CYBERACTU'

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

Juillet 2023

Protéger ses données pour zéro euro !

Dossier page 10

Et aussi

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

SERVICE PROTECTION DES DONNÉES · CENTRE DE GESTION DU GARD ·

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

CENTRE DE GESTION
DU GARD

Contactez-nous

04 66 38 86 86
cdg30@cdg30.fr

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous

CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

SOMMAIRE

ÉDITO

Sujet encore peu évoqué jusqu'à il y a encore quelques années, la protection des données est devenue un incontournable de la vie de nos collectivités et établissements publics depuis l'entrée en vigueur du RGPD en 2018, puis avec l'explosion des atteintes aux données suite à la crise sanitaire de 2020.

Au sein de nos collectivités, ce sujet inquiète. Il fait peur de par son apparente technicité.

Mais si le sujet n'était pas si complexe qu'attendu ? Et s'il était possible de se protéger simplement, voire même gratuitement ?

C'est pour tenter de répondre à cette question que notre équipe vous propose ce premier numéro qui, on l'espère, vous permettra d'avancer sur le chemin de la conformité.

Pierre BONANNI – Ana VEGA

Contacts

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

SERVICE PROTECTION DES DONNÉES · CENTRE DE GESTION DU GARD

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

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

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

Rendez-vous sur cybermalveillance.gouv.fr

LES TEXTES RÉGLEMENTAIRES

Décret n° 2023-188 du 17 mars 2023 relatif à la création d'un traitement de données à caractère personnel visant à faciliter le partage de données entre les acteurs de l'insertion sociale et professionnelle et portant diverses dispositions en matière d'insertion

Ce décret crée un traitement de données à caractère personnel, dénommé « *Parcours insertion emploi* », permettant le partage de données entre les acteurs de l'insertion sociale et professionnelle.

Il définit les finalités du traitement, les catégories et la durée de conservation des données enregistrées, ainsi que les modalités de sa mise en œuvre. Il précise ainsi les modalités d'accès, d'alimentation et de transmission des données du traitement. Il détermine en outre les conditions spécifiques du traitement du numéro d'inscription des personnes au répertoire national d'identification des personnes physiques dans le cadre du partage de données entre les acteurs de l'insertion sociale et professionnelle et de l'accompagnement personnalisé des personnes en difficultés d'insertion sociale et professionnelle.

Il autorise l'import automatisé par Pôle emploi des données à caractère personnel de données de la Caisse nationale d'allocations familiales. Il transfère également la responsabilité du traitement du téléservice permettant d'accomplir les démarches relatives au parcours d'insertion par l'activité économique au groupement d'intérêt public « *Plateforme de l'inclusion* ».

Enfin, le texte prolonge de deux ans l'expérimentation de l'élargissement des formes d'insertion par l'activité économique au travail indépendant.

Décret n° 2023-361 du 11 mai 2023 relatif aux échanges d'informations et de données entre administrations dans le cadre de démarches administratives

Ce décret organise les échanges d'informations et de données entre administrations quand celles-ci sont nécessaires pour traiter les déclarations ou les demandes présentées par le public, pour informer les personnes sur leurs droits au bénéfice éventuel d'une prestation ou d'un avantage et pour attribuer, le cas échéant, lesdits prestations ou avantages.

Décret n° 2023-526 du 29 juin 2023 portant application de l'article L. 241-3 du code de la sécurité intérieure et relatif à la mise en œuvre de traitements de données à caractère personnel provenant des caméras individuelles des sapeurs-pompiers et des marins-pompiers

Ce décret détermine les modalités d'autorisation par l'autorité préfectorale de l'emploi des caméras individuelles par les sapeurs-pompiers et marins-pompiers des services d'incendie et de secours. Il autorise la mise en œuvre des traitements de données à caractère personnel issues des enregistrements audiovisuels et notamment leurs finalités, les données enregistrées, les modalités et la durée de leur conservation, les conditions d'accès aux enregistrements ainsi que les droits des personnes concernées.

Les décisions des autorités chargées de la protection des données

02 novembre 2022 : Pologne – 1 700 €

Le Maire de Dobrzyniewo Duże (Pologne) s'est vu infliger une amende pour ne pas avoir pris les **mesures organisationnelles** nécessaires pour protéger les données de ses administrés.

