CYBERACTU'

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

Janvier 2025

Idée de bonne résolution : Prenez soin de vos collaborateurs !

Dossier page 13

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

ÉDITO

Après une année chargée en matière de protection des données, nous avons souhaité prendre un peu de temps pour réfléchir à une nouvelle orientation bénéfique pour notre service. Avec le temps et les nombreuses visites en collectivités, il nous est apparu nécessaire de nous orienter vers le côté humain de notre action. Car si notre but c'est de protéger les données des citoyens, nous n'oublions pas que dans nos collectivités, de nombreux agents travaillent avec la meilleure volonté du monde pour rendre un service public de qualité. Et ce sont ces hommes et ces femmes envers qui nous avons souhaité nous tourner à l'aube de cette nouvelle année.

Nous allons donc redoubler d'efforts pour que cette année 2025 soit placée sous le signe du bien-être et de la qualité de vie au travail.

A toutes et tous, nous vous souhaitons la meilleure des années 2025, pleine de réussites et de joies. Car c'est bien là le plus important.

Pierre BONANNI – Ana VEGA

Sarah ROMAN

Contacts

Service « Protection des données »

☎ : 04 66 38 86 86

@ : dpd@cdg30.fr

LANCEMENT DU « 17CYBER » PAR CYBERMALVEILLANCE

Par un communiqué du 17 décembre 2024, le GIP cybermalveillance.gouv.fr a officiellement lancé son nouvel outil d'aide aux acteurs numériques dénommé « 17Cyber ». Référence directe au numéro d'urgence des services de police, cet outil consiste en un guichet unique, disponible 24h/24 et 7j/7, permettant aux victimes de réaliser un rapide diagnostic afin de comprendre à quel type de menace ils sont confrontés et ainsi recevoir des conseils personnalisés en fonction de l'atteinte subie.

Si le diagnostic confirme la gravité de l'atteinte subie, ou si la victime la connaît déjà, celle-ci peut alors **échanger par tchat avec un policier ou un gendarme** pour disposer des conseils de première urgence et engager les démarches de judiciarisation.

Lorsque cela est nécessaire, les usagers peuvent également recevoir une assistance technique d'un prestataire référencé ou labellisé par cybermalveillance.

En complément du site 17cyber.gouv.fr, cybermalveillance met également à disposition **de tous un module « 17Cyber » qui peut être directement intégré aux sites web** afin de rendre accessible au plus grand nombre ce nouveau service de diagnostic et d'assistance aux victimes.

Ainsi, à partir de n'importe quel site ayant intégré ce module, tout utilisateur, particulier comme collectivité, association ou entreprise, peut effectuer ses démarches et bénéficier d'une aide personnalisée. **Entièrement gratuit**, ce module a été conçu pour être facilement intégré à n'importe quel site web en moins de 10 minutes.

Pour plus d'informations, vous pouvez vous rendre sur le site de cybermalveillance.gouv.fr

---

CLÔTURE DE LA PROCÉDURE À L'ENCONTRE DE LA MAIRIE DE KOUROU

La commune de Kourou (Guyane), comme toute collectivité, a pour obligation de désigner un délégué à la protection des données (article 37 du RGPD). La CNIL lui avait rappelé cette obligation à plusieurs reprises, successivement par une mise en demeure puis par une décision de sanction d'un montant de 5 000 € en février 2023.

En raison de la persistance des manquements, une seconde sanction de 5 000 € avait été prononcée le 12 décembre 2023, assortie d'une astreinte, c'est-à-dire une somme d'argent à payer en cas de non-respect d'une décision, de 150 € par jour de retard à l'issue d'un délai de deux mois.

Le 22 juillet 2024, constatant que la commune de KOUROU n'avait toujours pas désigné un délégué à la protection des données, la formation restreinte avait alors procédé à la liquidation de l'astreinte (c'est-à-dire

l'amende pour les jours de retard) pour un montant de 6 900 €, correspondant à la période du 19 février 2024 au 4 avril 2024.

Après la liquidation de cette astreinte, la commune de Kourou a enfin désigné un délégué à la protection des données, débutant ainsi son travail de mise en conformité au RGPD. La CNIL a ainsi décidé, par une décision en date du 7 novembre 2024, de clore cette procédure qui aura coûté à la commune, et donc à ses administrés, pas moins de 16 900 € cumulés pour ne pas avoir pris la peine de simplement désigner un délégué à la protection des données.

28 JANVIER 2025 : N'OUBLIEZ PAS LA JOURNÉE MONDIALE DE LA PROTECTION DES DONNÉES

Créée en 2006 à l'initiative du Conseil de l'Europe, la journée européenne de la protection des données est désormais célébrée dans le monde entier le 28 janvier de chaque année et est ainsi l'occasion de rappeler l'importance de la protection des données personnelles et de la vie privée à l'occasion d'actions de sensibilisations.

Marquez donc cette date d'une croix rouge sur votre calendrier. Elle sera l'occasion de démontrer à vos collaborateurs et à vos usagers votre engagement envers la protection de leur vie privée tout en les sensibilisant au respect des gestes de sécurité élémentaires.

VIDÉOSURVEILLANCE INTELLIGENTE : LA CNIL MET EN DEMEURE SIX COLLECTIVITÉS

Si le cadre juridique de la vidéosurveillance ou de la vidéoprotection intelligente (aussi dite « algorithmique ») était peu étoffé et ne s'était pas développé aussi rapidement que les technologies concernées, laissant nombre de collectivités dans le flou, la CNIL est venue depuis apporter sa pierre à l'édifice en renforçant sa doctrine en la matière.

A l'issue de contrôles réalisés au sein du Ministère de l'Intérieur et de plusieurs collectivités territoriales, la CNIL a ainsi rendu publique plusieurs mises en demeure le 5 décembre 2024.

Mais tout d'abord, reprenons le contexte de cette affaire…

A l'automne 2023, le média d'investigation « Disclose » avait dénoncé une utilisation illégale par la police de l'utilisation du logiciel Briefcam, qui permet des reconnaissances automatiques des images grâce à l'intelligence artificielle. Une polémique avait alors éclaté, et la CNIL avait entamé des investigations auprès des principaux concernés, dont plusieurs collectivités ; l'enquête menée par « Disclose » ayant démontrée qu'une centaine de villes en France avaient également recours à cet outil.

