CYBERACTU'

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

Juillet 2024

Entretien exclusif :

Rencontre avec les gendarmes du Gard

Dossier page 18

Et aussi

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

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

Page 4

L'ACTUALITÉ DE LA PROTECTION DES DONNÉES

Page 14

LES DÉCISIONS DES AUTORITÉS CHARGÉES DE LA PROTECTION DES DONNÉES

Page 17

NÉCROLOGIE : LES DERNIÈRES VICTIMES DE CYBERATTAQUES

Page 18

LE DOSSIER

ENTRETIEN EXCLUSIF : RENCONTRE AVEC LES GENDARMES DU GARD

Page 24

LE POINT ARCHIVES

Page 26

LE BON GESTE

LA GÉOLOCALISATION DES VÉHICULES

ÉDITO

Ce trimestre a été riche en rencontres. En effet, dans cette édition de notre magazine nous avons voulu communiquer sur les autres acteurs qui accompagnent les structures publiques en matière de protection des données personnelles.

C'est ainsi que vous trouverez dans le dossier toutes les informations liées à l'action des Gendarmes du Gard qui font partie de la Section Opérationnelle de Lutte contre la Cybercriminalité dans les collectivités territoriales. Ils présentent leur prestation à zéro coût, accessible à l'ensemble des collectivités de notre département.

La rencontre des DPO des CDG d'Occitanie a été organisée au mois de juin au CDG 30. Ce groupe de travail nous permet d'échanger et d'enrichir notre manière de servir grâce au partage d'idées et la mise en réseau.

Pierre BONANNI – Ana VEGA

Sarah ROMAN

Contacts

Service « Protection des données »
☎ : 04 66 38 86 86
@ : dpd@cdg30.fr

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

L'ACTUALITÉ DE LA PROTECTION DES DONNÉES

Loi n°2024-449 du 21 mai 2024 visant à sécuriser et réguler l'espace numérique, dite « Loi SREN »

Cette loi, destinée à renforcer la protection des internautes, notamment les plus jeunes, vient confier à la CNIL de nouvelles missions.

Ses principales dispositions visent à protéger les enfants de la pornographie, à contrer les arnaques, la haine et la désinformation, mais également à transposer dans le droit français des dispositions venues de règlements européens, tel que le règlement sur les services numériques ou le règlement sur les marchés numériques.

Concernant la sécurité, la loi prévoit la mise en place d'un **filtre de cybersécurité anti-arnaque** à destination du grand public. Un message d'alerte avertira les personnes lorsqu'après avoir reçu un SMS ou un courriel frauduleux, elles s'apprêtent à se diriger vers un site malveillant. Ce message renverra vers un site officiel de l'État. Le dispositif, qui doit être précisé par décret, vise à protéger les citoyens contre les tentatives d'accès frauduleux à leurs coordonnées personnelles ou bancaires.

La publication en ligne d'hypertrucages ou "deepfake" (vidéos, images et autres contenus, notamment à caractère sexuel, visant à nuire générés par intelligence artificielle - IA) sera mieux réprimée. Une **réserve citoyenne du numérique**, comme réserve thématique de la réserve civique, est par ailleurs instaurée.

Enfin, **concernant la CNIL**, celle-ci sera désormais compétente pour vérifier le respect par les plateformes des limitations posées en matière de profilage publicitaire (interdiction pour les mineurs ou à partir de données sensibles). Elle travaillera également avec les autres autorités administratives, tel que l'ARCOM ou l'ARCEP, ainsi qu'avec les services de l'État au sein d'un réseau national de coordination de la régulation des services numériques.

JURISPRUDENCE

Cour de cassation, 30 avril 2024, n°23-80.962

Un enquêteur privé avait effectué des recherches dans le cadre d'une enquête sur des personnes, portant sur des données à caractère personnel, et avait été condamné à un an d'emprisonnement avec sursis et 20 000 euros d'amende. L'enquêteur avait cependant utilisé des données en libre accès, jetant un doute sur la déloyauté de leur collecte.

La cour de cassation a cependant estimé que le libre accès aux données ne retirait en rien le caractère déloyal de la collecte dès lorsqu'elle s'effectuait à l'insu des personnes concernées sans rapport avec l'objet de leur mise en ligne, privant ainsi les personnes concernées de leur droit d'opposition. La cour a ainsi confirmé le jugement condamnant l'enquêteur.

Attention donc à l'utilisation de données publiées en libre accès, notamment via les réseaux sociaux !

Conseil d'Etat, 30 avril 2024, n°468513

Un citoyen avait demandé au service des archives départementales de la Seine-Saint-Denis de lui communiquer l'intégralité des jugements rendus par le tribunal correctionnel de Bobigny entre 1971 et 1987, et s'était vu opposer un refus devant le caractère considéré par les archives comme abusif de sa demande.

Le Conseil d'État est ainsi venu trancher sur cette qualification et a tenu compte du fait que la demande portait sur un peu plus de 200 000 jugements contenus dans quelques 1 270 boîtes, et dont certains jugements ne pouvaient en outre être communiqués du fait de leur nature.

Le juge administratif a donc estimé que cette demande nécessitant une charge de travail excessive pour le service des archives départementales, tant du fait des moyens du service que du fait de la nécessité d'identifier, pour chaque jugement demandé, le régime de communicabilité dont il relève.

EN BREF

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

MonAideCyber
INNOVATION ANSSI

Service **gratuit** de diagnostic cyber développé par l'ANSSI, Mon Aide Cyber est une plateforme permettant aux organismes, dont les collectivités territoriales, d'améliorer leur niveau de cybersécurité. Ce service repose sur un réseau d'aidants qui réalise un diagnostic cyber qui sera ensuite accompagné par un plan d'actions composé de 6 mesures de sécurité prioritaires à mettre en œuvre sur les 6 prochains mois. Par cet outil, un suivi et des conseils sont prodigués par les aidants.

Plus d'informations sur le site monaidecyber.ssi.gouv.fr

OPEN DATA : LA CNIL PUBLIE SES RECOMMANDATIONS

Obligation pour toutes les communes de plus de 3 500 habitants, l'ouverture des données publiques est parfois difficile à accorder avec la réglementation sur la protection des données.

Pour aider les diffuseurs de données, telles que nos collectivités, la CNIL a ainsi publié plusieurs fiches pratiques destinées à concilier l'ouverture et la réutilisation des données publiées sur internet avec les enjeux de la protection de la vie privée.

Pour retrouver ces fiches, rendez-vous sur le site cnil.fr

CNIL.

La CNIL et Départements de France renouvellent leur partenariat

Partenaires de longue date, la CNIL et Départements de France, association réunissant les présidents de plus d'une centaine de collectivités territoriales, dont 95 conseils départementaux, s'assurent ensemble de la bonne application du RGPD au sein des départements et de la sécurisation de leurs fichiers et systèmes d'information dans un contexte où de plus en plus de départements sont ciblés par des attaques.

Par ce renouvellement, les deux partenaires entendent poursuivre leurs travaux communs, notamment dans le domaine de l'intelligence artificielle permettant l'amélioration de la qualité et de l'efficacité du service public.

Ont ainsi été retenus, pour la période 2024 – 2027, deux priorités : **le développement du partage de données** entre les différents acteurs institutionnels, ainsi que **le recours à l'IA pour améliorer la qualité des services publics et l'efficacité de l'administration** tout en protégeant la vie privée des administrés.

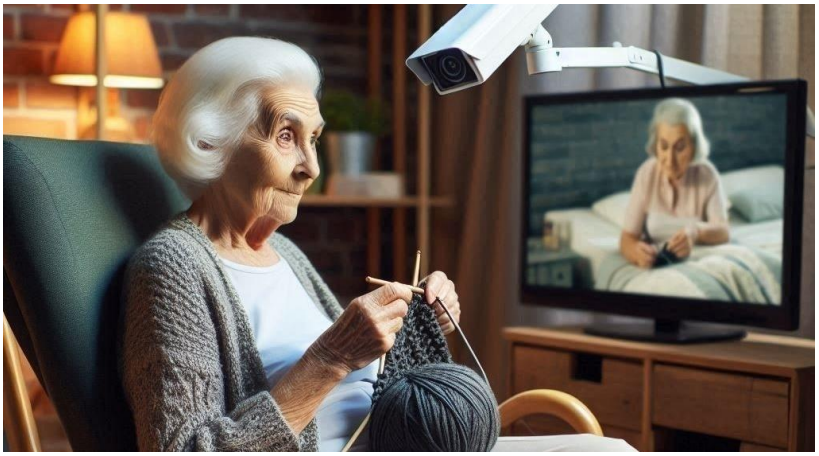
Vidéosurveillance des chambres des EHPAD : La CNIL appelle à la vigilance

Dans le contexte actuel où la sécurité des personnes âgées hébergées en EHPAD est devenue une préoccupation majeure, la vidéosurveillance est souvent évoquée comme une solution potentielle. Cependant, cette mesure soulève d'importantes questions relatives à la protection de la vie privée et des données personnelles.

