CYBERACTU'

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

Avril 2024

Mon DPO, ce héros !

Dossier page 24

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

Le rôle de délégué à la protection des données est encore mal connu et mal compris par beaucoup. Nouveau métier créé par le RGPD en 2018, il est en effet encore très récent.

Par ce numéro, nous souhaitions vous apporter un éclairage nouveau sur ce rôle qu'est le notre et que nous avons à cœur de faire connaître.

De plus, nous avons souhaité étoffer notre contenu en nous centrant sur une actualité débordante du point de vue de la sécurité des données en ce début d'année 2024 qui promet d'être une année chargée avec la prochaine entrée en vigueur d'une nouvelle directive européenne venant renforcer les obligations de tous en matière de cybersécurité.

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

LES TEXTES RÉGLEMENTAIRES

Règlement UE n°2024/903 du 13 mars 2024 établissant des mesures destinées à assurer un niveau élevé d'interopérabilité du secteur public dans l'ensemble de l'Union, dit « Règlement pour une Europe interopérable ».

Ce nouveau règlement européen vient soutenir la création d'un **réseau d'administrations publiques numériques souveraines et interconnectées** et accélérer la transformation numérique du secteur public européen.

Il vient ainsi poser les bases de la notion de « services publics numériques transeuropéens » par lesquels les organismes du secteur public des États membres de l'UE seront amenés à interagir entre eux par-delà les frontières en partageant des données, des informations et des connaissances au moyen de processus numériques afin d'offrir une continuité des services publics au sein de l'ensemble de l'UE.

Il pose ainsi des dispositions garantissant une coopération structurée de l'UE au sein de laquelle les administrations publiques se réunissent dans le cadre de projets détenus conjointement par les États membres, ainsi que par les régions et les villes. Il apporte également un cadre de gouvernance à plusieurs niveaux pilotés par le comité "Europe interopérable", qui est au cœur de la nouvelle structure mise en place par le règlement.

Ce règlement prévoit également la possibilité de partager et de réutiliser des solutions d'interopérabilité, alimentées par un guichet unique pour les solutions et la coopération communautaire (portail "Europe interopérable") et soutenues par des mesures visant à promouvoir l'innovation et à renforcer l'échange de compétences et de connaissances.

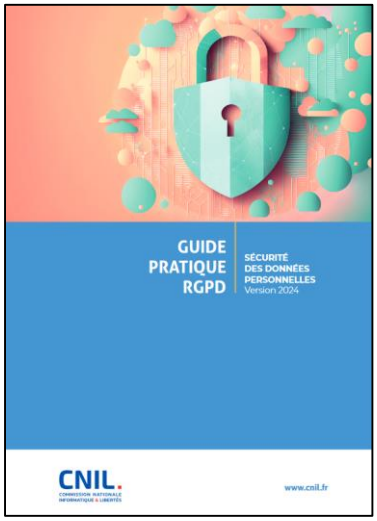
Son entrée en vigueur est prévue au **11 avril 2024**. Si son impact reste pour l'heure limitée pour les collectivités territoriales, de prochaines évolutions réglementaires et législatives pourraient ainsi apporter quelques nouveautés que nous ne manquerons pas de communiquer dans nos prochains numéros.

ATTENTION !

Entrée en vigueur de la directive NIS-2 le 17 octobre 2024

Cette directive viendra apporter de nouvelles obligations en matière de cybersécurité. Les collectivités territoriales et établissements publics **seront concernés**.

Plus de détails à venir lors de la transposition de la directive en droit français…



Pour retrouver cette édition 2024 du guide de sécurité des données, cliquez sur l'image ci-dessus

CNIL.

Publication du nouveau « Guide de sécurité des données » édition 2024

Le guide de sécurité des données est LA bible de tout délégué à la protection des données sur lequel se basent l'essentiel de ses recommandations en matière de sécurité. Mis à jour régulièrement aux vues des évolutions technologiques, ce guide a pour but de rappeler les précautions de sécurité à mettre en œuvre et recommandées par la CNIL.

Cette nouvelle version restructure le guide et introduit de nouvelles fiches, notamment sur l'intelligence artificielle, les applications mobiles, l'informatique en nuage (cloud) et les interfaces de programmation applicatives (API).