Par son communiqué du 5 décembre, la CNIL est cependant venue se montrer plus rassurante, et a rappelé que c'est l'utilisation **en temps réel** de ce genre de logiciel qui est interdite, l'utilisation en différé étant autorisée dans le cadre des enquêtes judiciaires et sous réserve

du respect d'un certain nombre d'obligations. Elle rappelle également que la détention d'un tel logiciel n'est pas illégal tant que la fonctionnalité n'est pas utilisée en temps réel.

Au final, six collectivités ont été mises en demeure. Si elles n'ont pas utilisé le logiciel pour effectuer de la reconnaissance faciale, elles ont en revanche utilisé le logiciel pour détecter automatiquement des événements anormaux, comme un stationnement interdit, une circulation à contresens ou des attroupements.

De même, et pour d'autres usages pourtant autorisés, la

CNIL a pointé du doigt l'absence ou l'insuffisance d'information du public. Ces utilisations couvraient notamment des études statistiques sur la fréquentation d'une zone pour le calcul des mobilités.

Enfin, la CNIL a profité de cette mise en demeure pour rappeler que **l'utilisation des fonctionnalités de recherches automatique dans les images** (système LAPI, par exemple) **pour répondre à des réquisitions judiciaires ne doit pas se faire à l'initiative des agents de police municipale**.

JOURNÉE RGPD À MONTPELLIER : LE CDG 30 Y ÉTAIT !

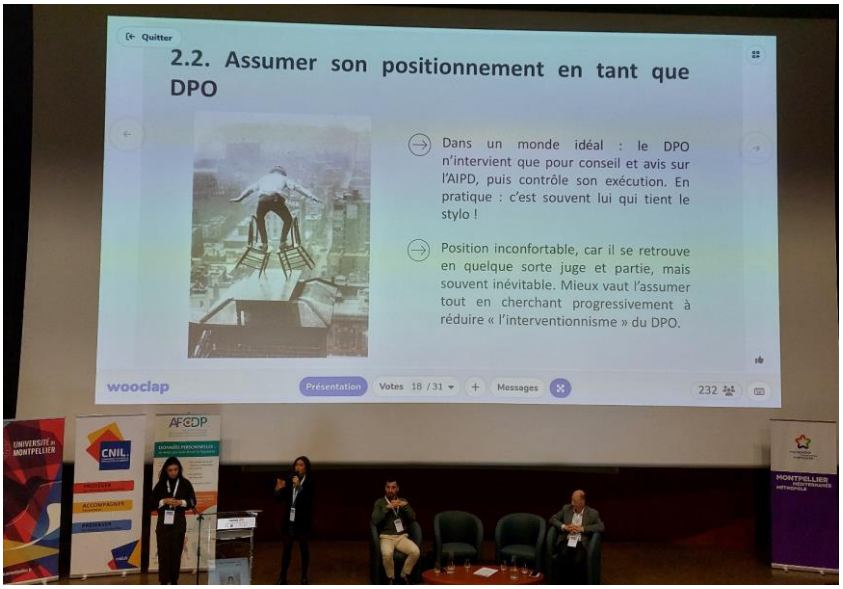
Lancées par la CNIL en 2022 en partenariat avec l'AFCDP, les journées RGPD consistent en une suite de déplacements en région afin d'échanger sur l'application du RGPD, de la conformité et des outils pour y parvenir.

Dernière en date, celle du 4 décembre 2024 organisée à Montpellier en partenariat avec la région Occitanie, la Métropole de Montpellier, l'AFCDP ainsi que l'Université de Montpellier, autour de thématiques diverses, tel que l'application du RGPD au secteur RH, un partage de bonnes pratiques pour l'activité de délégué à la protection des données, ou encore la gestion des plaintes auprès de la CNIL.

Cette journée très enrichissante a été l'occasion d'échanger avec de nombreux acteurs de la protection des données, notamment d'autres délégués à la protection des données, mais également de professionnels, dont Laurence Franceschini, commissaire de la CNIL, ou encore Marc Sztulman, conseiller régional délégué au numérique et Président de Cyber'Occ. C'est ainsi devant une salle pleine que de nombreux intervenants se sont succédés pour présenter tant les dernières actualités de la protection des données et de la cybersécurité que de nombreux conseils dans l'exercice du métier de délégué à la protection des données, ou dans la mise en conformité de nos organisations.

Présent toute la journée, notre délégué à la protection des données a ainsi eu l'occasion d'échanger avec Mathieu Ginestet, juriste au service des délégués de la CNIL, au sujet de l'évolution du RGPD dans les collectivités, mais aussi avec Sophie Genvresse chef du service de l'exercice des droits et des plaintes de la CNIL.

Ainsi, selon les interlocuteurs de la CNIL, l'essentiel des plaintes effectuées, qu'il s'agisse de plaintes à l'encontre des collectivités où à l'encontre de sociétés privés, s'effectuent à l'encontre de traitements de données du quotidien, dès lors qu'un traitement vient à gêner un usager. Un administré aura donc moins tendance à porter plainte envers sa collectivité pour un problème lié aux registres d'Etat civil que pour un problème lié à l'utilisation de la vidéoprotection.



La CNIL ajoute également que le nombre de plaintes a explosé ces dernières années, y compris à l'encontre de collectivités territoriales, rendant donc de plus en plus pressant la mise en conformité de celles-ci, bien que l'autorité reconnaisse avoir conscience des difficultés des très petites communes pour s'adapter et préfère ainsi orienter son action à leur destination vers de la sensibilisation.

Notre service espère donc l'organisation prochaine d'une nouvelle journée RGPD, centrée sur d'autres thématiques intéressantes, qui nous permettront d'accompagner encore mieux nos collectivités et établissements publics.

3ÈME ÉDITION DU BAROMÈTRE DE LA MATURITÉ CYBER DES COLLECTIVITÉS

Menée par cybermalveillance, cette enquête montre cette année un phénomène de plus en plus inquiétant avec l'accroissement de l'écart dans la prise de conscience du risque cyber entre les petites et les grosses collectivités.

Ainsi, 47% des collectivités de moins de 1 000 habitants s'estiment faiblement exposées aux risques. Ces collectivités représentent pourtant l'essentiel de nos communes sur le territoire français, et 1/10ème des répondants déclarent avoir déjà été victime d'une ou plusieurs cyberattaques au cours des 12 derniers mois.