La CNIL a ainsi récemment publié une recommandation qui clarifie les conditions d'utilisation de caméras dans les chambres des EHPAD. L'autorité a adopté une position prudente et mesurée concernant l'installation de dispositifs de vidéosurveillance dans les chambres des résidents. Selon la recommandation publiée le 2 mai 2024, ces dispositifs ne sont pas censés être installés, sauf dans des circonstances très exceptionnelles. Ces exceptions sont strictement encadrées et ne peuvent être envisagées que pour assurer la sécurité des personnes hébergées, notamment dans le cadre d'une enquête pour maltraitance.

Aussi, avant d'envisager la mise en place d'un tel dispositif dans les chambres d'un EHPAD, plusieurs conditions cumulatives doivent être remplies : Une suspicion étayée de mauvais traitements doit exister, malgré les dispositifs alternatifs mis en place pour assurer la sécurité des personnes hébergées. De plus, les procédures d'enquêtes préalables ne doivent pas avoir permis de détecter une situation de maltraitance, et un doute doit donc subsister.

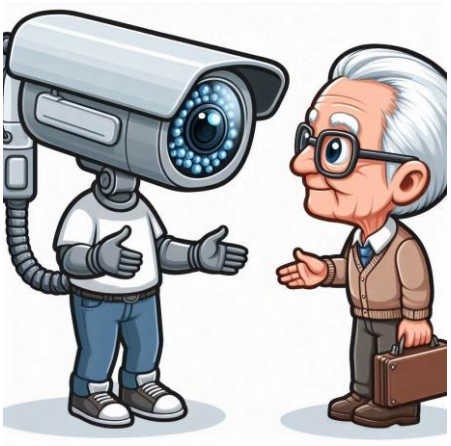
En outre, l'établissement doit respecter des garanties telles que la limitation de l'activation dans le temps, la désactivation du dispositif lors des visites des proches, et l'établissement d'un cadre interne strict quant aux conditions justifiant l'installation. Il est également impératif d'informer les agents et de



recueillir le consentement des personnes hébergées ou de leurs représentants légaux.

La CNIL souligne l'importance de trouver un équilibre entre la sécurité des résidents et le respect de leur vie privée. La chambre d'un résident d'EHPAD représente son seul espace d'intimité et l'installation de caméras pourrait porter atteinte à cette intimité. Par conséquent, toute décision d'installer un dispositif de vidéosurveillance doit être prise avec la plus grande prudence et dans le respect des droits fondamentaux des individus.

La CNIL nous rappelle ainsi que la technologie doit être au service de l'humain et non l'inverse, et que la protection des données personnelles est indissociable du respect de la dignité des personnes âgées dépendantes ■

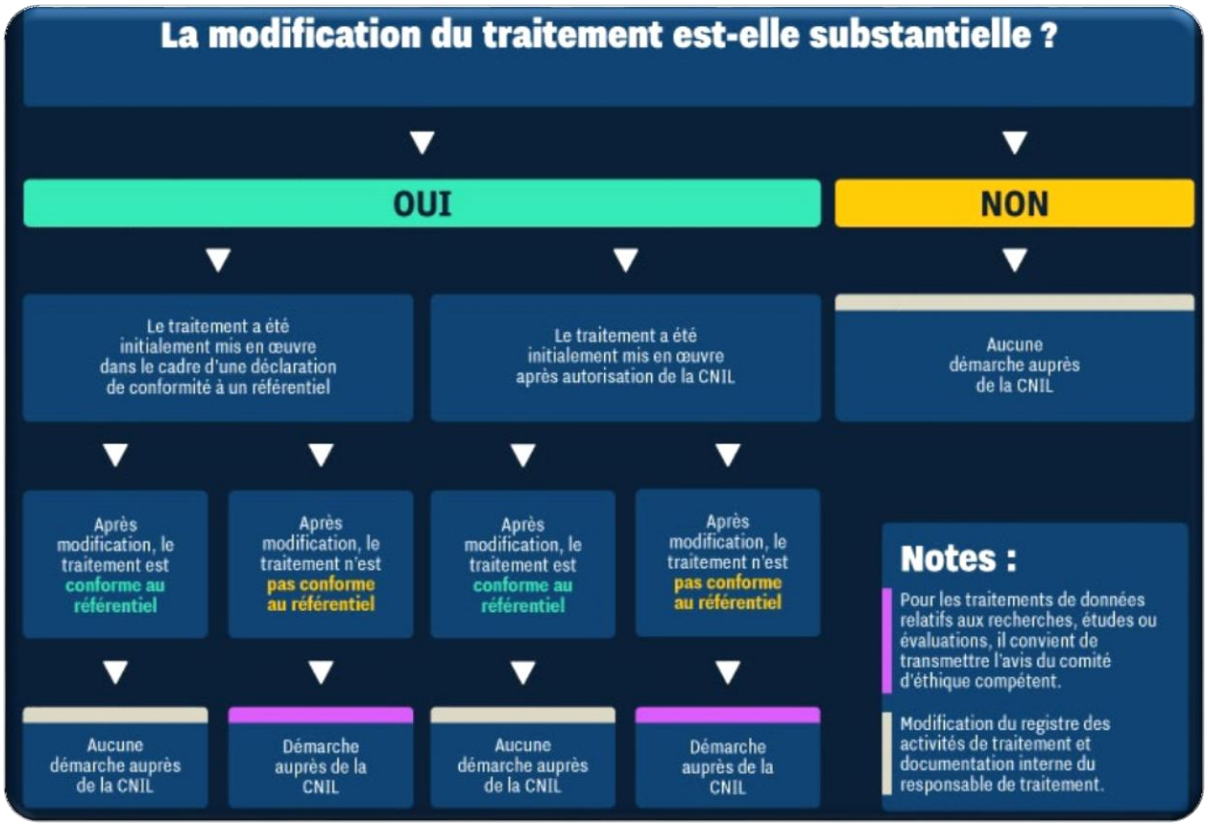


La CNIL précise les démarches à mener pour modifier un traitement de données soumis à formalités

La Commission est venue préciser par un article du 13 juin les démarches à accomplir pour modifier un traitement de données dont la nature impose des formalités préalables à sa mise en œuvre.

Pour rappel, la loi Informatique et Libertés prévoit un régime particulier pour certains traitements, notamment concernant les données de santé, dont des formalités préalables, telles qu'une déclaration ou une demande d'autorisation auprès de la CNIL, sont nécessaires pour pouvoir légalement mettre en œuvre le traitement. Si, dans les collectivités territoriales, de tels traitements sont rares, certains traitements peuvent venir nécessiter de telles démarches, telles que la mise en place de programmes de vaccination.

Cependant, au cours de sa mise en œuvre, le traitement est susceptible d'évoluer. La CNIL est donc venue préciser que désormais, seules les modifications substantielles du traitement devront faire l'objet de nouvelles démarches, les modifications mineures ne devant faire l'objet que d'une documentation interne, dont notamment la mise à jour du registre de traitements, ou encore l'information des personnes concernées par les données traitées. Afin d'y voir plus claire, une infographie a ainsi été publiée par la CNIL à ce sujet :



Source : CNIL, « Modification des traitements de données soumis à formalités : quelles démarches ? » - 13 juin 2024

LES PIRATES
C'EST COMME LES FANTÔMES

VOUS NE LES VOYEZ PAS MAIS ILS SONT LÀ !

04 66 38 86 86
dpd@cdg30.fr

SERVICE
PROTECTION DES DONNÉES
CENTRE DE GESTION DU GARD

LA TRIBUNE DU DPO

PAR PIERRE BONANNI
DÉLÉGUÉ À LA PROTECTION
DES DONNÉES DU CDG 30

Les pièges photographiques dans la lutte contre les décharges sauvages, une bonne ou une mauvaise idée ?

La problématique des dépôts sauvages d'ordures est une préoccupation majeure pour les collectivités, qui cherchent des solutions efficaces pour y remédier. Depuis de nombreuses années, les dépôts sauvages se multiplient malgré une gestion des déchets toujours mieux organisée, le plus souvent au niveau intercommunal.

Parmi les outils envisagés, les pièges photographiques se présentent comme une option technologique prometteuse. Moins coûteux qu'une caméra de vidéoprotection, mais aussi moins polémique, ces pièges pourraient permettre de prendre en flagrant délit et de confondre ceux qui souillent un territoire communal de plus en plus fragilisé par les questions environnementales.