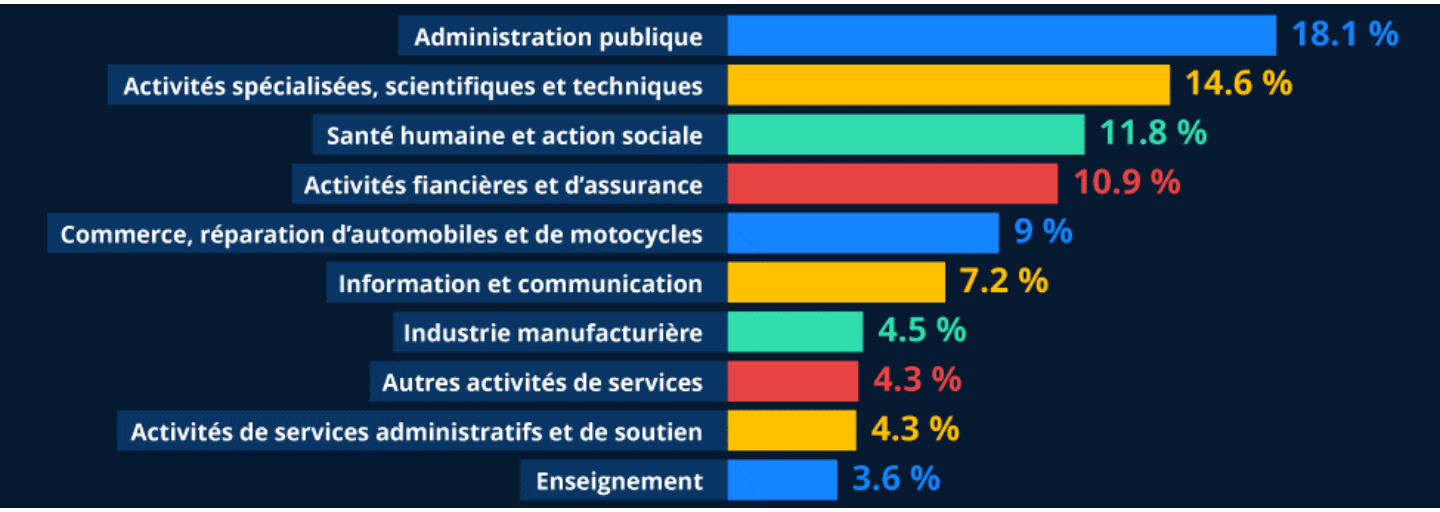
CYBER MALVEILLANCE .GOUV.FR

Publication du rapport d'activité 2023 du GIP Cybermalveillance.gouv.fr

À l'occasion de la publication de son rapport d'activité annuel, le dispositif action contre la cybermalveillance partage son état de la menace et revient sur les tendances et les faits marquants de l'année 2023, ses nouvelles productions et les différents projets auxquels il a contribué pour sensibiliser ses publics.

Pour retrouver ce rapport d'activité, cliquez sur l'image ci-dessus

Les notifications de violations de données reçues par la CNIL selon le type d'activité



Source : CNIL, « Violations de données personnelles : bilan de 5 années de RGPD » – 27 mars 2024

CNIL. Marie-Laure DENIS reconduite à la tête de la CNIL

Par décret publié au Journal officiel du 31 janvier 2024, Marie-Laure DENIS est reconduite dans ses fonctions de Présidente de la Commission nationale de l'informatique et des libertés pour un mandat de cinq ans.

Issue de la promotion « Condorcet » (1990 – 1992) de l'ENA, Marie-Laure DENIS a occupé diverses fonctions d'envergure, allant de la direction du cabinet de l'ancien Maire de Paris, Jean TIBERI, à la direction adjointe du cabinet de l'ancien Ministre de la santé, Jean-François MATTEI, ou encore en intégrant l'ancien Conseil supérieur de l'audiovisuel (désormais ARCOM) en qualité du groupe « radio » à compter de 2004.

Conseillère d'État depuis 2007, Marie-Laure DENIS succède à Isabelle FALQUE-PIERROTIN à la présidence de la CNIL à compter du 2 février 2019. Elle devient ainsi à cette même date la première Présidente de la CNIL désignée sous une nouvelle procédure qui accroît l'indépendance de l'autorité de contrôle française vis-à-vis du gouvernement.

C'est ainsi que, par décret du 31 janvier 2024, elle est reconduite dans ses fonctions suite à proposition du président de la République et avis favorable des commissions des lois de l'Assemblée nationale et du Sénat.

« *Honorée de ce renouvellement* », Marie-Laure DENIS voit dans cette décision la reconnaissance du travail accompli par la CNIL ces dernières années, malgré une explosion des usages numériques. Elle souhaite ainsi continuer sur la voie de la protection effective des données personnelles et du droit à la vie privée tout en « *privilégiant une régulation pragmatique et équilibrée* ».

Lors de ses diverses auditions parlementaires, elle a ainsi présenté certaines de ses **ambitions et priorités pour les cinq années à venir** :

- La protection de l'enfance dans les usages en ligne et l'éducation au numérique
- Le maintien d'un équilibre entre libertés et sécurité
- La régulation de l'intelligence artificielle
- La prévention des risques cyber
- La participation à une gouvernance partagée, des textes issus du « paquet numérique européen »
- La possibilité pour la CNIL de se projeter sur l'ensemble du territoire.

2024 : Les thématiques prioritaires des contrôles de la CNIL

Chaque début d'année, la CNIL présente les thématiques prioritaires sur lesquelles porteront une partie des contrôles (environs 1/3 du total des contrôles) qu'elle sera amenée à réaliser au cours de l'année. Ce début d'année 2024 ne fait donc pas exception, et l'autorité de contrôle a ainsi présenté ce 8 février quatre thématiques, dont certaines pourront intéresser fortement les collectivités territoriales…

La collecte des données dans le cadre des Jeux Olympiques et Paralympiques

La CNIL entend s'assurer que le dispositif de sécurité mis en place pour l'organisation des jeux de Paris en 2024 respecte la réglementation, notamment en ce qui concerne la mise en place de QR codes pour les zones à accès restreints, les habilitations d'accès et l'utilisation de caméras augmentées.

Outre l'aspect sécuritaire, la CNIL entend s'intéresser également au volet commercial des JO et notamment à la collecte des données lors de la vente des billets.

Les données des mineurs collectées en ligne

Afin de s'assurer que la vie privée des mineurs, considérés comme personnes à protéger, soit respectée, la CNIL entend cibler les applications et sites destinés à la collecte des données des mineurs, notamment en matière de contrôle de l'âge, des mesures de sécurité des données et de respect du principe de minimisation des données.

Les programmes de fidélité et tickets de caisse dématérialisés

Les enseignes commerciales peuvent être amenées à traiter l'ensemble de ces données pouvant révéler de nombreuses informations privées (habitudes alimentaires, présence d'animaux, composition du foyer, etc.). De plus, des traitements additionnels peuvent être menés pour l'envoi des tickets par SMS ou par mail. La CNIL entend ainsi contrôler le respect des droits des clients, notamment concernant le consentement à la réutilisation commerciale de ces données.

Le droit d'accès des personnes concernées

Conjointement avec ses partenaires européens, la CNIL va procéder à des vérifications sur les conditions de mise en œuvre du droit d'accès.

Ce droit vise à permettre aux usagers l'accès à leurs données détenues dans nos administrations.

2024 : Panorama de la menace cyber

Parce que les criminels ne se reposent jamais, et que nos collectivités territoriales sont de plus en plus ciblées, voici un panorama des tendances en matière de cybermenace à prendre en compte pour l'année à venir.

1

Le phishing et l'ingénierie sociale : La manipulation psychologique était déjà l'un des outils privilégiés des criminels numériques. Il n'y a hélas aucune raison de s'attendre à un quelconque changement pour l'année 2024.