En l'espèce, les agents de la municipalité n'avaient pas reçu pour consigne de quelconque interdiction d'emporter les ordinateurs professionnels à leur domicile. Or, l'un des agents ayant emporté son ordinateur s'est vu dérober son matériel lors d'un cambriolage ayant conduit à la perte de données à caractère personnel.

17 janvier 2023 : Suède – 17 900 €

La Région de Dalarna (Suède) s'est vue infliger une lourde sanction financière en raison d'un manquement à son **devoir de confidentialité** après avoir envoyé à des patients leur convocation à des rendez-vous médicaux par courrier sous enveloppes à fenêtres par lesquelles étaient visibles des données de santé (données sensibles)

23 mars 2023 : Italie – 30 000 €

La commune de Bolzano (Italie) a subi une lourde sanction pour ne pas avoir pris les **mesures techniques nécessaires** pour protéger les données personnelles traitées par ses services suite à une violation de données déclarée après un accès non autorisé à des données via une faille de sécurité exploitable par une adresse URL du site internet communal.

13 avril 2023 : Italie – 3 000 €

La commune de Cogollo del Cengio (Italie) a écopé d'une amende de 3 000 euros pour avoir manqué à son **devoir de minimisation des données** en publiant sur son site internet des données non nécessaires au respect de la finalité d'un traitement de données concernant son personnel.

En l'espèce, et en souhaitant respecter son obligation de publicité d'actes administratifs, la commune a publié certains documents en omettant d'anonymiser les données non nécessaires au respect de cette obligation.

26 avril 2023 : Suède – 17 600 €

La Région de Scanie (Suède) s'est vue infliger une lourde amende de 17 600 euros après que l'un de ses agents ait perdu une clé USB non chiffrée contenant des données personnelles sensibles portant sur la santé des administrés.

L'autorité suédoise de protection des données personnelles a ainsi estimée qu'il s'agissait d'un manquement aux obligations de la Région d'avoir pris les **mesures organisationnelles** nécessaires pour protéger les données de ses administrés.

27 avril 2023 : Italie – 176 000 €

La Ville de Rome s'est vue sanctionner très lourdement pour ne pas avoir mis en place les **procédures organisationnelles** garantissant la confidentialité des données dans le traitement réalisé dans le cadre de la gestion des cimetières communaux.

En l'espèce, la commune, qui est en charge de l'inhumation des fœtus décédés suite à un avortement, apposait sur les corps une étiquette mentionnant l'identité des femmes ayant choisi de réaliser un avortement. En a résulté une violation de données ayant conduit à l'identification de ces femmes par des personnes non habilitées à accéder à ces données.

05 MAI 2023 : POLOGNE – 2 200 €

Une commune de Pologne a été sanctionnée, elle aussi, pour ne pas avoir pris les **mesures organisationnelles** nécessaires.

La commune avait omis d'interdire à ses agents d'effectuer des copies de documents vers un support amovible (clé USB). Or, l'un des agents a effectué une copie de données sensibles vers un tel support, lequel a ensuite été perdu.

En outre, la commune a également été sanctionnée pour ne pas avoir réalisé l'analyse d'impact sur la vie privée obligatoire relative à ce traitement, laquelle aurait pu permettre d'anticiper les manquements sanctionnés.

16 MAI 2023 : POLOGNE – 6 700 €

Une commune polonaise a subi une double peine pour ne pas avoir mis en œuvre les **mesures techniques** nécessaires à la protection des données traitées par ses services.

En effet, suite à l'attaque de son système d'information par un rançongiciel ayant chiffré ses données, la commune s'est également rendue compte avec horreur que ses sauvegardes, pourtant existantes, étaient défectueuses. La commune a donc été sanctionnée pour ne pas avoir, en plus de ne pas avoir pris les mesures nécessaires pour se protéger d'une telle attaque, mis en œuvre des **tests réguliers des mesures appliquées par ses services**.