Cependant, leur utilisation soulève des problématiques importantes en matière de protection des données et de respect de la vie privée.

Dans certains départements, comme le Var, des pièges photographiques ont été installés pour identifier les auteurs de

dépôts sauvages. Ces dispositifs, similaires à ceux utilisés pour l'étude des animaux sauvages, se déclenchent automatiquement à chaque passage et peuvent fonctionner de jour comme de nuit.

Des expérimentations ont eu lieu dans la Drôme et les Pyrénées-Orientales, ce qui a significativement aidé à identifier les contrevenants.

Pour autant, leur utilisation est-elle légale ? Repose-t-elle sur la même réglementation que la vidéoprotection ? Si la question semble simple, la réponse est, hélas, loin de l'être…

Il apparaît ainsi que la mise en place et l'utilisation de pièges photographiques n'est pas expressément encadrée par la loi ou la réglementation. Il existe donc ici un vide juridique qu'un rapport de la délégation sénatoriale aux collectivités territoriales a tenté de combler le 25 février 2022.

Ce rapport précise que, sans cadre juridique clair, l'emploi

d'un tel dispositif « *semble illégal* », et la délégation recommande ainsi la prudence quant à une telle utilisation, sans pour autant venir trancher définitivement la question.

Ainsi, faute de réponse claire, et dans l'attente d'une loi ou d'une réglementation spécifique, que pouvons nous répondre, nous autres délégués à la protection des données, quant à savoir si une collectivité peut ou non utiliser de tels moyens pour protéger leurs zones naturelles ?

Si l'installation d'un tel système n'est pas prévue, penchons nous donc sur son fonctionnement pour ensuite rechercher un cadre juridique adéquat qui nous permettrait de venir vous recommander ou non son utilisation.

Prenez la pose, vous êtes photographié !

Les pièges photographiques sont des dispositifs installés dans la nature aux endroits stratégiques habituellement pour évaluer, comptabiliser et/ou simplement photographier la faune sauvage. À la différence des systèmes de vidéoprotection, ces pièges n'enregistrent pas des images en continue et se déclenchent au passage d'un individu.

Ce fonctionnement est de nature à entraîner la capture de l'image d'un individu sans son consentement. Si cela ne pose aucun problème dans le cas de la vidéoprotection, dont le cadre juridique clairement établi permet un traitement légal de la donnée, cela n'est pas le cas du piège photographique qui souffre de ce vide juridique ! A ce sujet, le RGPD est pourtant très clair : dans son article 6, le règlement européen prévoit que les données ne puissent être traitées que si une base légale ne venait en justifier la licéité.

À défaut de l'une des bases légales mentionnées à cet article, seul le consentement de la personne pouvait venir autoriser le traitement de données.

Or, à défaut de cadre juridique, et à défaut de recueillir le consentement de la personne photographiée, il parait difficile d'autoriser la mise en place d'un tel système qui présente par conséquent un risque, d'une part, d'atteinte au droit à la vie privée, d'autre part, d'irrecevabilité des preuves obtenues par ce moyen.

Vers une évolution ?

Si les collectivités ne peuvent utiliser ces pièges dans la lutte contre les dépôts sauvages, l'article L.251-2 du code de la sécurité intérieure prévoit bien, parmi une liste de situations où l'autorité publique est autorisée à procéder à la captation d'images, la possibilité de constater « *des infractions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets* ». De ce fait, d'autres moyens peuvent êtres utilisés pour confondre les contrevenants, pour peu qu'un cadre légal vienne en autoriser l'utilisation.

C'est pourquoi, et face aux incertitudes du régime juridique des pièges photographiques (ou plutôt face à une certitude de leur interdiction au regard du RGPD), je ne peux que conseiller d'utiliser un bon vieux système de vidéoprotection classique, bien encadré et dont l'installation est contrôlée par le représentant de l'État dans le département.

Pour autant, si en tant que délégué à la protection des données, je ne peux que donner ce conseil, en tant qu'usager je ne peux que souhaiter qu'à terme une évolution réglementaire vienne permettre l'installation de tels outils pour sauver nos espaces naturels de la malveillance de ceux qui imposent leur pollution à tous ■

Le CDG 30 adhère officiellement à l'association française des correspondants à la protection des données à caractère personnel !

Dans notre volonté de fournir toujours un meilleur service public aux collectivités qui nous font confiance, notamment pour leur mise en conformité au RGPD, le Centre de Gestion du Gard a décidé d'adhérer à l'Association Française des Correspondants à la protection des Données Personnelles (AFCDP).

Il s'agit d'une structure qui regroupe une diversité de profils de professionnels de la protection des données personnelles au niveau national, parmi lesquels se trouvent notamment de spécialistes de la fonction publique territoriale.

La richesse que nous apporte cette adhésion se reflète dans l'accès à une veille juridique spécialisée que nous pouvons désormais mettre au profit de nos collectivités. De même, cette inscription nous permet de tirer parti et de participer aux échanges sur les problèmes opérationnels liés à la protection des données personnelles auxquels nous faisons face au quotidien et au déploiement du numérique dans le milieu de la fonction publique territoriale.

Le Centre de Gestion du Gard manifeste ainsi sa détermination à mettre en œuvre tous ses moyens pour respecter le RGPD et protéger les données personnelles et la vie privée des personnes qui sont sous sa responsabilité.

Rencontre annuelle des délégués à la protection des données des CDG de la région Occitanie à Nîmes

Les mardi 18 et mercredi 19 juin a eu lieu la 5ème réunion du Groupe de travail des Délégués à la Protection des Données des CDG d'Occitanie. Pour cette année le CDG 30 a eu le plaisir d'accueillir à Nîmes nos collègues venus de toute la région pour discuter autour d'un ordre du jour visant à mieux répondre aux enjeux actuels auxquels nos centres de gestion ainsi que nos collectivités adhérentes sont confrontées.

Cette réunion a rassemblé, comme chaque année, un éventail de spécialistes de la donnée des collectivités territoriales, cette année au nombre de 16 : des informaticiens, des archivistes, des juristes et des délégués à la protection des données qui ont pu mettre au profit leurs connaissances et leurs expériences sur le terrain. Les échanges ont notamment porté sur l'archivage des dossiers médicaux et les mesures visant à protéger ces données, sur l'hébergement des données de santé et enfin, sur les limites entre deux spécialistes aux métiers qui se croisent : le délégué à la protection des données et l'archiviste.

Ces échanges nous ont en outre permis de travailler sur l'impact de la directive NIS-2, dont la transposition est attendue au plus tard pour le 17 octobre prochain et dont l'objet sera de renforcer les mesures de cybersécurité dans de nombreux domaines, pour nos collectivités territoriales, concernées de par la gestion des carrières des agents, notre objectif étant de nous préparer d'ores et déjà aux changements qui seront nécessaires.

Enfin l'utilisation de l'intelligence artificielle dans les collectivités a été présentée, avec un test grandeur nature des outils existants, qui se trouvent performants et qui promettent d'apporter une vraie valeur ajoutée aux missions des agents.

Enfin, et parce que notre objectif est de toujours mieux vous servir, voici ci-contre une liste des outils conformes au RGDP recommandés au sein de la coordination régionale.

DOMAINE	OUTIL RECOMMANDÉ
Transfert de fichiers lourds	GrosFichiers, Smash, BlueFiles
Gestionnaire de mot-de-passe	Lockpass, Keepass
Messagerie instantanée	Tchap, Olvid
Gestionnaire d'agendas	Framagenda
Intelligence artificielle	Territorial GPT
Anti spam	MailInBlack
Sauvegarde des données	Duplicati

Recrutements : la CNIL rappelle les règles de la collecte des données personnelles des candidats

Saisie d'une plainte à l'encontre d'une société qui collectait de trop nombreuses données des candidats à l'embauche, la CNIL est venue rappeler les règles en matière de recrutements en adressant au responsable de traitements une mise en demeure de se conformer au RGPD.

En l'espèce, la société demandait des informations non pertinentes, telles que des informations relatives aux membres de la famille, le lieu de naissance du candidat, sa nationalité, ou encore le montant des salaires perçus par le passé.

La CNIL a ainsi estimé que ces données n'étaient en rien nécessaires au respect de la finalité du recrutement, et donc contraire au principe de **minimisation** de la collecte de données.

Ainsi, la CNIL est venue rappeler les règles à suivre lors d'un recrutement, à savoir que l'employeur ne peut **collecter que les données pertinentes ayant un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles**.