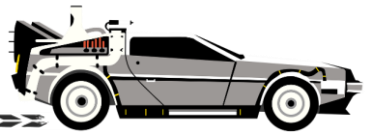
A la lecture de ces chiffres, nous renouvelons notre appel à une prise de conscience quant à l'importance de se protéger des cyberattaques qui font non seulement peser un risque juridique lourd sur nos collectivités, avec de fortes sanctions à la clé, mais également un risque technique critique avec une interruption des activités et des services, mais également une destruction ou un vol des données de nos citoyens.

Pour retrouver l'intégralité du baromètre, rendez-vous sur cybermalveillance.gouv.fr

RETOUR VERS 2024

NOMBRE DE COLLECTIVITÉS → 128
NOMBRE DE VISITES → 58

→ LE FAIT MARQUANT LES CYBERMATINÉES ←



NOS FÉLICITATIONS 2024 POUR LA COMMUNE DE SAINT-GERVAIS !

Située dans le Gard Rhodanien, aux portes de la vallée de la Cèze, la commune de Saint-Gervais (809 habitants) a adhéré au service protection des données à la toute fin de l'année 2019.

Avec l'arrivée en 2020 d'une nouvelle équipe, et malgré les difficultés liées au contexte sanitaire de l'époque, de lourds travaux ont été menés pour sécuriser la Mairie et accueillir convenablement les usagers.

Un nouvel audit de sécurité a ainsi été mené en cette fin d'année 2024 ayant démontré que la commune… remplissait toutes les exigences de sécurité préconisées par la CNIL !

Nous ne pouvons que féliciter l'équipe pour son engagement envers la protection des données de ses citoyens et l'exemple qu'ils peuvent inspirer pour les autres collectivités gardoises.

Mairie de Saint-Gervais – Source : Archives du CDG30

INGÉNIERIE SOCIALE : LES ESCROCS NE FONT PAS DE PAUSE. VOUS NON PLUS, RESTEZ VIGILANT !

SERVICE PROTECTION DES DONNÉES

CENTRE DE GESTION DU GARD

04 66 38 86 86

dpd@cdg30.fr

Les décisions des autorités chargées de la protection des données

21 octobre 2024 : Norvège – 20 800 €

L'autorité norvégienne de protection des données a infligé une amende de 20 800 euros à la municipalité de Grue (Østlandet) à la suite de la notification par la municipalité d'une violation de données*. La municipalité a indiqué que des données personnelles d'étudiants avaient été publiées illégalement sur un portail public. Au cours de son enquête, l'autorité a constaté que la municipalité **n'avait pas pris suffisamment de mesures techniques et organisationnelles** pour assurer la protection des données à caractère personnel.

17 octobre 2024 : France – Rappel à l'ordre

La CNIL a rappelé à l'ordre le ministère de l'Intérieur et le ministère de la Justice pour leur mauvaise gestion du fichier de traitement d'antécédents judiciaires (TAJ). Fichier recensant des informations relatives aux victimes, aux personnes mises en causes et aux prévenus, le traitement d'antécédents judiciaires est habituellement utilisé dans le cadre d'enquêtes judiciaires.

Pourtant, la CNIL a constaté plusieurs manquements, et notamment la conservation de données inexactes, du fait de la non transmission par les parquets des décisions de relaxe, d'acquittement, de non-lieu ou de classement sans suite.

La CNIL a également relevé que l'information communiquée lors de la collecte des données n'était pas spécifique au fichier TAJ et pouvait être lacunaire, voire inexistante. Ainsi, les intéressés étaient susceptibles d'ignorer jusqu'à l'existence même de ce fichier. Enfin, la CNIL a également relevé que les services gestionnaires du TAJ éprouvent des difficultés à obtenir des réponses de la part des parquets consultés dans le cadre des demandes de droit d'accès de particuliers et considère que cela porte atteinte à l'effectivité des droits des personnes.

**une telle sanction peut inciter les collectivités à ne pas notifier leurs violations de données lorsqu'elles surviennent.*

*Cependant, ne pas notifier une violation de données fait encourir à la collectivité un risque juridique important avec un **doublement des sanctions encourues**, le **refus de la prise en charge du sinistre par les compagnies d'assurance**, ou encore un risque de **poursuites pénales envers l'autorité territoriale**.*

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Le Havre
31 décembre 2024

Clairefontaine-en-Yvelines
15 octobre 2024

Hospi Grand Ouest « La Sagesse »
03 octobre 2024

Angers
31 décembre 2024

Poitiers
31 décembre 2024

Bordeaux
31 décembre 2024

Oyonnax
02 octobre 2024

Tarbes
31 décembre 2024

Nice
31 décembre 2024

Département des Hautes-Pyrénées
07 novembre 2024

Marseille
31 décembre 2024

Montpellier
31 décembre 2024

Nîmes
31 décembre 2024

Mauguio
22 octobre 2024

Département de La Réunion
13 novembre 2024

** Sur les trois derniers mois*


17 CYBER
MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER
Cybermalveillance.gouv.fr
Ayez le nouveau réflexe cyber :
rendez-vous sur le site
17Cyber.gouv.fr
Gratuit et sans abonnement

IDÉE DE BONNE RÉSOLUTION POUR LA NOUVELLE ANNÉE : PRENEZ SOIN DE VOS COLLABORATEURS !

Voici maintenant plus de six années que notre service existe et vole de collectivité en collectivité, apportant chaque jour ses conseils, ses recommandations, afin d'aider les décideurs publics à protéger les données de leurs administrés et de leurs agents.

Mais pas un jour depuis ne passe sans que l'on se retrouve face aux inquiétudes et aux angoisses de nos interlocuteurs quant aux changements qu'implique la mise en conformité au RGPD, ou encore face à la charge mentale qu'impose la transformation numérique de nos administrations et de nos services. Presque à chaque rendez-vous, elle est là, silencieuse et tapie dans l'ombre. Pourtant, la présence de l'anxiété qu'implique l'usage du numérique se fait ressentir, tel un écho invisible.

C'est pourquoi nous nous sommes interrogés sur nos moyens d'action envers cette crainte ainsi que sur son fondement. Nous avons alors découvert un monde dans lequel nous n'avions pas imaginé mettre le pied. En notre qualité de délégué à la protection des données, nous avons en effet nous même assez de choses à traiter, entre cybersécurité, durées de conservation des archives, information des usagers et autre licéité des traitements de données. Nous n'avions jamais pris le temps de nous interroger

sur la charge mentale qui pesait sur les agents de par l'utilisation qu'ils faisaient du numérique et l'anxiété qui grandissait depuis la prise de conscience des risques entourant les données sous leur responsabilité.