Utilisant de plus en plus les données laissées en libre accès par leurs victimes elles-mêmes (notamment via les réseaux sociaux, dont LinkedIn et Facebook sont leurs « bases de données » favorites), les criminels ont pour but de convaincre leurs victimes de cliquer sur des liens piégés, contournant ainsi toutes les mesures de sécurité mises en place.

L'exemple-type ? L'arnaque au Maire/Président, par lequel l'attaquant usurpe l'identité de l'autorité et donne de faux ordres, et notamment concernant la modification des données de paiement.

Le conseil du DPO : Lors de toute demande portant sur les données personnelles, prenez l'habitude de vérifier l'identité de votre interlocuteur par tout moyen approprié. En cas de doute, n'hésitez pas à contacter votre DPO qui pourra vous conseiller.

2

L'externalisation et le cloud : La multiplication de l'externalisation des applications numériques (cloud, logiciel SaaS, etc.) fait que les cyberattaques contre ces applications devient une activité rentable pour les criminels qui peuvent ainsi toucher un grand nombre de victimes en attaquant une seule application.

L'interconnexion des réseaux entraine ainsi un agrandissement des fenêtres de tir des criminels qui n'ont que l'embarras du choix pour lancer leurs attaques.

Le conseil du DPO : Vérifiez que vos prestataires sont conformes au RGPD en prenant contact avec eux et en leur demandant toutes les garanties. Par ailleurs, signez avec eux un avenant les contraignant à prendre en compte la protection des données que vous leurs confiez.

3 ***L'essor de l'intelligence artificielle :*** L'arrivée fracassante de l'intelligence artificielle au cours de ces derniers mois est une véritable mine d'or pour les criminels numériques qui bénéficient ainsi d'une variété d'outils de plus en plus sophistiqués pour nous nuire.

Les outils tels que ChatGPT (et ses dérivés) permettent à quiconque d'apprendre facilement à réaliser un code (quand l'outil ne code pas lui-même) ou à planifier leurs attaques.

Mais le risque principal vient de l'utilisation de « *deepfakes* » (trucage vidéo et/ou sonore visant à usurper l'identité d'une personne), qui pourrait ainsi drastiquement augmenter, posant de sérieux défis vis-à-vis des risques d'usurpation d'identité.

Ainsi, en fin d'année 2023, un employé d'une multinationale hong-kongaise a été piégé par des criminels ayant réalisé un deepfake usurpant le visage et la voix du directeur financier du groupe lors d'une visioconférence. Comme cette personne ressemblait à une personne réelle, la victime a effectué sur ses ordres 15 transactions sur cinq comptes bancaires pour un montant total de 24 millions d'euros.

(Source : LeMondeInformatique.fr – 05 février 2024)

> ***Le conseil du DPO :*** Renforcez vos mesures de sécurité techniques en suivant les recommandations minimales en matière de sécurité (*Cf : Les 10 mesures essentielles pour assurer votre cybersécurité – cybermalveillance.gouv.fr).*

4 ***La cyber-guerre :*** Les tensions internationales se multipliant, de même que l'utilisation du numérique s'étend toujours plus, il ne serait pas étonnant de voir une multiplication des cyberattaques entrant dans ce contexte.

A ce titre, les collectivités territoriales restent des cibles privilégiées, n'ayant pas les mêmes moyens d'action que l'État, mais restant aux yeux des criminels des administrations publiques liées à l'État. Les collectivités, moins bien protégées, pourraient ainsi faire l'objet d'attaques ayant pour but, *in fine*, d'atteindre une cible étatique plus importante.

> ***Le conseil du DPO :*** En cas de violation de données, quelle qu'en soit la cause, prenez le réflexe de prévenir immédiatement la gendarmerie, qui dispose d'équipes spécialisées en la matière.

Répondre à une demande de droit d'accès

Toute personne peut obtenir

Des informations la concernant, de manière claire :
- Quelles données collectées ?
- Quelles durées de conservation ?
- Quels destinataires ?
- etc.

Une copie de ses données, quel que soit leur support de conservation

1 Si nécessaire, vérifiez qui est le demandeur

FACTURE
Numéro de client : 123456

En cas de doute :

2 Si nécessaire, demandez si la demande concerne

Des données spécifiques

Toutes les données de la personne

3 Vérifiez que la demande ne concerne pas un tiers

- Conjoint
- Collègue
- Secret des affaires
- Propriété intellectuelle

4 Répondez à la demande

- **1 mois max.** — Demande simple
- **8 jours max.** — Données de santé
- **3 mois max.** — Demande complexe (par ex. beaucoup de données)

Vous pouvez refuser si
- la demande est infondée ou excessive
- les données ont été effacées

Dans tous les cas, informez la personne sous un mois maximum

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

ZOOM sur une décision essentielle

DÉCISION DU CONSEIL D'ÉTAT DU 2 FÉVRIER 2024, N°461093

L'encre des registres de baptêmes reste indélébile aux tentatives d'effacement par les apostats.

Tel en a ainsi conclu le Conseil d'État ce 2 février 2024. Ainsi, une personne désirant renoncer à tout lien avec l'Église catholique a demandé l'effacement de son nom figurant dans le registre des baptêmes du diocèse d'Angers, conformément aux dispositions du RGPD.

Le diocèse, prenant acte de son apostasie, a simplement indiqué la mention « *a renié son baptême* » sur le registre. Estimant ainsi que ses droits n'avaient pas été respectés, l'homme en question a saisi la CNIL pour faire respecter son droit à d'opposition et à l'effacement de ses données personnelles.

L'autorité de contrôle a cependant clôturé sa plainte en affirmant que la mention apposée par l'association diocésaine suffisait à l'exercice de son droit d'opposition.

Saisi au contentieux, le Conseil d'État s'est ainsi penché sur cette question et a suivi l'avis de la CNIL en rejetant à son tour l'argumentation du demandeur.

Le Conseil d'État rappelle tout d'abord que pour l'Église catholique, les registres des baptêmes sont destinés à conserver la trace d'un évènement constituant l'entrée dans la communauté chrétienne et que le baptême ne peut être reçu qu'une seule fois dans la vie d'une personne.