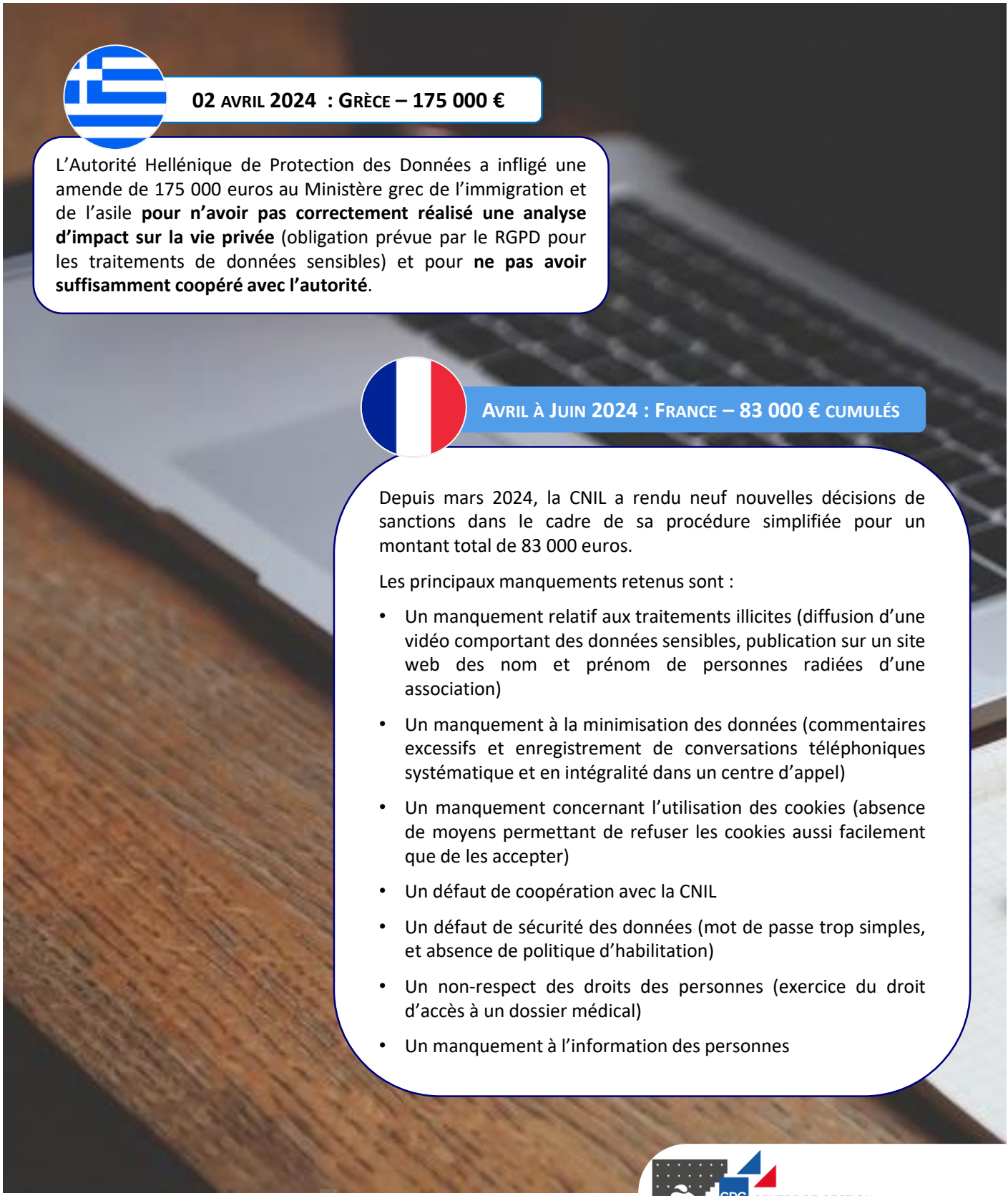
Ces recommandations sont donc les suivantes :

- Possibilité de demander des informations destinées à identifier le candidat
- Possibilité de demander des données liées aux compétences professionnelles (connaissances, savoir-faire ou savoir-être)
- Possibilité de demander les qualifications du candidat (diplômes, titres et expériences)
- Pour la fonction publique, possibilité de demander la nationalité (puisque celle-ci conditionne l'accès à un emploi en qualité de fonctionnaire)

Ainsi, seules ces données sont jugées pertinentes lors de la sélection des candidats. Ce n'est qu'au moment de l'embauche, soit une fois que les candidatures auront été définitivement retenues, que l'employeur pourra collecter des données supplémentaires, telles que l'état civil complet, comprenant la date et le lieu de naissance, l'adresse postale, le numéro de sécurité sociale, etc.

Il est donc important de savoir séparer chaque traitement pour ne collecter que les données strictement nécessaires au bon déroulement du traitement.

Les décisions des autorités chargées de la protection des données



02 avril 2024 : Grèce – 175 000 €

L'Autorité Hellénique de Protection des Données a infligé une amende de 175 000 euros au Ministère grec de l'immigration et de l'asile **pour n'avoir pas correctement réalisé une analyse d'impact sur la vie privée** (obligation prévue par le RGPD pour les traitements de données sensibles) et pour **ne pas avoir suffisamment coopéré avec l'autorité**.

Avril à Juin 2024 : France – 83 000 € cumulés

Depuis mars 2024, la CNIL a rendu neuf nouvelles décisions de sanctions dans le cadre de sa procédure simplifiée pour un montant total de 83 000 euros.

Les principaux manquements retenus sont :

- Un manquement relatif aux traitements illicites (diffusion d'une vidéo comportant des données sensibles, publication sur un site web des nom et prénom de personnes radiées d'une association)
- Un manquement à la minimisation des données (commentaires excessifs et enregistrement de conversations téléphoniques systématique et en intégralité dans un centre d'appel)
- Un manquement concernant l'utilisation des cookies (absence de moyens permettant de refuser les cookies aussi facilement que de les accepter)
- Un défaut de coopération avec la CNIL
- Un défaut de sécurité des données (mot de passe trop simples, et absence de politique d'habilitation)
- Un non-respect des droits des personnes (exercice du droit d'accès à un dossier médical)
- Un manquement à l'information des personnes

11 avril2024 : Italie – 6 000 €

La CNIL italienne a infligé une amende de 6 000 euros au Consortium communal libre d'Enna pour avoir **omis de désigner un délégué à la protection des données**.

11 avril2024 : Italie – 25 000 €

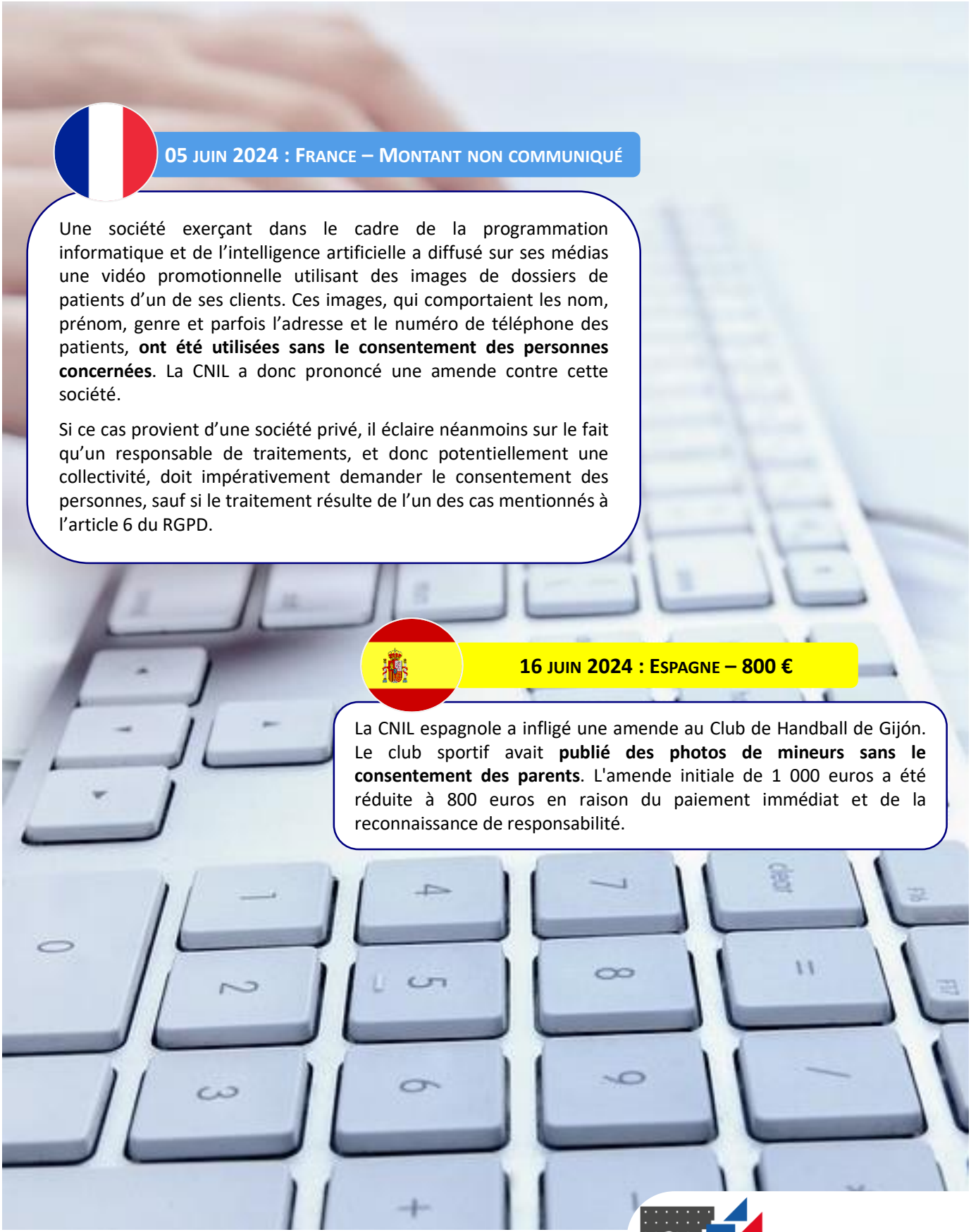
La CNIL italienne a infligé une amende de 25 000 euros à Innova Camara. Le contrôleur a subi une cyberattaque au cours de laquelle des bases de données ont été consultées et des fichiers malveillants ont été insérés. Au cours de son enquête, l'autorité de contrôle a constaté que le responsable du traitement **n'avait pas mis en œuvre les mesures techniques et organisationnelles appropriées pour protéger les données** personnelles afin d'éviter un tel incident.