C'est donc dans le but de réparer cette injustice que nous avons aujourd'hui souhaité entamer une réflexion autour des risques psychosociaux liés à l'utilisation du numérique.

Une hyperconnexion à risque

Les risques psychosociaux, plus communément appelés par le signe « RPS », regroupent divers risques pouvant mener à un état de stress au travail qui peuvent affecter la santé mentale des agents. Si de nombreux facteurs peuvent favoriser leur apparition et leur développement, l'arrivée du numérique a créé de nouveaux défis en matière de RPS, malgré l'apport d'avantages indéniables.

Les technologies du numérique facilitent aujourd'hui une disponibilité constante, renforcée par l'introduction massive du télétravail depuis la pandémie de Covid-19, ce qui peut brouiller les frontières entre vie personnelle et vie professionnelle. Cela peut entraîner notamment un épuisement professionnel des agents qui se sentent parfois obligés de répondre aux communications professionnelles en dehors de leurs heures de travail, voir même de travailler au-delà du temps professionnel. Cette hyperconnexion peut être accrue par un sentiment de surveillance et de contrôle par

la technologie, que ce sentiment soit réel, notamment dans le cas de l'utilisation d'outils servant à la surveillance des agents, tel qu'un logiciel de gestion du temps permettant de savoir si et quand l'agent a pris son poste, y compris en télétravail, ou alors tout simplement imaginé par l'agent qui peut craindre qu'on ne le pense pas à son poste s'il ne travaille pas assez. L'usage du numérique peut alors venir augmenter la pression et l'anxiété liés à la performance, et nuire au passage au bien-être mental.

Il est donc essentiel de prendre le temps de réfléchir aux solutions qui pourraient être apportées à ces risques que l'on a tendance à ne pas voir, mais que l'on peut notamment ressentir lors, par exemple, d'un départ en vacances. En effet, rares sont les personnes à ne pas se reconnaître lorsque l'on pense aux bienfaits du départ en vacances, sans avoir à gérer le flux constant des mails, de la messagerie instantanée, des notifications ou des appels téléphoniques. Cette surcharge d'informations est devenue, hélas, si naturelle dans notre environnement professionnel que peu se rendent compte qu'elle est pourtant stressante et accablante.

Savoir raccrocher à temps

Face aux enjeux de cette connexion à outrance, il faut savoir poser des limites claires et accompagner les agents dans une démarche de déconnection. Le plus difficile est moins ici de recueillir l'aval des agents que d'arriver à trouver le temps pour réfléchir à des solutions opérationnelles pour limiter la connexion des agents. Mais c'est pourtant essentiel de savoir s'arrêter un temps, de se couper de ce flux terrible dans lequel on s'enfonce au quotidien, pour pouvoir prendre du temps pour soi et améliorer son quotidien au travail. Après tout, l'on passe la majorité de notre temps éveillé auprès de nos collaborateurs… Ce temps ne doit pas être vécu comme perdu, mais comme un investissement. Comme nous le disions plus haut, mettre un frein aux RPS permet de gagner en performances et en productivité, outre le fait de prendre soin de sa santé mentale. C'est donc un jeu gagnant-gagnant qui s'ouvre maintenant dès lors que l'on peut prendre ce temps.

A partir de là, une intense réflexion peut être menée sur les moyens de limiter les RPS de ses agents (et les siennes, par la même occasion). Cela peut passer par l'incitation des agents à déconnecter après les heures de travail, mais également à les encourager à prendre des pauses régulières. Sur ce dernier point, certains managers vont bondir sur leur siège en lisant ces lignes, mais les études ont clairement prouvé que l'augmentation du nombre de pauses, même de courte durée, permet au cerveau de se régénérer et de retrouver toute sa concentration, permettant ainsi aux agents de gagner en productivité. Philippe Zawieja, qui est psychosociologue, consultant, auteur et chercheur associé aux Universités de Paris, de Montréal, du Minho et de Florence, recommande ainsi, en plus de la pause déjeuner, deux pauses de 15 minutes réparties équitablement au cours de la journée.

D'autres méthodes préconisent une micro-pause de 5 minutes toutes les 90 minutes. Mais peu importe la méthode employée, l'essentiel reste de permettre à l'agent de retrouver ses forces mentales pour assurer ses missions avec l'efficacité qu'exige notre professionnalisme et le sens du service public inhérent à nos tâches.

C'est pourquoi il est également essentiel de savoir former les agents et de les accompagner dans un changement de rythme qui peut parfois être déroutant en leur faisant prendre conscience qu'une pause n'est pas forcément répréhensible, et que personne ne viendra leur reprocher de raccrocher leur attention le temps d'un café. Car c'est aussi là, le piège infernal des RPS : l'agent va parfois s'auto-convaincre que sa hiérarchie attend de lui un travail digne des mineurs du XIX^{ème} siècle avec la peur de se faire mal voir s'il s'arrête de travailler ou s'il ne

rend pas de bons résultats à temps. Cette crainte est par ailleurs renforcée avec le développement du télétravail, encore trop perçu dans la société comme un moyen de ne rien faire en restant chez soi avec la télévision à côté de l'ordinateur.

Une autre crainte, peut être plus légitime, est celle de la masse de travail toujours plus importante en collectivités. De plus en plus de normes, de dossiers, de compétences à gérer… Nos collectivités sont débordées, et avec elles les agents qui ont parfois peur de perdre du temps en prenant une pause qui pourrait pourtant leur être salvatrice. Là encore, savoir s'arrêter semble contre naturel, mais reste essentiel pour arriver à gagner en productivité. Cela passe tant par le repos du cerveau que par la possibilité de prendre du recul sur une organisation que l'on peut parfois améliorer pour gagner en efficacité.

Privilégier la convivialité

Mais la pause n'est pas la seule voie vers le bien être mental. D'autres éléments, parfois complémentaires des pauses, vont venir aider à lutter contre les RPS chez les agents en matière de numérique.

L'être humain est un animal grégaire. Comme le mouton ou les vaches. Cela signifie qu'il a besoin de vivre en société. Ainsi, même au travail, il a besoin de contacts humains et d'un support social. De ce fait, l'un des leviers à envisager pour un employeur serait de favoriser et promouvoir un environnement de travail qui encourage le soutien entre collègues, même à distance.