Puis, relevant que l'effacement définitif de l'enregistrement du baptême pourrait empêcher la personne concernée de réintégrer la communauté chrétienne si elle le souhaite, le Conseil d'État considère que la mention du baptême initial est donc indispensable à l'Église.

Pour le Conseil d'État, les données figurant sur les registres des baptêmes bénéficient d'un traitement permis du fait de leurs conditions d'accès, de conservation et d'archivage, ainsi que de leur objectif tenant au suivi du parcours religieux des personnes baptisées et de l'établissement éventuel d'actes ultérieurs dans le cadre de l'administration du culte catholique.

L'intérêt qui s'attache, pour l'Église, à la conservation des données personnelles relatives au baptême figurant dans le registre, doit être regardé comme un motif légitime impérieux, prévalant sur l'intérêt moral du demandeur à demander l'effacement définitif de ses données.

Il est cependant **important de noter** que, si cette décision s'applique aux baptêmes religieux, **il n'en va pas de même aux baptêmes civils**, puisque ceux-ci n'ont nulle valeur juridique et n'ont pas vocation à lier une personne à un acte qui ne pourra se produire qu'une seule fois dans une vie. De plus, les baptêmes civils reposant sur le consentement des personnes (lequel peut être retiré à tout moment), les données concernant les baptêmes civils **devront être effacées si une demande est faite en ce sens**.

ATTENTION AUX PICKPOCKETS ! PROTÉGEZ VOS DONNÉES ET VOS OUTILS !

À près de quatre mois des Jeux Olympiques Paris 2024, les mesures de sécurité déployées par le comité organisateur ne cessent pas de soulever des interrogations. En l'espace d'une semaine, les vols des matériels informatiques sont déjà au nombre de deux et incluent deux clés USB ainsi que deux ordinateurs professionnels.

Le premier vol date du lundi 26 février et a été dénoncé par un agent ingénieur de la mairie de Paris. L'agent, qui se trouvait dans une rame du RER D s'est fait dérober sa sacoche avec son ordinateur professionnel et deux clés USB contenant des informations liées à l'organisation des jeux olympiques, de plus la sacoche contenait également son badge professionnel. Cependant, ses déclarations ont permis de savoir qu'une des clés USB était chiffrée et contenait uniquement des données personnelles. Sur la seconde clé USB, qui n'était pas chiffrée, se trouvait un compte-rendu de réunion sur les JO en lien avec les plans de voirie de Paris.

Par la suite de cet évènement, la maire de Paris, Anne Hidalgo, a demandé à l'inspection générale de la Ville d'ouvrir une enquête face à ces « manquements avérés aux procédures de sécurité interne », ainsi elle précise que des sanctions seront prises en fonction des conclusions de l'enquête.

Quelques jours plus tard dans la même semaine un deuxième vol a été signalé. Le vendredi 1er mars la secrétaire générale de la direction de l'hôpital d'Avicenne de Bobigny (Seine-Saint-Denis) a remarqué, en revenant de ses courses, que son sac contenant son ordinateur portable de travail avait disparu de sa voiture.

Elle a porté plainte signalant que son sac contenait des documents confidentiels en lien avec les jeux olympiques, notamment des plans d'accès et de circulation.

Une enquête a été ouverte pour vol avec dégradation. Quelques jours après il a été annoncé que ces informations n'étaient pas confidentielles et qu'elles étaient destinées à être publiques, notamment sur les plans de circulation de divers hôpitaux du département.

Dans l'univers de la sécurité des données le « *niveau de sécurité parfait* » n'existe pas. Mais pour s'y rapprocher le plus possible, la stratégie optimale est celle de mettre en place des mesures de sécurité organisationnelles. Parce que la sécurité c'est de l'organisation !

"*Lorsqu'il y a un aussi grand événement, il y a forcément l'implication d'une très grande variété de personnes qui ne sont pas toujours familières des procédures de sécurité. C'est la raison pour laquelle il est donc impératif de fonctionner avec des environnements chiffrés. C'est-à-dire que si on a des ordinateurs qui se retrouvaient perdus ou volés, ils ne pourraient pas être exploités et les informations resteraient confidentielles. Il convient de diffuser cette connaissance à l'ensemble des personnes qui sont amenées à gérer des informations sensibles*", pointe le spécialiste du risque numérique Nicolas Arpagian.

Ces évènements sont une occasion à saisir pour essayer de s'améliorer. Si ce type de situations ne sont pas corrigées et arrivent de nouveau, ce serait par contre inexcusable et une sanction par défaut de sécurité des données pourrait être appliquée par la CNIL. Pour rappel, elle l'a fait en décembre 2023 vis-à-vis de la société Amazon France Logistique qui a été imposée une amende de 32 millions d'euros. De même, pour des faits similaires, le Maire de Dobrzyniewo Duże (Pologne) s'est vue sanctionner pénalement d'une lourde amende pour ne pas avoir interdit à ses agents d'emporter leur ordinateur professionnel à leur domicile. Or, l'un des agents s'est vu dérober son matériel lors d'un cambriolage, d'où une sanction de 1 700 € prononcée le 22 mars 2022. Il sera donc intéressant d'offrir une attention particulière aux suites que la CNIL réservera à la Mairie de Paris ■

CYBERATTAQUE CHEZ VIAMEDIS ET ALMERYS : FOCUS SUR L'IMPORTANCE DU NIR

Deux mois après « la plus grosse faille de sécurité en France » on ne nous en parle plus !

Entre le 21 janvier et le 4 février dernier, deux opérateurs de tiers payant, Viamedis et Almerys, ont été ciblés par une cyberattaque, entrainant ainsi la fuite des données de 33 millions d'assurés, c'est-à-dire 1 français sur 2. Pour rappel, ces deux opérateurs sont chargés de gérer pour le compte des mutuelles les avances des frais et la télétransmission de nos actes médicaux et, ainsi, d'assurer la gestion du tiers payant pour de nombreuses complémentaires.

Les données qui ont été volées sont, pour les assurés et leur famille, l'état civil, le numéro de sécurité sociale, le nom, le prénom et la date de naissance, de même que les données correspondantes aux garanties couvertes par le tiers payant.