09 mai 2024 : Italie – 75 000 €

La CNIL italienne a infligé une amende de 75 000 euros à la Société hospitalo-universitaire de Padoue. Au cours de son enquête, la commission a constaté que **des employés avaient accédé aux dossiers des patients sans autorisation** et que le responsable **n'avait pas mis en place de restrictions d'accès** appropriées. Cela permettait aux employés d'accéder aux dossiers des patients qui n'étaient pas nécessaires à leur travail, parce qu'ils ne soignaient pas les patients en question.

04 juin 2024 : Pays-Bas – 6 000 €

La CNIL néerlandaise a infligé une amende de 6 000 euros à la société de recrutement Ambitious People Group B.V. Le responsable du traitement **n'avait pas supprimé les données des personnes concernées après que celles-ci l'avaient demandé**.



05 juin 2024 : France – Montant non communiqué

Une société exerçant dans le cadre de la programmation informatique et de l'intelligence artificielle a diffusé sur ses médias une vidéo promotionnelle utilisant des images de dossiers de patients d'un de ses clients. Ces images, qui comportaient les nom, prénom, genre et parfois l'adresse et le numéro de téléphone des patients, **ont été utilisées sans le consentement des personnes concernées**. La CNIL a donc prononcé une amende contre cette société.

Si ce cas provient d'une société privé, il éclaire néanmoins sur le fait qu'un responsable de traitements, et donc potentiellement une collectivité, doit impérativement demander le consentement des personnes, sauf si le traitement résulte de l'un des cas mentionnés à l'article 6 du RGPD.

16 juin 2024 : Espagne – 800 €

La CNIL espagnole a infligé une amende au Club de Handball de Gijón. Le club sportif avait **publié des photos de mineurs sans le consentement des parents**. L'amende initiale de 1 000 euros a été réduite à 800 euros en raison du paiement immédiat et de la reconnaissance de responsabilité.

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Dammartin-en-Goële
26 mai 2024

Fleury-les-Aubrais
24 juin 2024

Gravelines
25 avril 2024

Saint-Nazaire
18 avril 2024

Raucourt-au-Bois
17 mai 2024

Saint-Nazaire agglomération
10 avril 2024

Communauté de communes du bassin de Pont-à-Mousson
04 avril 2024

Cenans
14 avril 2024

Floirac
18 avril 2024

Centre Hospitalier Cannes Simone Veil
15 avril 2024

Albi
22 avril 2024

Vauvert
mai 2024

Réseau internet de la Nouvelle-Calédonie
21 mai 2024

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

** Sur les trois derniers mois*

ENTRETIEN EXCLUSIF : RENCONTRE AVEC LES GENDARMES DU GARD !

Le lundi au soleil c'est une chose que l'on ne voit jamais, disait Claude François. Et c'est effectivement ce que je me dis, tandis qu'avec ma collègue, nous attendons serrés sous notre parapluie devant la grille de la Gendarmerie du Gard en ce lundi pluvieux du mois de mai. Par chance, le froid n'a pas réellement le temps de nous transpercer plus que les os, car rapidement, nous sommes accueillis chaleureusement par le Major Jean-Michel Macé, chef de la section opérationnelle de lutte contre les cybermenaces (SOLC). A la fraicheur du temps succède la chaleur de l'accueil des membres de la section, visiblement heureux de pouvoir nous accueillir dans leurs locaux.

"L'informaticien", ça n'existe pas

Après un rapide tour du propriétaire, nous présentant leur environnement de travail, le Major Macé nous en révèle un peu plus sur leur fonctionnement centré sur deux principes essentiels : la sécurité absolue et la confidentialité. Toutes les solutions logicielles, du système d'exploitation aux logiciels métiers sont ainsi développés en interne pour et par les services de la Gendarmerie nationale. Chaque poste et appareil téléphonique ou informatique doit ainsi être paramétré et équipé directement par les gendarmes de la section qui ont chacun leur spécialité. Car oui, « *l'informaticien* », ça n'existe pas : « *cette appellation regroupe un panel de spécialités très vaste* » sourit le Major Macé.

La section opérationnelle de lutte contre les cybermenaces est composée de 12 gendarmes basés à Nîmes. A ces 12 spécialistes s'ajoutent une centaine de « *correspondants N'TECH* », acronyme signifiant « *nouvelles technologies* », répartis sur tout le territoire et rattachés aux brigades locales du département du Gard.

Ces correspondants, formés à la cybersécurité sur toute une semaine, constituent la première ligne vers laquelle sont orientées les victimes des cyberattaques pour obtenir des conseils et un soutien qui peut s'avérer décisif dans les premières heures suivant l'un de ces événements. « *Les collectivités et les entreprises ont 72 heures pour déposer plainte, faute de quoi les assurances ne prendront pas en charge les*

conséquences et dommages de la cyberattaque » nous glisse le Major Macé tandis qu'il nous expose l'état de la menace dans le département.

La principale menace, c'est l'ignorance

Pour les gendarmes de la section, aucun doute : le principal défaut en matière de cybersécurité, c'est d'ignorer la menace et/ou de la glisser sous le tapis. Car si, selon le Major, les collectivités restent de bons élèves et portent facilement plainte en cas de cyberattaque, ce n'est pas forcément le cas pour les entreprises pour des raisons de réputation. Cependant, « les choses pourraient changer » nous explique le Major. « *Avec cette obligation de déposer plainte dans les 72 heures sans quoi l'assurance n'interviendra pas, on touche la corde sensible. Et c'est très important pour nous d'avoir connaissance de ces faits* » insiste le Major, qui explique que sans les plaintes, aucune investigation ne peut être menée, et de ce fait, la menace ne peut que continuer à se répandre.

Et en parlant des investigations, le Major Macé nous présente les gendarmes en charge du volet « Police judiciaire » de la section et dont les missions sont d'exploiter les nouvelles technologies pour assister les enquêteurs dans leurs recherches. Allant de la recherche de personnes disparues à la lutte contre la pédopornographie en passant par la lutte contre le narco banditisme, ces « cyber-enquêteurs » sont ainsi capables d'interroger et de faire avouer l'ordinateur le plus récalcitrant. Historique de recherches ou d'appels, messages envoyés ou reçus, photographies enregistrées ou effacées, géolocalisation de l'appareil… rien n'échappe aux gendarmes de la section qui sont capables de situer avec précision l'utilisation à un instant T de n'importe quel appareil, y compris d'en contrôler l'utilisation ou non lors d'un accident mortel de la route.