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Mairie d'Egreville
03 mai 2023

Mairie de Marcoussis
03 mai 2023

Mairie de Saint-Martin-lez-Tatinghem
21 juin 2023

Conseil départemental des Côtes d'Armor
13 mai 2023

Mairie de Mandeure
26 mai 2023

Mairie de Juziers
03 mai 2023

Conseil départemental de Saône-et-Loire
17 avril 2023

Mairie de Bry-sur-Marne
03 mai 2023

Mairie de Bouchemaine
17 juin 2023

SM d'Energies de l'Ariège
25 mai 2023

Mairie de Cerisay
08 juin 2023

** Sur les trois derniers mois*

PROTÉGER SES DONNÉES POUR ZÉRO EURO

Le soleil n'était pas près de se lever, en ce lundi matin pluvieux. Et pourtant, Marie-Amélie, secrétaire d'une petite Mairie d'un peu moins de 300 habitants, était déjà affairée à chercher les clefs de son bureau dans son sac, tenant difficilement son parapluie qui vacillait avec le vent. Ce jour-là, elle avait fort à faire ! Plusieurs dossiers de demandes d'autorisations d'urbanisme trainaient sur son bureau qu'elle n'avait pas eu le temps de ranger, et le retard accumulé la semaine précédente en préparant le budget n'arrangeait rien. Elle s'était en outre engagée à enfin rédiger les derniers arrêtés d'avancement des deux agents techniques de la commune, qui étaient passés la voir une bonne demi-douzaine de fois ces dernières semaines. Enfin, et comme si le destin avait fait d'elle son dernier jouet, le vieil Edmond, personnalité très connue dans le petit village dans lequel il avait vécu toute sa vie, venait de passer de vie à trépas au cours du week-end. Si la tristesse de l'événement l'avait, bien entendu, saisie comme tous les habitants, un petit pincement supplémentaire lui avait fait vibrer la poitrine lorsqu'elle avait réalisée qu'elle devrait, en plus de tout son travail, rédiger l'acte de décès.

Mais le pire, c'était ce rendez-vous pris dans la matinée… Oh, elle s'en voulait d'avoir dit oui, tant la masse de travail s'était accumulée dernièrement. Mais il était désormais trop tard pour reculer. Elle devrait recevoir cette personne qui se faisait appeler le « délégué à la protection des données ». Quel titre ! Encore un type qui va lui parler d'informatique, sujet pour lequel elle n'avait aucune appétence, et duquel elle ne connaissait que le bouton par lequel on allumait et éteignait cette satanée machine qui encombrait son bureau.

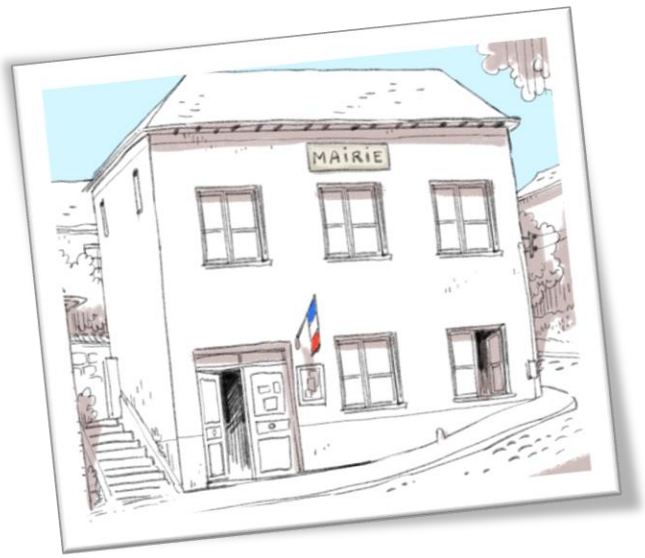


Image issue de : cybermalveillance.gouv.fr

Elle avait pourtant essayé, pendant quelques minutes, de comprendre un peu mieux le sujet pour lequel elle avait accepté ce rendez-vous. Mais à la lecture de termes barbares, tels que « *privacy by design* », de « cybersécurité » ou encore de « traitements de données », elle avait abandonné et préférait laisser ça à des informaticiens, ces gens étranges qui parlaient un dialecte qu'elle ne comprenait pas. Elle espérait simplement que cette personne n'allait pas lui prendre trop de son temps pour ces « sottises » trop compliquées, et sans doute trop chères, par-dessus le marché !

Si Marie-Amélie est un personnage de fiction, inventé par notre service, toute ressemblance avec une situation réelle n'est pas fortuite et est parfaitement volontaire. Le sujet de la protection des données souffre aujourd'hui d'une double méprise : trop pensent encore qu'il s'agit d'un **« truc d'informaticiens »**, et trop pensent encore que ce sujet **n'est pas une priorité pour nos collectivités**.