Mais en quoi cette cyberattaque peut vraiment nuire à la vie des personnes concernées ? Nous vous l'expliquons dans cet article.

En tête de liste des dangers potentiels se trouve la réutilisation de données la plus courante, c'est-à-dire la vente des données volées sur le darkweb. La commercialisation des données peut être très dangereuse : en effet la transmission peut atteindre de échelles très larges très rapidement.

Malheureusement, une fois que la fuite est effective nous n'avons que peu de moyens pour limiter les dégâts. Une autre pratique non moins courante pour les criminels du numérique est l'usurpation de l'identité. Dans la cyberattaque contre les deux opérateurs, il sera intéressant d'analyser les risques directement liés au vol du numéro de sécurité sociale.

Dans ce sens, nous allons analyser les risques liés à un usage malveillant du numéro de sécurité sociale. Le numéro d'inscription au répertoire (ou NIR) est géré par l'INSEE, ce numéro est

attribué dès la naissance aux personnes nées en France : il est unique et personnel, **il ne change pas**. Pour les personnes arrivant de l'étranger, il est attribué au moment de l'ouverture des droits à l'assurance maladie. Pour toutes ces raisons, **il est considéré comme une donnée à caractère hautement sensible au regard de la loi Informatique et Libertés**.

En effet ce numéro composé de 15 chiffres est un numéro unique qui permet d'identifier avec certitude la personne concernée. Il permet de connaître de nombreuses informations à lui seul, telles que nous pouvons le voir sur l'image ci-dessous.

De plus, au travers du dispositif numérique FranceConnect, il est possible de renseigner son NIR et un mot de passe pour accéder à de nombreux services publics (plus de 1400 services en ligne) parmi lesquels se trouvent la caisse d'allocations familiales (CAF), la caisse de retraite, France Travail, ou encore le site de l'Assurance Maladie.

Pour un malfaiteur, il est possible de trouver l'information qui lui manque, le mot de passe, par l'application de techniques telles que l'hameçonnage (phishing). Ainsi, un malfaiteur en possession de ces deux informations pourrait réaliser des crimes tels que :

Source : Magazine de l'assurance maladie de Paris

- Vol d'allocations : votre numéro de sécurité sociale est utilisé pour gérer les prestations sociales, telles que les allocations familiales, les indemnités journalières en cas de maladie, etc. Un individu mal intentionné pourrait voler ces avantages en utilisant votre numéro.
- Fraude fiscal : une personne pourrait remplir une déclaration d'impôts sur votre nom, entraînant des problèmes financiers et légaux pour vous.
- L'usurpation d'identité : l'auteur de menace pourrait demander des prêts en votre nom, recevoir des soins médicaux, ou même commettre des délits sous votre identité.
- Accès aux données médicales : Si quelqu'un obtient votre NIR, il pourrait accéder à votre historique de paiements médicaux et potentiellement abuser du système.
- Calcul de votre retraite : votre NIR est également utilisé pour calculer vos droits à la retraite. Une personne malveillante pourrait manipuler ces informations.

Nous vous invitons ainsi à consulter les recommandations et informations proposées par la CNIL et le goupement Cybermalveillance.gouv.fr.

Ainsi, si vous êtes parmi les personnes qui ont été affectées, il est possible de déposer plainte en utilisant le formulaire de lettre-plainte en ligne accessible sur le portail sécurisé de l'État Demarches-simplifiées.fr (*lien accessible en cliquant sur le bouton ci-dessous*) ■

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
demarches-simplifiees.fr

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

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

mémo

10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

ADOPTER LES BONNES PRATIQUES

1. Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez
2. Ne mélangez pas votre messagerie professionnelle et personnelle
3. Ayez une utilisation raisonnable d'Internet au travail
4. Maîtrisez vos propos sur les réseaux sociaux
5. N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles
6. Faites les mises à jour de sécurité de vos équipements
7. Utilisez une solution de sécurité contre les virus et autres attaques
8. N'installez des applications que depuis les sites ou magasins officiels
9. Méfiez-vous des supports USB
10. Évitez les réseaux Wi-Fi publics ou inconnus

Pour en savoir plus ou vous faire assister, rendez-vous sur Cybermalveillance.gouv.fr

Les décisions des autorités chargées de la protection des données

24 janvier 2024 : Italie – 6 000 €

La CNIL italienne a infligé une amende de 6 000 euros à une commune dont le nom n'a pas été révélé. La municipalité avait **illégalement publié des informations** sur les cas de Covid de citoyens sur sa page Facebook. La municipalité **n'avait pas non plus nommé de délégué à la protection des données** et donc n'avait pas fourni ses coordonnées à l'autorité en temps utile.

24 janvier 2024 : Italie – 8 000 €

La ville de Salento (1 793 habitants) s'est vue infliger une amende de 8 000 euros **pour ne pas avoir fourni à la CNIL italienne les coordonnées de son Délégué à la Protection des données** par la procédure en ligne spécifique et en temps utile.

29 janvier 2024 : Grèce – 25 000 €

L'Autorité Hellénique de Protection des Données a infligé une amende de 25 000 euros au Ministère du Développement rural et de l'Alimentation p**our avoir omis de nommer un délégué à la protection des données** et pour **ne pas avoir suffisamment coopéré avec l'autorité**.

29 janvier 2024 : Grèce – 5 000 €

L'Autorité Hellénique de Protection des Données a imposé une sanction de 5 000 euros à la Mairie d'Athènes pour **défaut de coopération**. Le contrôleur avait envoyé un questionnaire unique à la mairie, ce document était inscrit dans le projet du CEPD d'évaluer la définition et la position du Délégué à la protection des données. La municipalité d'Athènes n'a pas répondu à l'Autorité dans les délais impartis.

30 janvier 2024 : Roumanie – 2 000 €

La commune de Bucarest a écopé d'une amende de 2 000 euros pour **ne pas avoir fourni les informations demandées** par l'Autorité nationale roumaine de contrôle du traitement des données personnelles au cours d'une enquête.

