites sociétés, voire même des universités ont été sanctionnées au titre de cette procédure simplifiée destinée à faire prendre conscience aux responsables de traitements de toutes tailles qu'ils sont tous soumis aux mêmes règles.

Et parmi eux, une commune. Toute première collectivité territoriale française à être sanctionnée sur la base du

« Les procédures de sanction »
Publié sur cnil.fr

RGPD, cette commune, dont le nom n'a pas été dévoilé du fait de l'engagement d'une procédure simplifiée à son encontre, s'est ainsi vue écoper d'une amende de **5 000 euros** assortie d'une injonction **pour ne pas… avoir simplement désigné de délégué à la protection des données** (ainsi que pour défaut de coopération avec la CNIL) !

Les collectivités territoriales ne sont donc pas hors de danger, surtout avec l'introduction de cette procédure simplifiée qui entend imposer la mise en conformité. La diversification des usages des données personnelles rend en effet nécessaire aujourd'hui l'application la plus stricte des principes édictés par le RGPD, et il y a fort à parier que de nouvelles collectivités feront également les frais de leur méconnaissance ou de leur négligence de la thématique de la protection des données. A titre d'illustration, sur la seule année 2022, 16 contrôles de la CNIL ont concernés des collectivités territoriales ou des établissements publics[2].

Mais il n'est pas non plus à oublier que, outre ces sanctions administratives et financières, est prévue par la loi Informatique et Libertés un régime de sanctions pénales pour le responsable de traitements qui, pour une collectivité ou un établissement public, est toujours et par principe… l'autorité territoriale ! Et oui, ce n'est plus seulement l'organisme qui est ici sanctionné, mais bien la personne physique qui en est responsable ! Si la procédure répressive de la CNIL est indépendante de la justice pénale, cela signifie en effet que le juge pénal pourra prononcer une sanction en parallèle de celle de la CNIL pouvant aller jusqu'à cinq ans d'emprisonnement et une amende de 300 000 euros. Il est donc essentiel aujourd'hui pour les élus de prendre conscience que les sanctions pour le non respect du RGPD vont s'accélérer, tant les besoins de se mettre en conformité s'accroissent de jour en jour du fait de l'évolution toujours plus rapide des technologies de traitement de l'information.

Car face aux erreurs, si les torts sont parfois partagés, les sanctions ne le sont jamais ■

2 – Source : data.gouv.fr

CYBER MOIS

BIENVENUE AU **CYBER QUIZ FAMILLE !**

du **2 octobre** au **31 octobre** 2023

VENEZ TESTER VOS CONNAISSANCES ET PARTICIPER AU JEU-CONCOURS !

organisé par Cybermalveillance.gouv.fr et ses membres pour muscler vos réflexes en cybersécurité

DE NOMBREUX LOTS* À GAGNER !

Alors, qu'attendez-vous pour tenter votre chance ?
Pour participer, rien de plus simple,
répondez aux questions du Cyber Quiz Famille :

À VOUS DE JOUER !

* billets pour parcs d'attraction, spectacles et cinéma...

cybermois.cybermalveillance.gouv.fr

POUR RÉVISER

Les obligations des collectivités en matière de conservation des archives

Les archives publiques étant imprescriptibles et inaliénables, leur gestion et leur conservation sont soumises à plusieurs obligations légales.

En cas de non-respect de celles-ci, **les sanctions peuvent être sévères**.

Les obligations :