Car si les termes employés, tous très marqués par une connotation informatique, laissent à penser à un domaine lié au numérique, les multiples exemples de violations de données et de sanctions infligées par la CNIL et ses homologues européens démontrent néanmoins que la protection des données reste avant tout rattachée au monde de la sécurité.

Les apparences sont parfois trompeuses

Retournons dans la petite Mairie de Marie-Amélie : après un rapide café, la secrétaire prend son poste. Au bout de quelques minutes seulement, le téléphone sonne. Au bout du fil, une jeune demoiselle, à la voix pleine d'assurance, qui se présente comme inspectrice de la caisse des allocations familiales. Celle-ci lui demande alors de nombreuses informations sur l'un de ses deux agents techniques. Pensant bien faire, et souhaitant se débarrasser rapidement de cette contrainte supplémentaire, Marie-Amélie lui confie alors toutes les informations demandées.

Sans le savoir, elle venait de permettre à cette personne, dont elle n'avait pas douté de la sincérité, de commettre une grave usurpation d'identité.

Cet exemple tout simple, arrivé Ô combien de fois dans nos collectivités, nous montre qu'une violation de données peut arriver y compris sans le recours à l'informatique.

Qu'aurait-dû faire Marie-Amélie ? Ne pas répondre ? Mais si l'appel avait été sérieux ?

Comme dans de nombreuses situations, la protection des données résulte **avant tout de l'organisation**. La collectivité aurait pu (et aurait dû) se doter d'une procédure à suivre, d'une sorte de « mode d'emploi », pour répondre aux demandes d'informations confidentielles. Cette procédure aurait ainsi pu prévoir que Marie-Amélie s'assure de l'identité de son interlocutrice par des moyens prédéterminés, tels que l'envoi d'un mail de confirmation, avant de répondre à la demande.

Si un lien évident peut être fait avec le monde de l'informatique, il s'agira avant tout ici **d'encadrer les pratiques** des agents, des élus et des usagers afin **d'anticiper et de prévenir les risques**. Dans les faits, le volet informatique ne vient essentiellement que dans une logique de réparation si le risque venait à se produire.

« *ROUTINE N'EST PAS ORGANISATION, PAS PLUS QUE PARALYSIE N'EST ORDRE* »

Arthur HELPS

Ainsi, la voie la plus directe, la plus simple – et la moins chère – pour protéger les données que l'on a sous sa responsabilité est encore **de s'organiser** pour prévenir les incidents. Mais alors, comment faire ? Quels sont les leviers pour mieux organiser ses méthodes, ses procédures et s'adapter aux règles de la protection des données ?

La première règle, et la plus importante, sera d'adopter une **réglementation interne efficace et contraignante**. Bien que ni le code général de la fonction publique, ni le code général des collectivités territoriales ne le prévoient, il est fortement recommandé d'adopter un règlement intérieur, qui encadrera la vie de la collectivité sur tous les domaines, dont celui de la protection des données.

Comme l'a rappelé une fois encore la CNIL lors de la mise à jour de son guide pratique relatif à la protection des données en mai 2023, l'encadrement des processus internes est un incontournable de la protection des données. L'autorité recommande ainsi de rédiger cette réglementation tout en lui donnant un caractère contraignant, imposant aux agents d'en suivre les règles sous peine de sanctions.

Si le contenu de ce règlement est à adapter au fonctionnement de chaque entité, la CNIL recommande néanmoins certains éléments.

Ainsi, ce règlement devrait comporter au moins les éléments suivants :

- Le rappel des règles de protection des données et les sanctions encourues en cas de non-respect de celles-ci
- Le champ d'application du règlement, ce qui inclut entre autres (liste non-exhaustive) :
    - Les modalités d'intervention des équipes chargées de la gestion des ressources informatiques de la collectivité (qui appeler, comment les contacter, dans quel cas, etc.)
    - Les moyens d'authentification utilisés et la politique de mots de passe que l'agent devra respecter (nombre de caractères, complexité, etc.)
    - L'obligation de signaler toute violation (ou tentative de violation) de données, toute perte ou vol de matériel ou tout dysfonctionnement (qui prévenir, dans quel cas et comment)
    - L'interdiction de partager ses identifiants et ses mots de passe
    - Le verrouillage de l'ordinateur dès lors que l'agent quitte son poste de travail
- Les modalités d'utilisation des moyens informatiques et de télécommunication mis à disposition (ordinateur, smartphone professionnel, messagerie électronique, etc.)
- Les conditions d'administration du système d'information
- Les responsabilités et sanctions encourues en cas de non-respect du règlement

Oui, ça fait beaucoup de choses à prévoir !