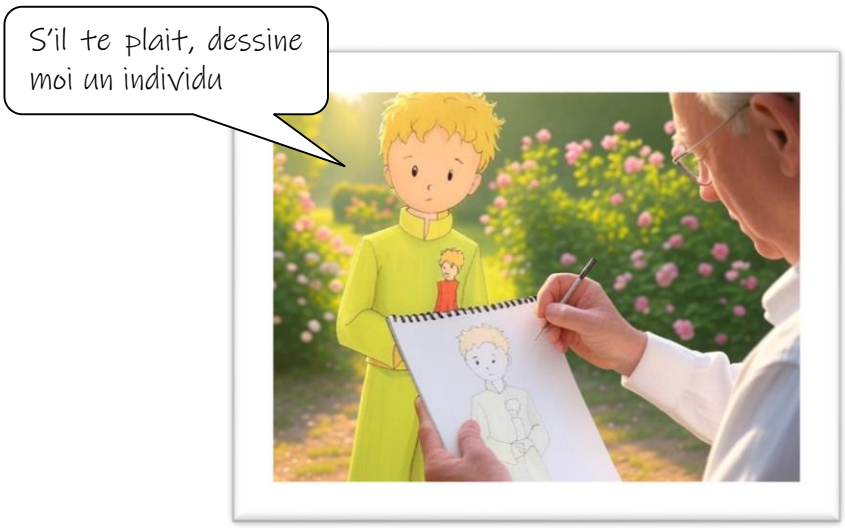
La réflexion sur la qualité de vie au travail vient donc en complément de ce besoin de prendre du recul et fait partie des tâches possibles pour un employeur qui arrivera à prendre le temps de reposer sa conscience.

Mais cela passe également par une réflexion globale sur l'organisation du travail, avec une répartition des tâches qui va inciter les collègues, surtout ceux en télétravail, à communiquer entre eux et à coopérer. Cela favorisera le sentiment d'appartenir à un collectif qui, même s'il reste ténu, aidera les agents à garder le moral et à se sentir soutenus face à une charge de travail parfois lourde.

Enfin, il est également essentiel pour les agents de se sentir soutenus par leur hiérarchie qui doit communiquer efficacement et faire sentir qu'elle garde confiance dans ses agents. Cela passe tant par de petites attentions, tel qu'un simple merci lorsqu'une tâche est terminée, que par de plus gros leviers tel que la prise en compte du travail accompli et de l'implication de l'agent dans son régime indemnitaire. Pour un agent, qui est un être humain avant tout, rien ne vaut plus que la reconnaissance de son employeur. Pour reprendre les mots de Napoléon I[er], « *un homme ne risque pas sa vie pour trois sous par jour ou pour une médaille. Il faut parler à son âme, la galvaniser* ».

Et le RGPD dans tout ça ?

L'arrivée du RGPD, si elle a été salvatrice pour nos données personnelles et notre vie privée, ne s'est pas faite sans dégâts sur la santé mentale des agents de nos collectivités. La prise de conscience de détenir une mine d'or concernant la vie privée de nos usagers et de nos agents a entrainé l'apparition d'une angoisse sourde qui a pu provoquer deux types de réactions. La plupart ont, pendant un temps, occulté le RGPD et les obligations qu'ils incombaient, tel le phénomène psychologique de l'évitement, qui consiste à éviter ce qui peut nous inquiéter. Mais d'autres ont immédiatement pris la pleine mesure de l'importance du sujet et de l'ampleur de la tâche à accomplir, venant ajouter une charge mentale à celle déjà présente du fait d'un travail acharné. Et avec l'augmentation frappante du nombre de cas de cyberattaques ces dernières



années à l'encontre des collectivité, les premiers ont fini par cesser l'évitement pour rejoindre les second en subissant à leur tour une charge mentale croissante, car doublée de l'inquiétude liée aux attaques.

Or, il reste du devoir de l'employeur de s'assurer du bien être physique et mental de ses agents. C'est même une obligation reconnue par le code du travail, dans l'une des rares parties directement applicables à la fonction publique. Il revient donc à l'employeur de chercher des solutions pour faire diminuer cette charge mentale.

Bien entendu, il s'agira de faire en sorte de respecter les mesures essentielles de sécurité recommandées tant par la CNIL que par l'ANSSI, l'agence nationale dédiée à la sécurité des systèmes d'information. Mais si ces deux organismes sont des experts en matière de sécurité, ils laissent le soin aux organismes d'appliquer ces mesures à leur manière. Et c'est bien là que le bât blesse souvent, car les mesures de sécurité deviennent vite un vrai casse-tête. Car si tous les agents peuvent arriver à comprendre qu'un mot de passe complexe et long est plus sécurisé qu'une suite de quatre chiffres, tous répondront unanimement qu'il est aujourd'hui devenu excessivement lourd à supporter de devoir retenir une multitude de mots de passe complexes qu'il faut en plus changer régulièrement, rendant impossible leur mémorisation.

Il reviendra donc aux employeurs de faire de même que pour tout risque psychosocial déjà vu auparavant : savoir prendre du temps pour réfléchir aux moyens de les atténuer, voire même de les contourner.

Dans le cas des mots de passe, l'une des solutions les plus simples revient à la mise en place d'outils tels que les gestionnaires de mots de passe. Certains sont même gratuits. Mais dans d'autres cas, la solution sera simplement organisationnelle. Car la cybersécurité, c'est avant tout de l'organisation. Comme le disait si bien Sun Tzu, « le vainqueur remporte la bataille avant de partir à la guerre. Le vaincu part à la guerre et rêve de triomphe ».

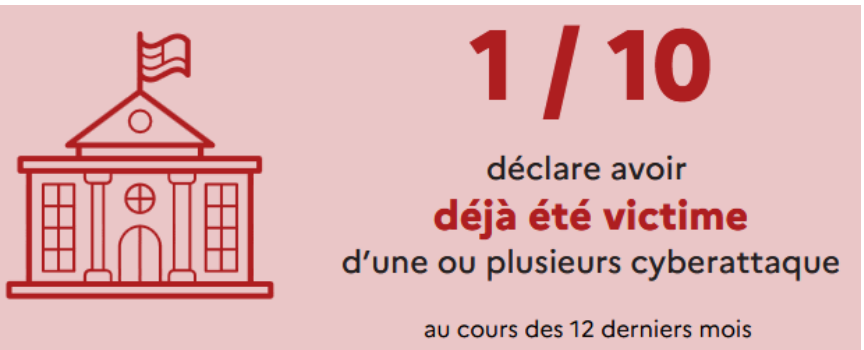
Ainsi, dans le cas d'un traitement de données consultable par les administrés, tel que les données du cadastre, il reviendra de mettre en place un simple registre où les administrés s'inscriront pour garder une trace des accès aux données. Cela permettra, entre autres, de décharger mentalement l'agent de ses potentielles craintes quant à un mauvais usage des données par la personne venue les consulter qui pourrait ensuite retomber sur la collectivité. Il en va de même pour la consultation de la liste électorale.