31 janvier 2024 : Italie – 5 000 €

La commune de Syracuse s'est vue infliger une amende de 5 000 euros **pour ne pas avoir fourni à la CNIL italienne les coordonnées de son Délégué à la Protection des données** par la procédure en ligne spécifique et en temps utile.

31 janvier 2024 : Italie – 2 000 €

Le Consortium municipal libre de Caltanissetta s'est vue infliger une amende de 2 000 euros pour **ne pas avoir fourni à la CNIL italienne les coordonnées de son Délégué à la Protection des données** par la procédure en ligne spécifique et en temps utile.

31 janvier 2024 : Italie – 2 000 €

La commune de Catanzaro (130 000 habitants) s'est vue infliger une amende de 2 000 euros **pour ne pas avoir fourni à la CNIL italienne les coordonnées de son Délégué à la Protection des données** par la procédure en ligne spécifique et en temps utile.

31 janvier 2024 : Italie – 2 000 €

La ville de Sassari, en Sardaigne (d'environ 85 000 habitants) s'est vue infliger une amende de 2 000 euros pour ne pas avoir fourni à la CNIL italienne les coordonnées de son Délégué à la Protection des données par la procédure en ligne spécifique et en temps utile.

NÉCROLOGIE

LES DERNIÈRES VICTIMES DE CYBERATTAQUES*

Sevran
17 janvier 2024

Une cinquantaine de lycées
21 mars 2024

Département de la Sarthe
24 janvier 2024

Fouesnant
1er janvier 2024

Communauté de communes du Pays fouesnantais
1er janvier 2024

CHU de Nantes
14 janvier 2024

CHU d'Armentières
11 février 2024

France Travail
13 mars 2024

Plusieurs Ministères
12 mars 2024

Communauté de communes de Gevrey-Chambertin et de Nuits-Saint-Georges
15 mars 2024

Dupont restauration (Délégataire - Mairie de Nîmes)
Février 2024

Conseil régional de Guadeloupe
21 février 2024

Saint-Philippe (Réunion)
1er janvier 2024

** Sur les trois derniers mois*

LE CENTRE CYBERSECURITE EN OCCITANIE

CYBER'OCC

Service d'Urgence Cyber

Soutenu par RÉPUBLIQUE FRANÇAISE

CSIRT régional*

*Computer Security Incident Respone Team

0 800 71 13 13

N° GRATUIT

Centre de Ressources

Guichet Unique

Veille Cyber et Alerte

Communauté Cyber

Facilitateur - Catalyseur

Sensibilisation

Laboratoire à idées

OCCITANIA European Digital Innovation Hub

EDIH

La Région Occitanie Pyrénées · Méditerranée

ADOCC Agence de Développement Économique

Pkitia Data et IA en pleine confiance

contact@cyberocc.fr

+0 800 71 13 13

www.cyberocc.com

RETOUR VERS 2023

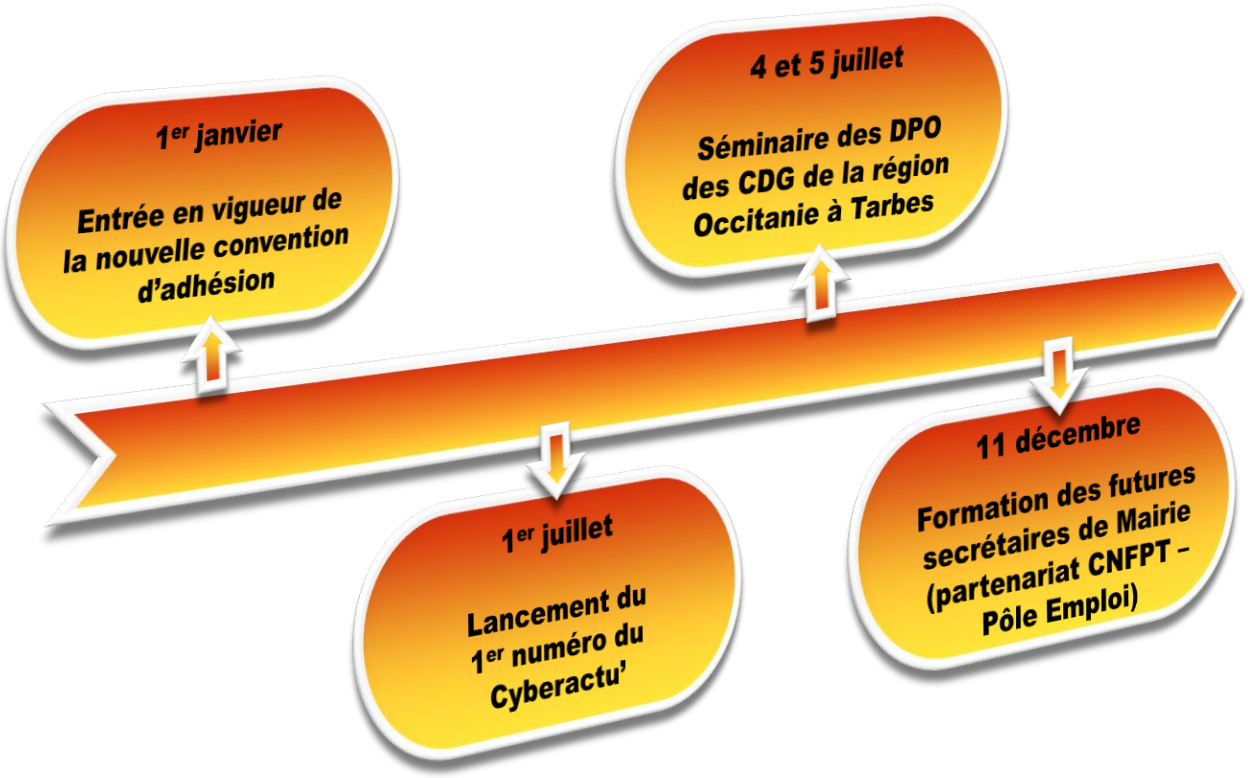
L'année 2023 fut une année de renouveau pour notre service, qui existe désormais depuis plus de 5 ans. La nécessité de s'adapter aux nouveaux défis qui s'offrent aujourd'hui aux collectivités territoriales, mais aussi de répondre à une demande de plus en plus croissante nous a conduit à revoir notre offre et à adapter notre convention d'adhésion en conséquences.