Afin de pouvoir prévoir tous les cas de figures, et d'adapter cette réglementation interne à tous les agents et aux spécificités de leurs métiers, il est recommandé d'en établir le contenu collégialement en les associant via la mise en place de groupes de travail.

De plus, il est essentiel de conserver à l'esprit qu'une telle démarche restera soumise, conformément aux règles statutaires de la fonction publique, à la consultation préalable du comité social territorial, organe du dialogue social destiné à connaître de tout projet concernant les règles collectives de travail.

Alors, certes, une telle démarche de révision de ses procédures organisationnelles est longue et fastidieuse. Mais elle n'en reste pas moins essentielle, tant la prévention des risques est importante, y compris lorsque le risque porte sur les données personnelles.

Destinée à empêcher la survenance des risques, la démarche organisationnelle constitue à elle seule la très large majorité de la mise en conformité à la réglementation sur la protection des données. La CNIL elle-même ne demande rien d'autre que de traiter les données avec méthode et organisation afin que celles-ci soient protégées contre tout accès illégitime ou frauduleux.

Et surtout, cette démarche a un avantage non négligeable vis-à-vis de la survenance du risque : **elle est gratuite !**

La minute détente

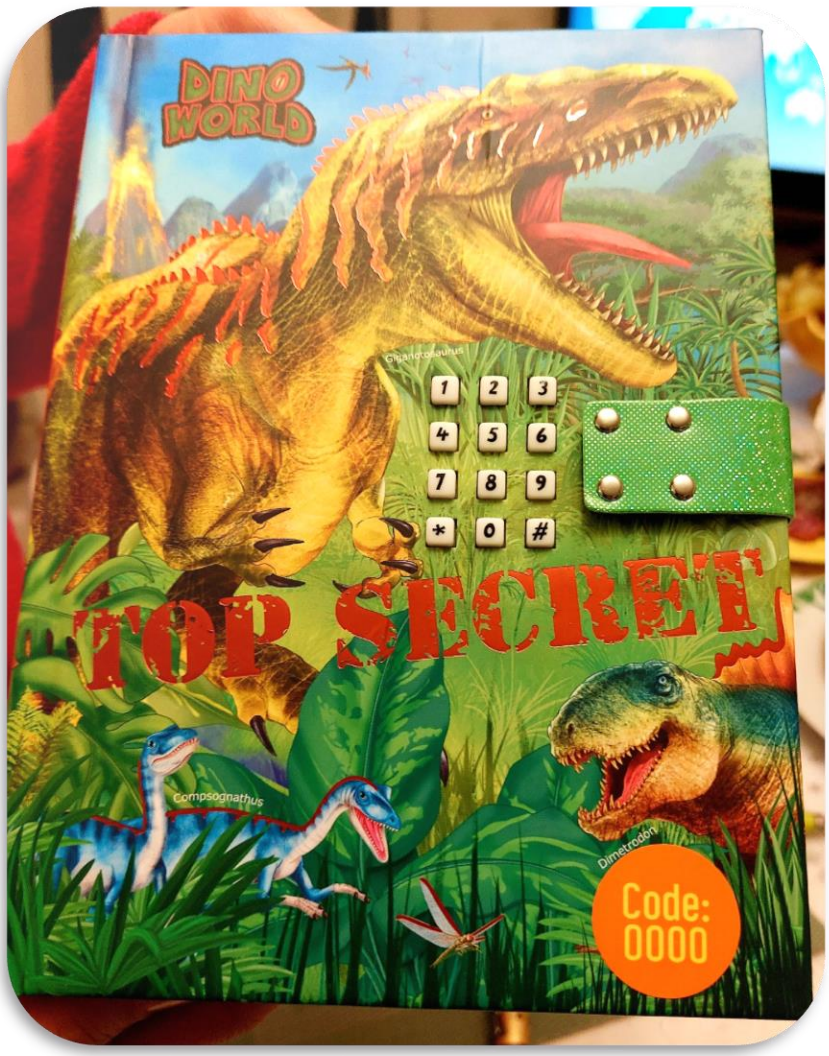
Horizontal	Vertical
1. Son orientation est considérée comme une donnée sensible	A. C'est l'un des droits des personnes concernées par les traitements de données et c'est une action réalisée sur les photos de son ex
2. Ce que l'on attend tant de son responsable de traitement que de son conjoint / sa compagne	B. Fait pour un responsable de traitement de ne récolter que les données nécessaires, ou fait pour votre partenaire de dédramatiser son erreur
3. Utile à la fois contre les MST et les cyber-attaques	C. Petite pâtisserie offerte lors d'un premier rendez-vous également synonyme de cadeau (souvent non consenti) déposé sur votre ordinateur
4. Première donnée personnelle recueillie avant un premier rendez-vous Tinder	D. Obligatoire dans toute relation sentimentale et souvent nécessaire au recueil des données
5. Peut servir tant à envoyer des mots doux qu'à désigner son délégué à la protection des données	E. Peut être spécial dans un mot-de-passe et mauvais chez sa belle-mère
6. Attitude attendue tant de la part du responsable de traitement que du bon père / de la bonne mère de famille	
7. Action servant à mesurer l'impact sur la vie privée d'un traitement de données, ou à rechercher la culpabilité de son partenaire	