A chaque problème, une solution. La liste des RPS dans le cadre de la protection des données est telle que nous ne pourrions pas établir une liste exhaustive de solutions. Pour autant, afin de garantir le bien être des agents, il est essentiel de savoir prendre un temps pour réfléchir aux solutions les plus simples, les moins coûteuses et les plus efficaces. C'est aussi ça, le rôle d'un délégué à la protection des données : aider les décideurs à prendre les meilleures décisions, celles qui seront les plus bénéfiques aux agents et grâce auxquelles ces derniers auront à cœur de respecter les nouvelles règles qui vont maintenant leur incomber du fait de l'évolution de la réglementation.

Le rôle du délégué à la protection des données n'est pas qu'un rôle d'empêcheur de tourner en rond. C'est aussi un conseiller en organisation redoutable qui a pour tâche essentielle d'aider à la conduite du changement au sein de nos administrations. Car si le changement peut faire peur, celui-ci peut être facilité lorsqu'il est bien accompagné.

Assurer un soutien

Mais si l'accompagnement du changement est essentiel, il ne faut pas non plus négliger les effets de la survenance du risque. En effet, tous les agents des collectivités ayant subi une cyberattaque le diront : une cyberattaque est un traumatisme. L'agent se sent impuissant et atteint personnellement lorsque



Source : 3ème édition du baromètre de la maturité cyber des collectivités – cybermalveillance.gouv.fr

son outil de travail est rendu inopérant. Lorsque son ordinateur, sur lequel il passe une grande partie de sa journée et sur lequel il a engagé des efforts et une énergie incroyable, lui procurant parfois du stress et une charge mentale lourde, est tout d'un coup attaqué et voit ses données perdues, l'agent va ressentir une blessure profonde qu'il ne faut pas négliger.

Ainsi, en cas de cyberattaque, si l'urgence reste la reprise d'activité, il ne faut pas négliger l'impact psychologique qui accompagne hélas à chaque fois cet événement. Un autre accompagnement est alors nécessaire, et si le délégué à la protection des données est également là pour dédramatiser les choses et accompagner les agents en les déculpabilisant, en leur faisant comprendre que dans une telle situation, un tel cas, on est toujours une victime, même lorsqu'on a cliqué sur le mauvais lien, rien ne vaut l'accompagnement par un professionnel de la santé mentale. Il revient donc à l'employeur de savoir proposer un accompagnement par un psychologue du travail qui pourra alors aider les agents à franchir le cap de la perte de l'outil de travail. Car si une cyberattaque vient détruire le matériel, le véritable risque lors de sa survenance reste la perte du capital humain grâce auquel nos collectivités continuent de fonctionner chaque jour malgré les difficultés rencontrées.

Et c'est peut-être là, la chose essentielle à retenir aujourd'hui : dans nos collectivités, ce qui fait notre force, c'est avant tout la capacité de nos agents à répondre aux besoins des administrés. C'est pour cela que, dans notre métier, l'on parle véritablement de « ressources » humaines ■

Les bienfaits du rangement de bureau

Le cerveau répondant à de nombreux stimuli, un environnement de travail en désordre peut influencer de manière négative l'état d'esprit d'une personne en créant une sensation de surcharge mentale. Différentes études scientifiques tendent à prouver qu'un bureau propre et organisé améliore l'efficacité, via une augmentation de la concentration en réduisant les distractions, et le bien-être des agents.

Ces bienfaits s'expriment notamment par une réduction du stress, mais aussi une augmentation de la productivité dès lors que tout est à sa place et que l'agent peut retrouver facilement ce dont il a besoin. Le rangement du bureau provoque également un sentiment d'accomplissement et de satisfaction, boostant la motivation de l'agent qui peut ainsi se détendre, favorisant sa créativité.

Enfin, chose sans doute la plus importante, un espace de travail propre et organisé peut contribuer à une meilleure santé mentale de l'agent en créant un sentiment de contrôle et de maîtrise de son environnement. En ayant un bureau bien rangé, il est également plus facile de planifier et de gérer son temps efficacement, évitant les retards et les oublis.

Ainsi, voici quelques conseils pour ranger efficacement son bureau :

1 – **Triez** les documents et ne conservez que ceux qui sont nécessaires à votre travail (archivez les autres et détruisez les brouillons)

2 – **Rangez** les documents conservés dans des pochettes et autres classeurs. Ne laissez pas les documents être visibles par les personnes reçues en rendez-vous

3 – **Compilez** les rendez-vous et événements à venir mentionnés sur des post-it dans votre agenda (papier ou électronique)

4 – N'oubliez pas votre bureau informatique ! Rangez les fichiers dans des dossiers et sous-dossiers sur votre serveur

5 – N'hésitez pas à **personnaliser** votre environnement de travail avec des photos ou des plantes (dans les limites permises par le professionnalisme)

GOUVERNEMENT
Liberté
Égalité
Fraternité

17 CYBER
Mon assistance en ligne

Un service proposé par

POLICE NATIONALE
Gendarmerie nationale
CYBER MALVEILLANCE .GOUV.FR

LE RECENSEMENT DE POPULATION

Loi n°51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques

Loi n°2002-276 du 27 février 2002 relative à la démocratie de proximité : article 156

Décret n°2003-561 du 23 juin 2003 portant répartition des communes pour les besoins du recensement de la population

Qu'est-ce que c'est ?