« *On est sur une menace mondiale* » précise le Major Macé. « *C'est fini, le lycéen qui attaque seul depuis sa chambre. On est plus sur des organisations criminelles importantes* ». Nous citant quelques exemples de motivations pour les attaquants, les gendarmes du Gard nous exposent ainsi l'état de la menace ciblant essentiellement les collectivités. « *Tout le monde peut se faire pirater. Un jour, fatigué, on baisse sa vigilance et on clique sur un fichier. Cela touche toutes les strates de la société : cela peut être des magistrats, des notaires… C'est même arrivé à des camarades qui, après s'être rendus compte de l'erreur, sont venus nous consulter* ».

« *Plus de 80% des attaques réussies sont le résultat d'un manque de vigilance* »

Pour autant, à ce volet « recherches et investigations » s'ajoute un dispositif dénommé « D.I.A.G.O.N.A.L. », qui consiste en une offre de diagnostic très poussé permettant aux collectivités et établissements publics d'évaluer leur maturité cyber et d'orienter leurs actions dans divers domaines liés aux nouvelles technologies.

A titre d'exemple, nos interlocuteurs nous présentent les statistiques révélées par l'ANSSI faisant état d'une moyenne de

10 incidents par mois déclarés par des collectivités territoriales entre janvier 2022 et juin 2023 (dont environs 2/3 de communes et d'EPCI à fiscalité propre).

Les principales cyber menaces vis-à-vis des collectivités et des administrations sont déjà très connues : le hameçonnage, le Rançongiciel et le piratage d'un système informatique.

Afin de parer à cette menace, les hommes du Major Macé sont unanimes : « *il faut sensibiliser nos agents, nos élus, et même nos usagers. Les délinquants trouvent aujourd'hui aisément des solutions « clé en main » pour se lancer dans les cyberattaques. Il est donc essentiel de savoir comment s'en prémunir* ».

Des diagnostics non-intrusifs

La Gendarmerie propose ainsi aux collectivités qui le souhaitent de réaliser un diagnostic non intrusif de leur sécurité numérique. « *C'est une démarche volontaire pour les collectivités* » précise le Major Macé. « *Plusieurs des collectivités qui nous sollicitent ont déjà eu des soucis et cherchent désormais à se protéger* ».

Ce diagnostic, organisé sur place et mené par le gendarme, permet l'établissement d'un rapport reprenant point par point l'ensemble des mesures de sécurité physique, informatique et organisationnelle nécessaires pour tenter de prévenir au maximum toute attaque contre les collectivités. Il s'agit d'une étude très vaste réalisée afin de fournir un service complet et adapté à chaque structure et de permettre à l'autorité territoriale d'avoir une vision plus claire de la situation de sa collectivité.

Cette offre permet d'orienter les actions dans tous les domaines clefs de la cybersécurité. Celui de l'organisation et de la stratégie, avec par exemple l'adoption d'une charte informatique. Des actions de sensibilisation et de veille, notamment par la prise en compte des risques liés au télétravail. Le sujet des prestataires est aussi abordé, en effet les gendarmes nous encouragent à avoir une connaissance approfondie des méthodes et pratiques liées à l'infogérance. Et, bien sûr, le RGPD fait partie également des sujets examinés et la désignation d'un Délégué à la Protection des données est une action incontournable et très utile. Ce sont juste quelques exemples des thématiques qui font partie du diagnostic D.I.A.G.O.N.A.L. « *Ce diagnostic est sans coût pour la collectivité* » insiste en souriant le Major Macé qui ajoute qu'à ce rapport sont également joints des outils, « *également sans coût* », pour permettre aux collectivités volontaires de renforcer leur sécurité.

Quelques outils recommandés

Sans coût !

FILIGRANE	Outil permettant d'ajouter un filigrane sur un document, rendant son utilisation sûre
HAVE I BEEN PWND	Site permettant de contrôler si votre adresse mail a été retrouvée parmi les données dérobée au cours d'une violation de données
KEEPASS	Gestionnaire de mots de passe certifié par l'ANSSI
ZEDFREE	Logiciel de transfert de fichiers chiffrés
OLVID	Messagerie instantanée française et sécurisée

Par la suite, les gendarmes de la SOLC se rendent sur place pour réaliser la restitution du travail dans le but de garder cette proximité et de « *répondre présent pour la cybersécurité* ».

Le rappel des règles d'hygiène informatique

Lors de notre rencontre, le Major ainsi que les gendarmes nous donnent naturellement plusieurs conseils d'hygiène informatique pour renforcer la sécurité des systèmes d'information. Ils conseillent, bien sûr, de se rendre sur le site de l'ANSSI et cybermalveillance.gouv.fr pour bénéficier des conseils et des outils mis à libre disposition. Dans ce sens, il est impératif de toujours opter pour une authentification forte, ou encore de contrôler rigoureusement les accès à nos différents comptes pour prévenir les intrusions non autorisées.

Notre messagerie doit être protégée par un mot de passe fort, de plus nous pouvons vérifier facilement et rapidement que notre mot de passe n'a pas été divulgué sur le Dark web grâce au site web « haveibeenpwned ». D'autre part, pour stocker nos mots de passe, ils nous encouragent à utiliser des solutions sans coût telles que le logiciel KeePass. Grâce à ce coffre-fort nous n'avons qu'à retenir un seul mot de passe pour ensuite avoir accès à tous les autres. Il est simple à télécharger et d'utilisation facile. Comme nous l'avons mentionné, les gendarmes du Gard possèdent aussi une mission de sensibilisation et de formation des administrés aux risques cyber. Ils recommandent aux collectivités de ne pas négliger cet aspect fondamental.

Sollicités par une commune, ils ont été présents en début de cette année 2024 dans le cadre d'une sensibilisation pour les parents aux risques qui affrontent les enfants sur le monde du cyber, des jeux vidéo ainsi que des réseaux sociaux. « *La plupart des jeux vidéo sur lesquels les enfants jouent sont des espaces où ils interagissent avec d'autres joueurs qui peuvent être des adultes se faisant passer par des gens de leur âge. Il faut donc rester vigilants sur tous les angles d'entrée pour ces personnes malveillantes* ».

Après avoir pris conscience de l'ampleur du risque, les parents ont pu profiter de l'occasion pour poser toutes leurs questions, auxquelles les gendarmes ont répondu à partir de leur vision en tant qu'experts de la cyber menace mais aussi, étant eux-mêmes des parents soucieux de la sécurité de leurs enfants.

D'autre part, suite à des mauvaises expériences de quelques malheureux, les gendarmes nous incitent à ne pas enregistrer notre carte bleue sur le web, notamment pour éviter les dégâts financiers si jamais un pirate a accès à nos comptes sur les sites des commerces en ligne. Pour mieux organiser la sécurisation des données détenues par nos collectivités des mesures organisationnelles sont ainsi évoquées, ils recommandent l'adoption d'une charte informatique, document qui détaille les droits et les devoirs de l'utilisateur. La sensibilisation des agents et des élus fait également partie des conseils fournis. En effet, le moyen le plus facile de réussir une cyberattaque contre une collectivité est de contourner la technique en ciblant le personnel. Des opérations de sensibilisation sur les risques cyber et les bonnes pratiques doivent être réalisées assez régulièrement. Il faut notamment être attentif aux techniques de manipulation de l'ingénierie sociale, les cybers délinquants cherchent à obtenir des informations ou des biens en exploitant la confiance ou la crédulité de tierces personnes. La mobilité et le télétravail sont aussi à prendre en compte comme des thématiques fondamentales.

Vers une collaboration renforcée

« *Nous parlons du service Protection des données par là où l'on passe* », nous confirment nos interlocuteurs avec le sourire. Nous sommes ainsi honorés de constater que, depuis qu'ils ont découvert notre service, les gendarmes du département du Gard recommandent notre prestation aux collectivités territoriales. « *Les collectivités sont de plus en plus volontaires pour se mettre en règle vis-à-vis de la protection des données* », ajoute le Major Macé.

Nos interlocuteurs nous confirment par ailleurs leur volonté de développer des partenariats avec l'ensemble des acteurs pouvant permettre aux collectivités territoriales de mieux se protéger. Nous partageons

bien entendu cette volonté de coordonner nos efforts. « *Nous intervenons également auprès des usagers* », ajoute le Major Macé. « Nous proposons des réunions d'information afin de les sensibiliser aux risques cyber ». Ces interventions, nous confie-t-il, sont essentiellement réalisées auprès d'un public jeune, au sein des établissements scolaires, mais peut également être à destination d'un public adulte sur demande de collectivités.

Vers la fin de notre rencontre, les gendarmes nous confient que de nouveaux renforts au sein de leurs équipes sont attendus prochainement. En effet, une formation sur deux ans est désormais proposée pour les personnes qui souhaitent intégrer les forces de l'ordre en matière cyber. Ce renfort, très demandé, répond à la montée de l'activité des gendarmes du Cybergend.