Solution en dernière page

Le bon geste

Adopter des mots de passe forts

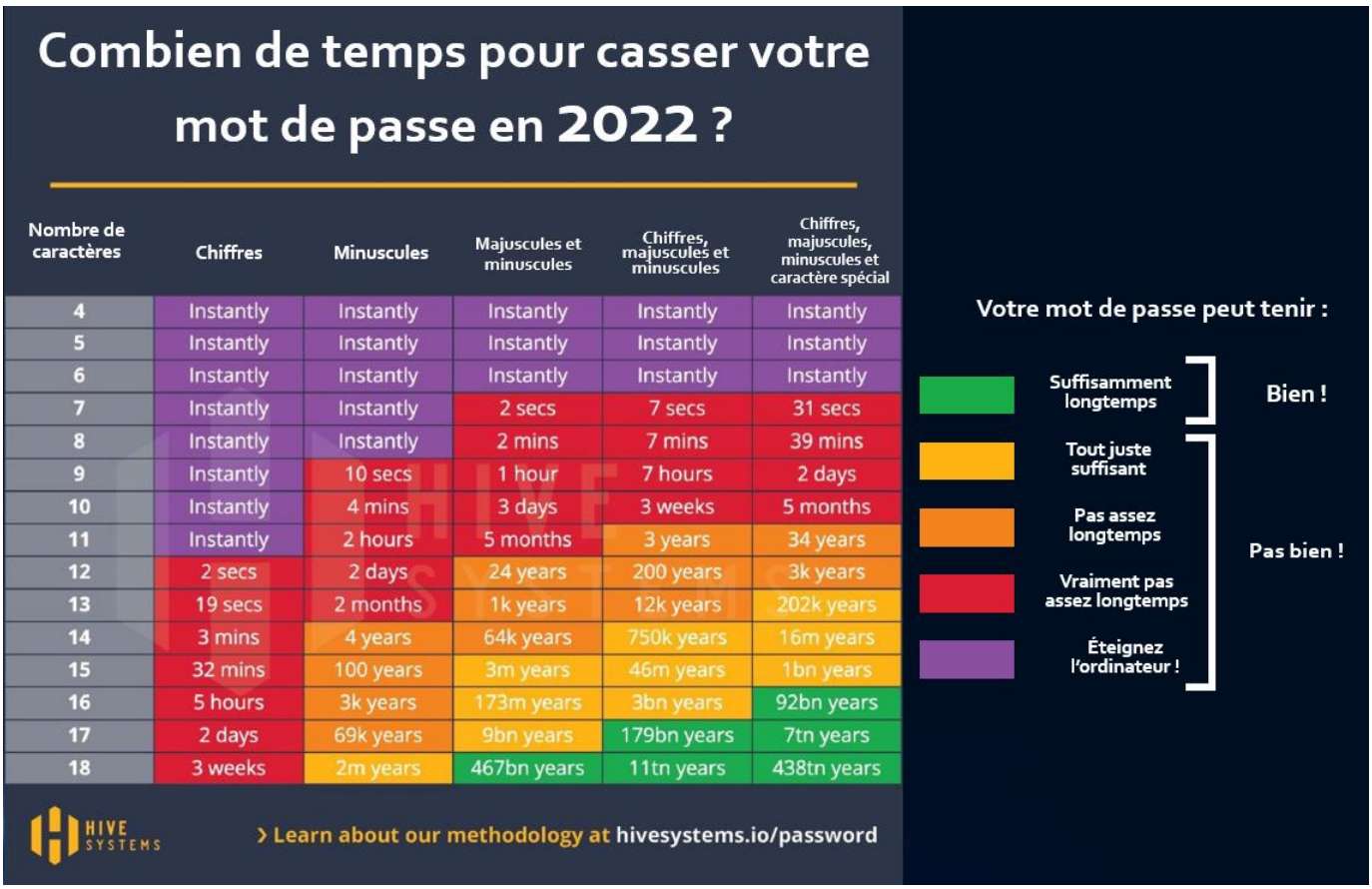
Ce livre et un grand nombre d'ordinateurs partagent un point commun. Saurez-vous l'identifier ?