Le recensement de la population est une collecte de données réalisée chaque année et concernant successivement tous les territoires communaux au cours d'une période de cinq ans. Cette enquête est obligatoire pour chaque collectivité et a lieu selon un rythme de :

- Tous les 5 ans pour les communes de moins de 10 000 habitants, par roulement (toutes les communes ne réalisent pas leur recensement la même année)
- Tous les ans pour les communes de plus de 10 000 habitants, mais sur un échantillonnage de population différent chaque année sur la base de 8% des adresses

Le recensement suit plusieurs objectifs dont certains sont essentiels pour les collectivités :

- **Connaitre la population de chaque commune** (et de ce fait, la population française), le nombre d'habitants ainsi que leurs caractéristiques (âge, profession, moyens de transport utilisé, conditions de logement, etc.)
- **Définir les moyens de fonctionnement des communes** en ajustant ainsi la dotation globale de fonctionnement, principale source de recettes des collectivités, à leur population
- **Définir les règles de fonctionnement des communes** au regard de leur population, et notamment le nombre d'élus au conseil municipal, la détermination du mode de scrutin, le nombre de pharmacies, la réglementation sur l'hébergement d'urgence, etc.
- **Aider à la prise de décisions**, tant au niveau national qu'au niveau local en permettant d'adapter les politiques publiques à la population vivant sur nos territoires

Ces données sont collectées par les collectivités, puis destinées **exclusivement** à l'INSEE (Institut national de la statistique et des études économiques).

La collecte des données

Si le recensement relève de la responsabilité de l'Etat, ce sont les communes qui préparent et réalisent la collecte via la désignation d'agents recenseurs.

Pour plus d'informations sur la désignation des agents recenseurs, retrouvez notre fiche pratique dédiée sur le site internet du CDG 30 ou en cliquant sur l'icône ci-contre :

La collecte commence toujours le 3ème jeudi de janvier et dure 4 semaines dans les communes de moins de 10 000 habitants et 5 semaines dans les communes de 10 000 habitants et plus. Elle se mène de deux manières :

- **Par internet :** C'est le mode de recensement par défaut. L'agent recenseur se présente chez la personne à recenser et lui remet une notice sur laquelle figurent leurs identifiants de connexion au site le-recensement-et-moi.fr
- **Par papier :** Pour les personnes ne pouvant pas répondre à l'enquête par internet, alors les agents recenseurs remettent aux habitants un questionnaire papier et conviennent d'un rendez-vous pour venir les récupérer.

Sont ainsi collectées les données suivantes :

Catégories de données	Justification de la collecte
• Bulletin individuel (imprimé n°3) : nom, prénom, adresse, sexe, date et lieu de naissance, nationalité, date d'arrivée en France (si né à l'étranger), situation scolaire, situation familiale, type de diplômes, situation professionnelle, nom de l'employeur, type d'activité, lieu de travail, mode de transport utilisé, type de contrat, signature • Feuille de logement (imprimé n°1) : adresse, type de logement, année de construction, présence d'un ascenseur, caractéristiques du logement, année d'emménagement, nombre de voitures et de places de stationnement, nom, prénom, sexe, année de naissance, conjoint, parents, garde des enfants, enfants, autres personnes hébergées	Collecte obligatoire et nécessaire au respect d'une obligation légale *article 6, 1, c du RGPD* *Article 3 de la loi n°51-711 du 7 juin 1951* La finalité déterminée est la réalisation d'analyses statistiques pour le compte de l'INSEE Les données d'identification des habitants suivent une finalité différente *(voir point dédié en page suivante)*

Tout autre collecte, notamment via des formulaires créés par la commune, **est interdite** : seuls les documents fournis par l'INSEE doivent être utilisés.

Précisions sur la collecte de l'identité des personnes

Si des données permettant d'identifier les personnes recensées sont transmises à l'INSEE, ce dernier exploitera malgré tout les questionnaires de façon **anonyme**. Aucun contrôle administratif ou fiscal ne peut ainsi avoir lieu suite à une enquête de recensement.

Les noms et adresses des habitants ne sont ainsi récoltées que dans le but de s'assurer que l'administré concerné ne sera pas compté plusieurs fois. Ces données ne seront toutefois pas enregistrées dans une quelconque base de données.

L'information des personnes

Les personnes répondant à l'enquête **doivent être informées** lors de la collecte de la raison de celle-ci et de l'utilisation qui sera faite de leurs données, notamment de leur transmission auprès de l'INSEE. Une mention d'information peut être ajoutée aux documents remis par les agents recenseurs. Cette information peut également être faite en amont par un courrier explicatif.

L'INSEE a mis en place une mention d'information que vous pouvez ainsi reprendre :

« Vu l'avis favorable du Conseil national de l'information statistique, cette enquête est reconnue d'intérêt général et de qualité statistique, en application de la loi n° 51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques. Elle a obtenu le visa n°2025A001EC du Ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique valable pour l'année 2025.

Cette enquête est obligatoire. En cas de défaut de réponse, vous pouvez être l'objet de l'amende prévue à l'article 131-13 du code pénal.

Les réponses à ce questionnaire sont protégées par le secret statistique et destinées à l'INSEE. Leur usage et leur accès sont strictement contrôlés et limités à l'élaboration de statistiques ou à des travaux de recherche.

Le règlement général 2016/679 du 27 avril 2016 sur la protection des données (RGPD) ainsi que la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'appliquent à la présente enquête.

L'Insee est seul destinataire des données identifiantes (nom et coordonnées), ainsi que le prestataire, habilité par le Comité du secret de la statistique publique, et les Archives de France, conformément aux dispositions de l'article L. 212-4 du code du patrimoine. Les données d'identification seront conservées par le service producteur jusqu'au plus tard le 31 décembre 2026.

Les personnes enquêtées peuvent exercer un droit d'accès, de rectification ou de limitation de traitement pour les données les concernant pendant la période de conservation des données d'identification. Ces droits peuvent être exercés auprès de la direction régionale de l'INSEE dont dépend la personne concernée et dont l'adresse figure sur le site www.insee.fr. Le délégué à la protection des données pour cette opération est le Délégué à la protection des données des ministères économiques et financiers que vous pouvez contacter à l'adresse : Délégation aux Systèmes d'Information – 139, rue de Bercy Télédoc 322 – 75572 PARIS Cedex 12. Vous pouvez également introduire une réclamation auprès de la Cnil. »

La transmission des données

Seul l'INSEE peut être destinataire des données ! Une fois le recensement terminé, toutes les informations devront ainsi être transmises dans un délai de 10 jours ouvrables à leurs services, et aucun document ne devra être conservé par la commune.