Après ces échanges riches, nous prenons congé des hommes de la SOLC et retournons sous une pluie battante dans notre bureau, riches de nouvelles idées pour aider nos collectivités à avancer dans leur mise en conformité et la sécurisation de leurs données. Nous tenions à remercier chaleureusement le Major Macé et ses hommes pour leur charmant accueil et les informations partagées ■

MINISTÈRE DE L'INTÉRIEUR

SECTION OPERATIONNELLE DE LUTTE CYBERMENACES

cybergend30@gendarmerie.interieur.gouv.fr

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

Tous les cookies ne se mangent pas !

Protégez votre vie privée, ne les acceptez pas !

SERVICE PROTECTION DES DONNÉES

CENTRE DE GESTION DU GARD

04 66 38 86 86

dpd@cdg30.fr

Assurer la sécurité 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]

Afin d'assurer la sécurité des archives de votre collectivité, voici quelques éléments d'informations sur les procédures à suivre en cas de vol ou de sinistre.

« *Les archives publiques sont imprescriptibles. **Nul ne peut détenir sans droit ni titre des archives publiques**. Le propriétaire du document, l'administration des archives ou tout service public d'archives compétent peut **engager une action en revendication d'archives publiques**, une action en nullité de tout acte intervenu en méconnaissance du deuxième alinéa ou une action en restitution. Lorsque les archives publiques appartiennent au domaine public, les actions en nullité ou en revendication s'exercent dans les conditions prévues aux articles L.112-22 et L.112-23. Les modalités d'application des dispositions qui précèdent sont fixées par décret en Conseil d'Etat.* » [Code du Patrimoine, article L.212-1].

« *Avant d'engager l'action en revendication ou en restitution prévue par l'article L.212-1, le propriétaire, l'administration des archives ou le service public d'archives compétent pour conserver les archives en cause adresse, par lettre recommandée avec demande d'avis de réception, une **mise en demeure** au détenteur de ces archives. Lorsque les archives publiques sont mises en vente, la mise en demeure est adressée à la personne qui procède à la vente, si l'identité du vendeur n'est pas connue.* » [Code du Patrimoine, article L.212-7].

En cas de vols, de disparition ou de détournement (articles 311-4-2, 433-4 et 432-15 du Code Pénal) :

- Effectuer un dépôt de plainte dès la constatation d'un vol, d'une disparition ou d'un détournement
- Réaliser un dossier documentaire nécessaire à l'identification des biens, effectuer un récolement
- Diffuser l'information auprès des services compétent (AD, SIAF, Pôle Judiciaire de la Gendarmerie Nationale (SCRC - Service Central de Renseignement Criminel, anciennement STRJD) et à l'Office Central de lutte contre le trafic des Biens Culturels (OCBC-Direction centrale de la Police judiciaire) et le conseiller sûreté des archives de la direction générale des Patrimoines (Mission Sécurité, Sûreté et Accessibilité – inspection des patrimoines))

En cas de sinistre

- Suivre les procédures précisées dans le plan de sauvegarde / plan de mise en sûreté de votre collectivité
- Informer immédiatement le sinistre à la Direction des Archives Départementales par téléphone ou mail puis **en adressant une notification écrite au préfet**
- En fonction de la gravité de l'événement, une équipe des Archives départementales se rend sur place pour guider et contrôler les mesures prises par la collectivité. Le directeur des Archives départementales transmet un rapport au préfet pour suite à donner

La prévention est de mise car il s'agit du moyen le plus sûr de protéger les archives de votre collectivité.

- L'accès au local archives doit être verrouillé (clé spécifique) et contrôlé grâce à un registre de consultation des archives
- La consultation, uniquement sur place, doit se faire sous la surveillance d'un agent territorial
- Le local archives doit être un local dédié, aux normes et sécurisé. Une subvention des Archives Départementales peut vous aider à sa réalisation (aménagement des espaces d'archivage et installation d'équipements de protection incendie)

LA GÉOLOCALISATION DES VÉHICULES

I. Pourquoi collecter ces données?

Des dispositifs de géolocalisation peuvent être installés dans des véhicules utilisés par des agents pour des finalités d'intérêt légitime (cf. article 6.1.f) du RGPD :

- ✓ ***Suivre, justifier et facturer une prestation de transport de personnes ou de services*** directement liée à l'utilisation du véhicule (par exemple dans le cadre des missions du service technique, des services de police municipale, des services de transport, etc.).
- ✓ ***Assurer la sécurité de l'agent ou des véhicules dont il a la charge***, et notamment retrouver le véhicule en cas de vol (par exemple, avec un dispositif inerte activable à distance à compter du signalement du vol).
- ✓ ***Mieux allouer des moyens*** pour des services à assurer en des lieux dispersés
- ✓ Accessoirement, ***suivre le temps de travail***, lorsque cela ne peut être réalisé par un autre moyen.
- ✓ ***Respecter une obligation légale ou réglementaire*** imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des bien transportés
- ✓ ***Contrôler l'utilisation adéquate du véhicule au regard des règles*** en vigueur dans la collectivité
- ✓ ***Permettre la traçabilité des interventions sur le territoire***

UTILISATIONS A EXCLURE :

Un dispositif de géolocalisation installé dans un véhicule mis à la disposition d'un agent ne peut pas être utilisé :

- Pour contrôler le respect des limitations de vitesse
- Pour contrôler un agent en permanence
- Pour suivre les déplacements des représentants du personnel dans le cadre de leur mandat
- Pour collecter la localisation en dehors du temps de travail (trajet domicile travail, temps de pause, etc.) y compris pour lutter contre le vol ou vérifier le respect des conditions d'utilisation du véhicule
- Pour calculer le temps de travail des employés alors qu'un autre dispositif existe déjà

II. Comment ça marche ?

Les actions à réaliser sont les suivantes :

1. Une **étude des risques sur la sécurité des données** est nécessaire afin de définir les mesures les mieux adaptées (analyse d'impact);
2. **Saisine du CST** auquel il faut joindre l'analyse d'impact;
3. **Délibération du Conseil municipal**

Le responsable du traitement doit procéder à **l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre du dispositif** de géolocalisation des agents.

Les agents doivent être informés individuellement de l'installation de ce dispositif et doivent pouvoir accéder aux données les concernant enregistrées par l'outil (dates et heures de circulation, trajets effectués, etc.). D'autre part, ils doivent pouvoir désactiver la collecte ou la transmission de la localisation géographique en dehors du temps de travail.

III. Quelles données collecter ?

Les catégories de données collectées sont les suivantes :

- **Données d'identification de l'agent** : nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule ;
- **Données relatives à l'utilisation du véhicule** : données de localisation, heures et dates d'utilisation du véhicule; historique des déplacements effectués, vitesse de circulation du véhicule, temps de conduite, nombre et localisation des arrêts, temps de stationnement, itinéraire emprunté, kilomètres parcourus et alertes entretiens.

IV. Assurer la sécurité des données

Des mesures de sécurité sont à prendre en compte afin **d'éviter que des personnes non autorisées accèdent aux informations du dispositif.** Par exemple, l'accès au dispositif de suivi en temps réel sur un site web doit se faire avec un **identifiant et un mot de passe**. Il faut prévoir :

- Une **politique d'habilitation**
- Une **sécurisation des échanges**
- Une **journalisation** des accès aux données et des opérations effectuées (prévoir un registre papier à défaut de système de journalisation électronique)
- Une **étude des risques sur la sécurité des données** (analyse d'impact).

ATTENTION:

Les **outils ou logiciels développés par des prestataires restent sous la responsabilité de l'autorité territoriale** qui doit vérifier que ces outils ou logiciels respectent les obligations de la loi (clause contractuelle sur les obligations du sous-traitant en matière de sécurité et de confidentialité des données), notamment les mesures de sécurité.

V. Le transfert des données vers un prestataire

L'accès aux informations du dispositif de géolocalisation doit être **limité au personnel habilité des services concernés et à l'autorité territoriale**.

Exemple : un salarié d'une société souhaitait obtenir de son employeur les relevés du dispositif de géolocalisation installé dans son véhicule à la suite d'un accident de la circulation. La société refusait que les salariés obtiennent une copie de ces documents. Saisie d'une plainte par le salarié, la société a été mise en demeure de fournir au salarié la copie de ses données. Faute de réponse satisfaisante de l'employeur, la CNIL a prononcé une sanction de 10 000 euros à son encontre.

VI. Combien de temps conserver les données ?

Les informations ne doivent pas être conservées plus de **deux mois**.

Elles peuvent être conservées **un an** lorsqu'elles sont utilisées pour conserver un historique des déplacements ou à des fins de preuve des interventions effectuées.