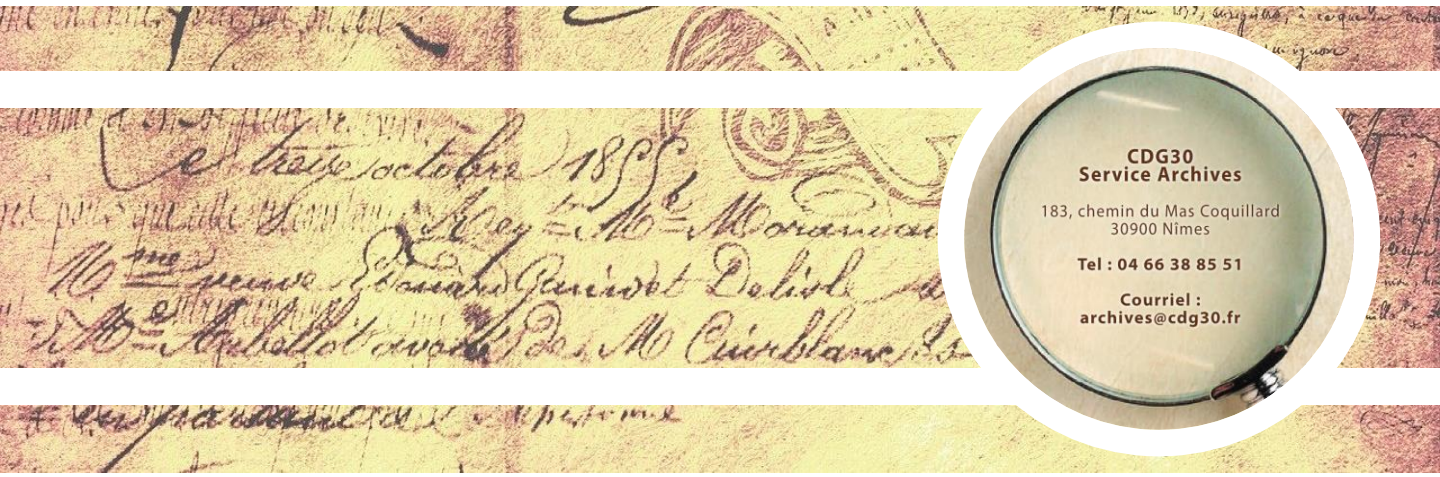
- Propriétaires de leurs archives, les collectivités sont tenues de les conserver et de les mettre en valeur (Code du Patrimoine, article L.212-1).
- Les frais de conservation des archives sont une dépense obligatoire de la collectivité (Code Général des Collectivités Territoriales, article L.2321-2).
- Les archives doivent être conservées dans un bâtiment public (circulaire DGP/SIAF/2016/005). Le préfet doit être informé de tout projet de construction, d'extension ou d'aménagement de bâtiments à usage d'archives ainsi que des projets de travaux dans ces bâtiments. (Code du Patrimoine, article R.212-54).
- L'élimination réglementaire d'archives ne peut se faire sans l'autorisation de la Direction des Archives Départementales qui assure le contrôle scientifique et technique de l'Etat sur les archives publiques (Code du Patrimoine L.212-3).
- Tout sinistre ou détournement doit être signalé au préfet. À savoir : celui-ci peut prescrire un dépôt au service départemental d'archives après une mise en demeure restée sans effet, lorsqu'il est établi que la conservation des archives du groupement n'est pas convenablement assurée. (Code du Patrimoine, article L.212-6-1).
- Le Maire est responsable au civil et au pénal du maintien de l'intégrité des archives de la commune (Code du Patrimoine, article L.214-3 et L.214-4). À savoir : un procès-verbal de décharge et de prise en charge des archives, appuyé sur un récolement, doit être établi à chaque élection municipale (article 4 de l'arrêté interministériel du 31 décembre 1926.)[1].
- Et enfin, « *Tout fonctionnaire ou agent chargé de la collecte ou de la conservation d'archives* […] *est tenu au secret professionnel en ce qui concerne tout document qui ne peut être légalement mis à la disposition du public* » (Code du Patrimoine, article L.211-3).

---

1 – « Le procès-verbal et le récolement servent à formaliser la passation de responsabilité du maire sortant au nouveau maire. Ils permettent de certifier de façon contradictoire l'existence des archives à un moment donné, le maire étant responsable pénalement de toute destruction non réglementaire (art.432-15 à 432-17 du Code pénal) » (Source : Service Interministériel des Archives de France)

Extraits du tableau récapitulatif des infractions en matière archivistique, « La sûreté du patrimoine archivistique, seconde édition », Service interministériel des archives de France, 2018

Infractions	Cordes concernés	Peines encourues
Atteinte au secret professionnel	• Code pénal – article 226-13 et 226-31	• 1 an d'emprisonnement • 15 000 € d'amende • Interdiction d'exercer une activité archivistique • Interdiction de certains droits
Vol de documents d'archives	• Code pénal – articles 311-4-2 et 311-13	• 7 ans d'emprisonnement et 100 000 € d'amende à la moitié de la valeur • 10 ans d'emprisonnement et 150 000 € d'amende (circonstances aggravantes)
Destruction, dégradation, détérioration de documents d'archives	• Code du patrimoine – article L.214-6 • Code pénal – articles 322-2, 322-3-1 et 322-4	• 3 ans d'emprisonnement et 45 000 € d'amende • 7 ans d'emprisonnement et 100 000 € d'amende
Abus de confiance : détournement de fonds, de valeurs ou d'un bien quelconque	• Code pénal – article 314-1	• 3 ans d'emprisonnement et 375 000 € d'amende
Soustraction, destruction et détournement de biens contenus dans un dépôt public (ou tentative)	• Code du patrimoine – articles L.214-3, L.214-4 et L.214-10 • Code pénal – articles 433-4 et 432-15	• 3 ans d'emprisonnement, 45 000 € d'amende et interdiction de certains droits • 7 ans d'emprisonnement et 100 000 € d'amende • 10 ans d'emprisonnement et 150 000 € d'amende • 5 ans d'interdiction d'accès aux archives
Négligence d'une personne dépositaire de l'autorité publique	• Code pénal – article 432-16 • Code du patrimoine – articles L.214-3 et L.214-2	• 1 an d'emprisonnement et 15 000 € d'amende



LE BON GESTE

RÉAGIR EN CAS DE FRAUDE AU VIREMENT

La fraude au virement, également appelée « arnaque au faux RIB » consiste à tromper une victime en usurpant l'identité d'un créancier avec lequel elle est en relation afin de lui faire réaliser un virement vers un compte bancaire détenu par l'escroc.

De plus en plus fréquente dans les collectivités, cette fraude fait régulièrement l'objet d'alertes de la part des services des finances publiques.