C'est ainsi que l'année 2023 a marqué le début de notre nouvelle convention qui a rencontré un véritable succès, permettant notamment aux petites communes de s'offrir une prestation aujourd'hui nécessaire du fait des évolutions législatives et de risques toujours plus nombreux. Notre volonté de nous tenir à vos côtés face à cette nouvelle donne nous a ainsi conduit à étendre nos domaines d'expertise. C'est également dans une volonté de sensibiliser toujours plus les agents et les élus que nous avons lancé dans le courant de l'année notre magazine qui a rencontré un écho inattendu et qui nous oblige désormais à toujours plus de qualité dans le contenu qui vous est ainsi offert.

Nous sommes donc heureux de pouvoir regarder le travail ainsi accompli et nous tenons prêts à relever les défis de l'année 2024 qui sera placée sous le signe du développement de la culture de la protection des données. Outre notre magazine, nous avons ainsi souhaité nous rendre encore plus sur le terrain à votre rencontre en multipliant les réunions et les séances d'information. Guettez donc votre messagerie : des invitations pour nos prochains événements vous seront envoyés dans les prochains mois !

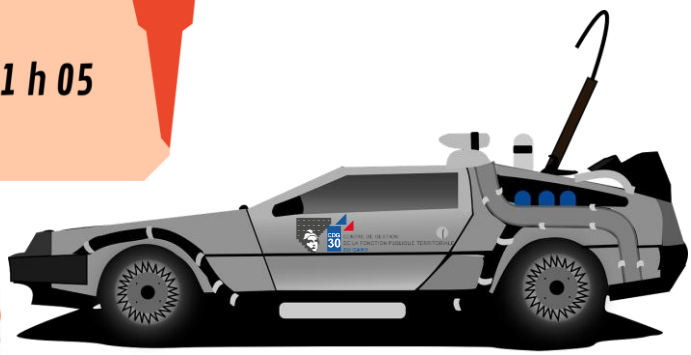
C'est également dans un objectif de toujours mieux vous servir que notre partie « protection des données » du site internet du centre de gestion sera amenée à évoluer pour vous permettre de retrouver au même endroit tous nos documents, modèles et fiches de procédures dédiés à la protection des données et à la cybersécurité.

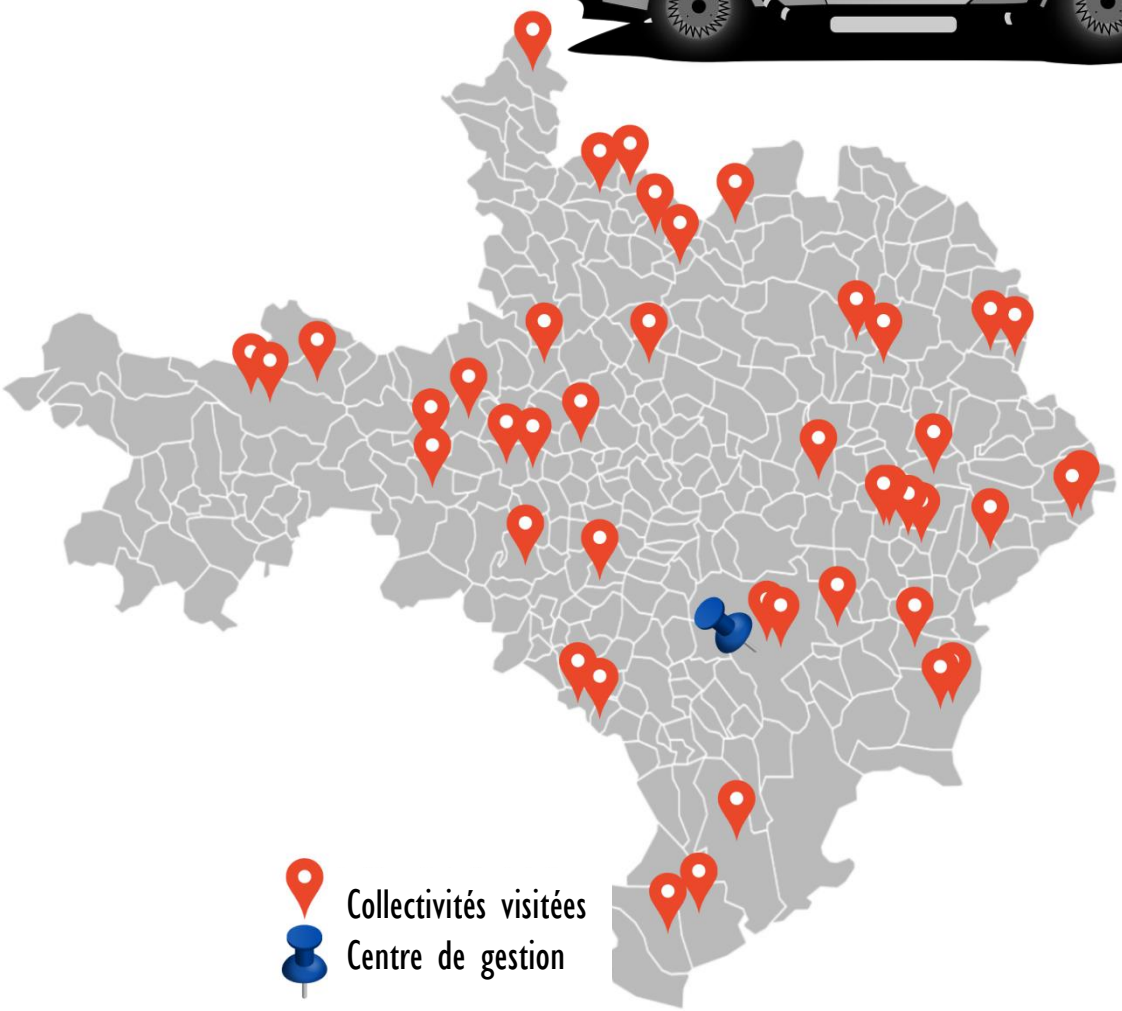
Nous vous remercions encore pour cette année 2023 et vous disons à très bientôt !