La recommandation du délégué à la protection des données

- Utiliser des mots de passe **différents pour chaque usage**
  - *Le risque étant que le pirate ait accès à tous les comptes de l'utilisateur en dérobant son mot de passe unique*
- Utiliser un mot de passe **personnel**
  - *Le mot de passe ne doit pas être facile à deviner*
  - *Il doit de préférence faire référence à quelque chose d'intime et de connu du seul utilisateur*
- Utiliser un mot de passe **complexe**

Mot de passe de 12 caractères	Mot de passe de 14 caractères
• Un chiffre • Une lettre majuscule • Une lettre minuscule • Un caractère spécial	• Un chiffre • Une lettre majuscule • Une lettre minuscule



- Et bien sur, **ne jamais le noter nulle part !**

La solution de la minute détente

							C					
							O					
							N					
							S					
				S	E	X	U	E	L	L	E	
								N				
						L	E	T	T	R	E	
C								E				
A								M				
R				M								
A				I								
C		S		T	R	A	N	S	P	A	R	E	N	C	E
T		U					I							N
E		P					M							T
R	E	S	P	O	N	S	A	B	I	L	I	T	E		
E			R					S							
			E					A				C			
			S		P	R	O	T	E	C	T	I	O	N	
			S					I				O			
			I					O				K			
			O					N				I			
P	R	E	N	O	M							E	N	Q	U	E	T	E
												S						

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

QUE FAIRE EN CAS DE CYBERATTAQUE ?
(élus/dirigeants de collectivités)

1 PREMIERS RÉFLEXES

- ÉLU — ALERTEZ IMMÉDIATEMENT VOTRE SUPPORT INFORMATIQUE
- TECHNICIEN — ISOLEZ LES SYSTÈMES ATTAQUÉS
- ÉLU — CONSTITUEZ UNE ÉQUIPE DE GESTION DE CRISE
- TECHNICIEN — TENEZ UN REGISTRE DES ÉVÉNEMENTS
- ÉLU — PRÉSERVEZ LES PREUVES DE L'ATTAQUE

2 PILOTER LA CRISE

- TECHNICIEN — IDENTIFIEZ L'ORIGINE DE L'ATTAQUE ET SON ÉTENDUE
- ÉLU — DÉPOSEZ PLAINTE
- ÉLU — NOTIFIEZ L'INCIDENT À LA CNIL
- TECHNICIEN — METTEZ EN PLACE DES SOLUTIONS DE SECOURS
- ÉLU — GÉREZ VOTRE COMMUNICATION

3 SORTIR DE LA CRISE

- TECHNICIEN — FAITES UNE REMISE EN SERVICE PROGRESSIVE ET CONTRÔLÉE
- ÉLU — TIREZ LES ENSEIGNEMENTS DE L'ATTAQUE ET DÉFINISSEZ LES PLANS D'ACTION

CONTACTS

VOTRE SUPPORT INFORMATIQUE

Nom du contact :

N° de téléphone :

CONSEILS, SIGNALEMENT 24H/24
www.cert.ssi.gouv.fr/contact

CONSEILS ET ASSISTANCE
www.cybermalveillance.gouv.fr

NOTIFICATION DE VIOLATION DE DONNÉES PERSONNELLES
www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

POLICE, GENDARMERIE 17

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :
avisca · BANQUE des TERRITOIRES · coTer numérique · DÉCLIC.

POUR PLUS D'INFORMATIONS
www.cybermalveillance.gouv.fr