L'INSEE ne peut divulguer les données récoltées et ne peut les transmettre à aucun tiers. Les enquêtes de recensement sont couvertes par les délais prévus par le code du patrimoine concernant l'accès aux archives publiques et ne pourront êtres rendues accessibles qu'après un délai de 75 ans (ou de 25 ans après le décès de l'administré).

Articles L.213-2 et L.213-3 du code du patrimoine

Article 6 de la loi n°51-711 du 7 juin 1951

La conservation des données

Type de document	Durée d'utilité administrative*	Sort final
Bulletin individuel et feuille de logement	Pas de conservation	Transmission à l'INSEE
Tableaux récapitulatifs	5 ans	Conservation définitive
Dossier de mise en œuvre (dossier remis aux agents recenseurs)	5 ans	Destruction après autorisation des archives départementales
Dossier d'organisation	5 ans	Destruction après autorisation des archives départementales

** La durée d'utilité administrative (DUA) constitue la durée pendant laquelle la collectivité est tenue de conserver le document et peut être amenée à le présenter aux autorités compétentes. Il s'agit, en quelques sortes, de la durée de conservation « minimale ».*

Petite précision au sujet des agents recenseurs

Il peut arriver que certains agents recenseurs ne soient pas des agents de la Mairie. Si les agents publics sont tous soumis à un devoir de secret professionnel reconnu par l'article L.121-6 du code général de la fonction publique, les agents vacataires et les autres personnes non soumises au statut des agents publics amenées à exercer les fonctions d'agents recenseurs **restent soumis à un devoir de secret professionnel**.

Article 6 de la loi n°51-711 du 7 juin 1951

Il peut ainsi être utile de sensibiliser ces personnes en leur rappelant cette obligation, notamment aux moyens d'une réunion préalable au recensement leur présentant leur mission et les conditions d'exercice de ces fonctions.

Horoscope 2025

Découvrez ce que vous réservent les cieux pour cette nouvelle année 2025. Nuages, horizon bleu et ensoleillé, nuit étoilée ou coup de foudre… Votre signe vous dit tout !

BELIER

21 mars – 19 avril

2025 vous réserve des nuits blanches à protéger des montagnes de données comme un super-héros masqué. Astuce : gardez toujours du café à portée de main et une playlist épique pour motiver votre esprit combatif !

TAUREAU

20 avril – 20 mai

Cette année, les Taureaux seront les champions des formulaires à remplir et à classer. Gardez votre calme légendaire et imaginez que chaque clic de souris vous rapproche du nirvana administratif… ou du gâteau de la pause café.

GEMEAUX

21 mai – 20 juin

Pour les Gémeaux, 2025 sera une aventure où vous découvrirez de nouvelles technologies comme si c'étaient des gadgets de James Bond. Attention aux miroirs espions et aux clés USB dissimulées : vos collègues ne sont jamais bien loin.

CANCER

21 juin – 22 juillet

Les Cancers auront la mission d'éduquer leurs collègues sur la protection des données. Préparez-vous à devenir le Yoda des fichiers Excel et des mots de passe : « Maître des données tu deviendras. »

LION

23 juillet – 22 août

Les Lions seront les leaders intrépides de la cybersécurité en 2025. Prêts à rugir et à bondir sur chaque vulnérabilité ? N'oubliez pas que même le plus courageux des félins a besoin de siestes réparatrices.

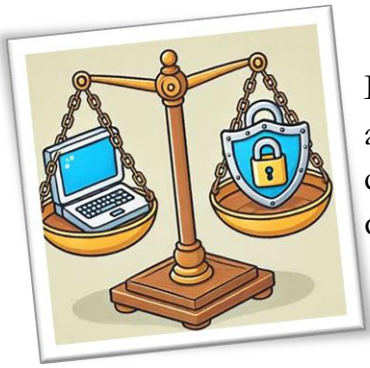
VIERGE

23 août – 22 septembre

Cette année, les Vierges joueront les détectives minutieux, traquant les moindres erreurs de données. Prenez une loupe et un trench-coat et plongez dans l'aventure, Sherlock ! Mais attention, Watson est peut-être votre imprimante qui ne fonctionne jamais.

BALANCE

23 septembre – 22 octobre



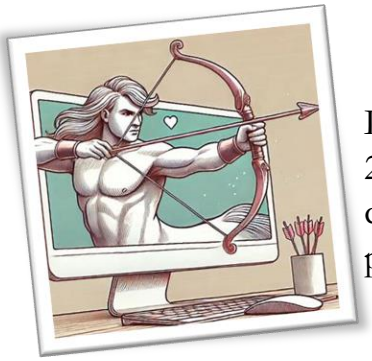
Les Balances devront trouver l'équilibre parfait entre sécurité et accessibilité des données. Un numéro d'équilibriste digne du Cirque du Soleil, avec des touches de clavier en guise de trapèze. Bonne chance et ne regardez pas en bas !

SCORPION

23 octobre – 21 novembre

Les Scorpions joueront aux vigiles numériques cette année. Avec leur instinct de détective, ils découvriront des failles avant même qu'elles n'existent. Conseil : évitez les paranoïas et les chapeaux en aluminium.

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



SAGITTAIRE

22 novembre – 21 décembre

Les Sagittaires exploreront de nouveaux horizons numériques en 2025. Préparez-vous à découvrir des terres inconnues de la cybersécurité, tel un Indiana Jones du digital. Mais rappelez-vous, pas de fouet, juste une souris !

CAPRICORNE

22 décembre – 19 janvier

Les Capricornes planifieront des stratégies infaillibles pour la protection des données. Vous serez les génies du rétroplanning et des plans sur Excel. Votre mantra : « Un plan bien conçu est à moitié exécuté. » Allez, courage, l'Excel est votre ami !

VERSEAU

20 janvier – 18 février

Les Verseaux seront les caméléons de la cybersécurité, s'adaptant à tous les changements. Avec leur esprit innovant, ils feront face à chaque défi comme des super-héros geek. Capacité spéciale : modifier un mot de passe avant même qu'il soit piraté.

POISSONS

19 février – 20 mars

Les Poissons créeront des environnements sécurisés et chaleureux pour les données. Imaginez des bulles protectrices et des mots de passe doux comme des oreillers moelleux. Vos données se sentiront comme dans un spa numérique.

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

Adieu les courriels malveillants, je passe par voie aérienne.

FACE AUX RISQUES CYBER VOUS N'ÊTES PAS SEUL.

De vraies solutions existent.

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