LA RECOMMANDATION DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Contactez directement votre créancier pour confirmation en cas de demande de changement de RIB

Utilisez des mots de passes complexes et différents pour chaque site et application que vous utilisez

(*voir Cyberactu' du mois de juillet 2023*)

Installez un anti-virus afin de protéger votre outil de travail

Méfiez-vous des messages piégés qui vous incitent à communiquer votre identifiant et/ou votre mot de passe, et n'y **répondez jamais** !

N'installez pas d'application inconnue ou provenant d'un site inconnu, au risque de télécharger une version infectée par un virus, et **privilégiez les sites officiels** des éditeurs.

Faire les mises à jour régulièrement qu'il s'agisse des applications, du système d'exploitation ou des logiciels.

QUE FAIRE SI VOUS ÊTES VICTIME D'UNE FRAUDE AU VIREMENT ?

1

Alertez immédiatement la DGFIP !
pour tenter de suspendre le virement ou à défaut demander le retour des fonds

2

Alertez au plus vite le créancier
pour l'alerter sur l'usurpation d'identité dont il a été victime afin qu'il prenne les mesures nécessaires

3

Conservez les preuves
afin de constituer un dossier en cas de procédures ultérieures

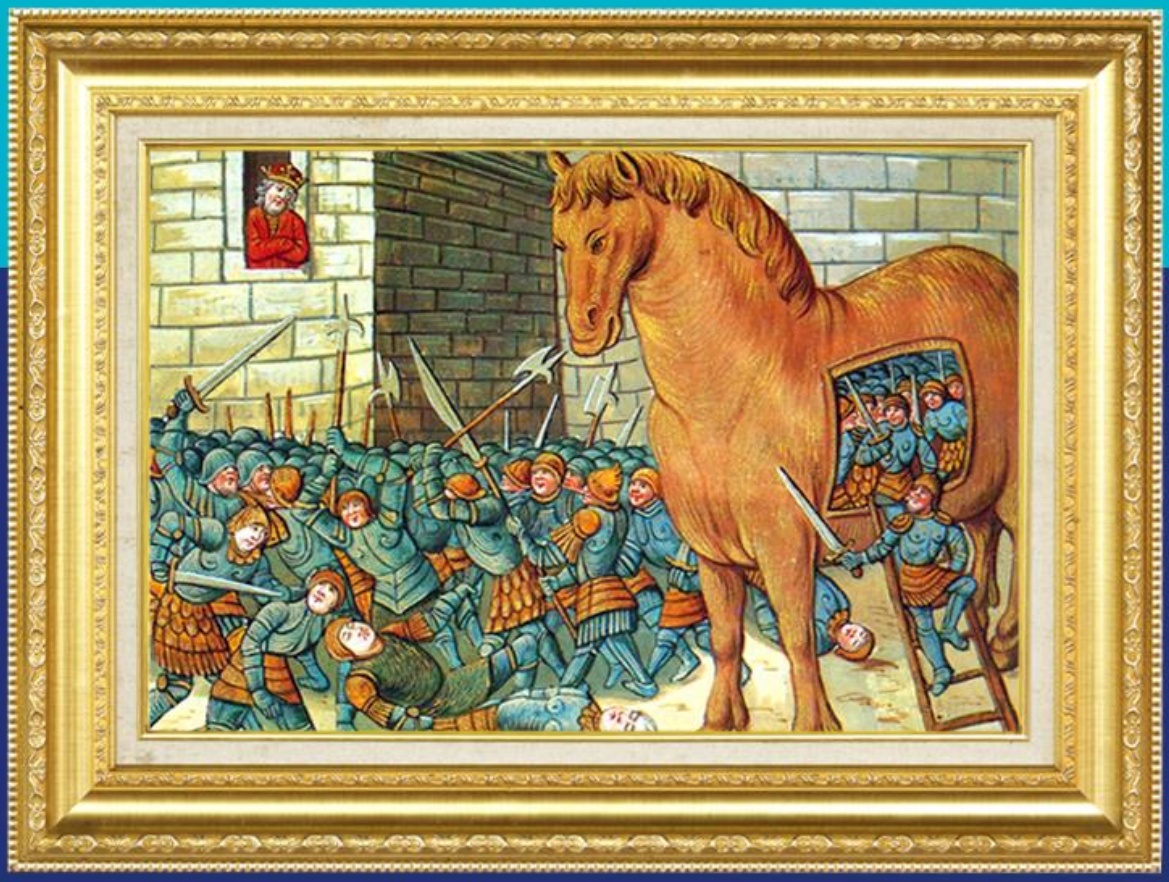
4

Vérifiez vos paramètres de messagerie
pour contrôler tout changement dans la redirection des mails ou les règles des filtrage, et **changez de mot de passe** !

5

Déposez plainte !
Le dépôt de plainte doit intervenir dans les plus brefs délais accompagné de toutes les preuves nécessaires

cybermois.cybermalveillance.gouv.fr



Histoire de la destruction de Troie
Artiste inconnu RHT-CNRS / Petit Palais

Méfiez-vous des messages suspects : ne cliquez pas sur les liens qui vous sont proposés

#CyberResponsable

CYBER MOIS