Pour le suivi du temps de travail, seules les données relatives aux horaires effectués peuvent être conservées pendant une durée de **cinq ans.**

VII. Les mentions d'information

Chaque **agent doit être informé** :

- ✓ de l'identité du responsable de traitement ;
- ✓ des finalités (objectifs) poursuivies ;
- ✓ de la base légale du dispositif (par exemple : obligation issue du code du travail, ou intérêt légitime de l'employeur) ;
- ✓ des destinataires des données issues du dispositif de géolocalisation ;
- ✓ de son droit d'opposition pour motif légitime ;
- ✓ de la durée de conservation des données ;
- ✓ de ses droits d'accès et de rectification ;
- ✓ de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'un **avenant au contrat de travail**, d'une **note de service** ou d'un **courriel adressé à chacun des agents**. Une **notice peut être fournie systématiquement à l'embauche d'un nouvel agent** lors de la signature de son contrat de travail.

Cette information doit également **figurer sur la charte informatique de la commune**.

Modèle de mention d'information

GÉOLOCALISATION DES VÉHICULES DE LA COMMUNE DE [ ]

Conformément aux obligations du règlement (UE) n°2016/679 du 27 avril 2016 dit « règlement général sur la protection des données » (RGPD), **la Mairie de [commune], représentée par M. / Mme. [ ], Maire, en tant que responsable du traitement**, vous informe de sa décision d'installer dans les véhicules qui sont mis à disposition des agents communaux un système permettant de les localiser en temps réel.

La base légale du traitement est **l'intérêt légitime** (cf. article 6.1.f) du Règlement européen sur la protection des données (RGPD).

Les données personnelles collectées ne seront utilisées que dans le but de répondre aux finalités citées ci-dessous, les données ne seront pas utilisées à des fins sortant du cadre de la finalité demandée.

- Suivre, justifier et facturer une prestation de transport de personnes ou de services directement liée à l'utilisation du véhicule (chercher des exemples) prestation d'archiviste, à voir d'autres.
- Assurer la sécurité de l'agent ou des véhicules dont il a la charge, et notamment retrouver le véhicule en cas de vol (par exemple, avec un dispositif inerte activable à distance à compter du signalement du vol).
- Mieux allouer des moyens pour des services à assurer en des lieux dispersés
- Accessoirement, suivre le temps de travail, lorsque cela ne peut être réalisé par un autre moyen.
- Respecter une obligation légale ou réglementaire imposant la mise en œuvre d'un dispositif de géolocalisation en raison du type de transport ou de la nature des bien transportés
- Contrôler l'utilisation adéquate du véhicule au regard des règles en vigueur dans la collectivité
- Permettre la traçabilité des interventions sur le territoire

Le système n'a pas pour objet le suivi du temps de travail des salariés et ne permet pas davantage de contrôler les déplacements en-dehors du temps de travail.

Les **catégories de données** collectées sont les suivantes :

- **Identification de l'employé :** nom, prénom, coordonnées professionnelles, matricule interne, numéro de plaque d'immatriculation du véhicule ;
- **Données relatives aux déplacements des employés** : données de localisation issues de l'utilisation d'un dispositif de géolocalisation, nombre de kilomètres parcourus, historique des déplacements effectués.

Les données collectées sont uniquement destinées aux agents habilités à en avoir accès. Elles ne seront conservées au-delà d'une durée de deux mois.

Vous pouvez accéder aux données vous concernant ou demander leur effacement. Vous disposez également d'un droit d'opposition, d'un droit de rectification et d'un droit à la limitation du traitement de vos données (cf. cnil.fr pour plus d'informations sur vos droits). Pour exercer ces droits ou pour toute question sur le traitement de vos données dans ce dispositif, vous pouvez contacter nos services à l'adresse [adresse mail], ou par voie postale à l'adresse suivante :

Mairie de [commune]

[adresse]

[code postal]

[commune]

Si vous estimez, après nous avoir contactés, que vos droits Informatique et Libertés ne sont pas respectés ou que le dispositif de géolocalisation n'est pas conforme aux règles de protection des données, vous pouvez adresser une réclamation ligne à la CNIL (www.cnil.fr) ou par voie postale à l'adresse :

Commission Nationale de l'Informatique et des Libertés

3 place de Fontenoy

TSA 80 715

75 334 PARIS CEDEX 07

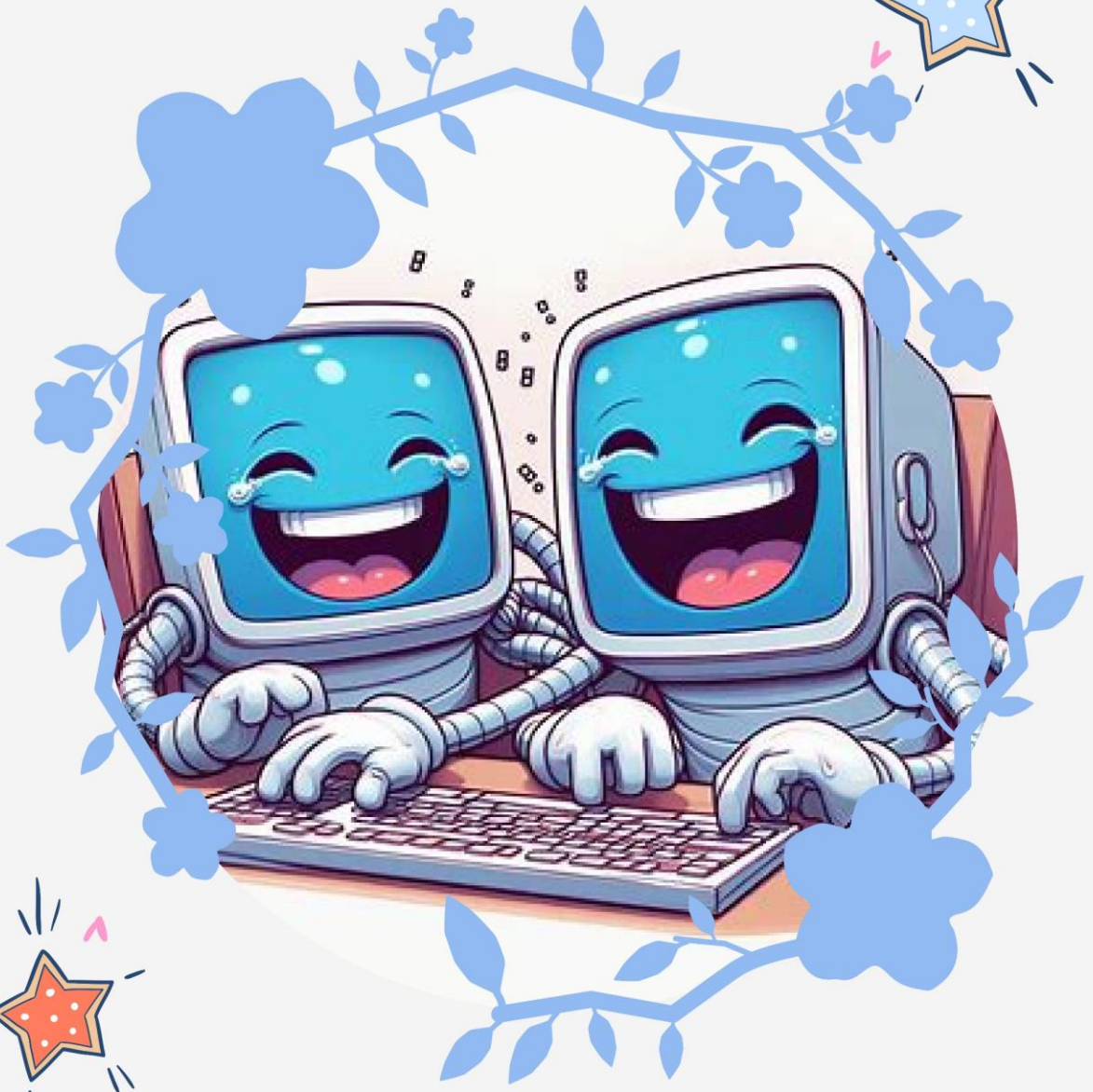
☐ J'autorise la Mairie de **[commune]** à conserver mes données dans un but d'information sur la vie municipale

Fait à

Le

Signature

LES DONNÉES, C'EST COMME LES BLAGUES



ON PEUT LES PARTAGER, MAIS PAS AVEC N'IMPORTE QUI !

SERVICE PROTECTION DES DONNÉES

CENTRE DE GESTION DU GARD

04 66 38 86 86

dpd@cdg30.fr