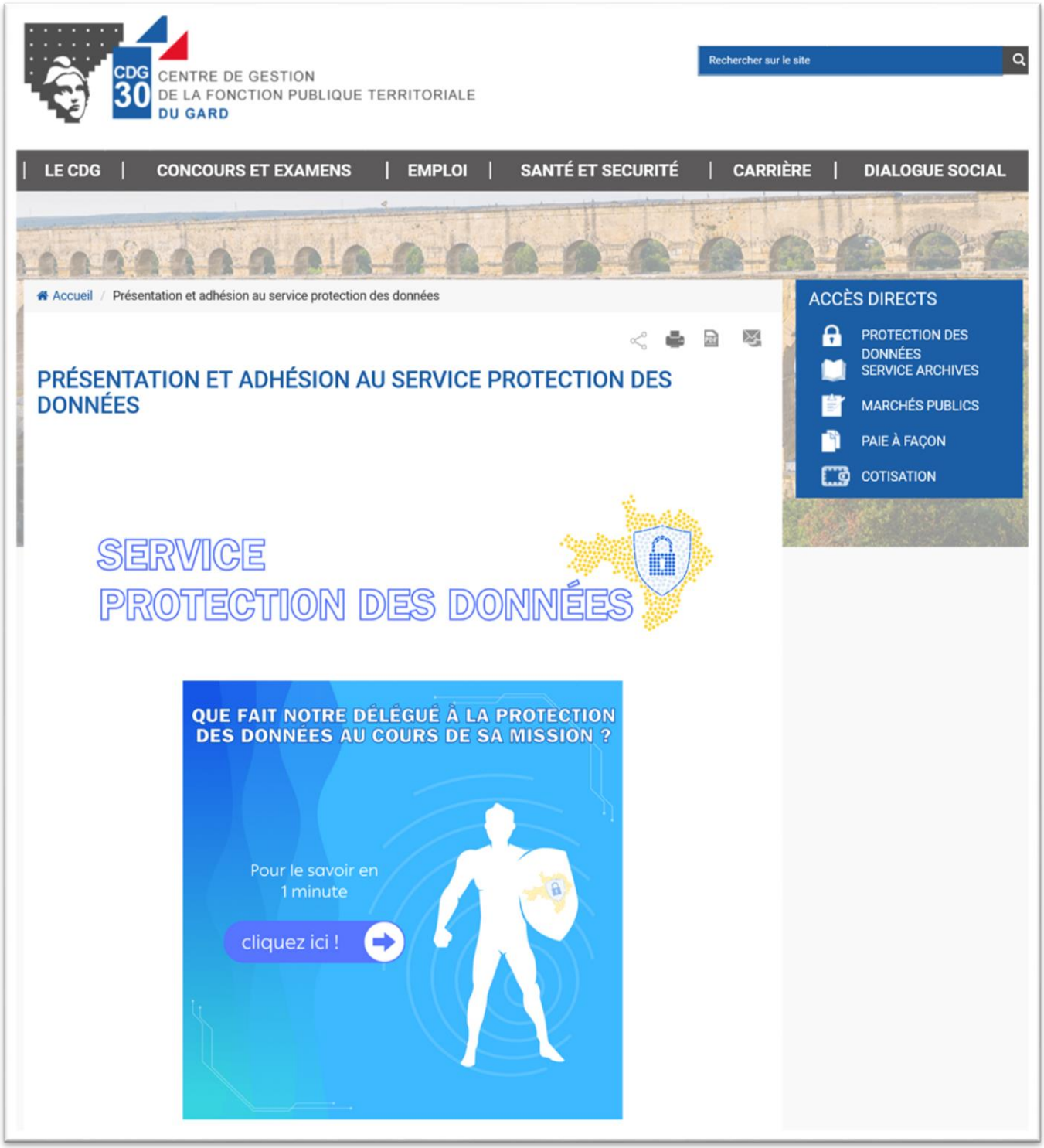


Les statistiques de l'année 2023

Nombre d'adhérents	106
Nombre de visites	49
Kilomètres parcourus	4 150,8 Km
Temps de déplacement à votre service	111 h 05







La partie « protection des données » du site internet du centre de gestion évolue !

Retrouvez nous sur :

cdg30.fr

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

Le yaourtophone, la garantie de conversations sécurisées.

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

MON DPO, CE HÉROS !

Il est cinq heures. Si c'est à cette heure-là que Paris s'éveille, selon Jacques Dutronc, c'est aussi le cas de Marie-Amélie, secrétaire de Mairie d'une petite collectivité rurale. Pourtant, ce jour-là, le café n'a pas le même goût que d'habitude. Les yeux lourds, la secrétaire a en effet très mal dormi. La veille, elle a eu rendez-vous avec son délégué à la protection des données. Ce rendez-vous, elle ne l'avait pas demandé. Elle avait en effet assez de tâches à accomplir, assez de travail à faire. Le budget communal était encore à finaliser, et de récentes inondations sur une partie de la commune avaient apporté leur lot d'ennuis supplémentaires.

Malgré ce, elle avait accepté de recevoir cette personne à qui elle espérait déléguer, comme son nom le laisse à penser, cette mise en conformité à un règlement imposé par l'Europe et qui ne fait que nous ajouter toujours plus de travail. Pourtant, ce rendez-vous ne s'était pas passé comme attendu…

Car son délégué à la protection des données lui avait fait peur. Très peur. Il lui avait en effet parlé, exemples à l'appui, des risques encourus à ne pas respecter cette réglementation. Il lui avait montré des cas d'usurpation d'identité résultant de collectivités à qui l'on avait dérobé des données. Il lui avait parlé des sanctions, très lourdes, qui avaient touché certaines communes, en France comme en Europe. Et bien sûr, il lui avait expliqué son rôle, qui était loin de ce qu'elle avait imaginé…

Hérité de l'ancien correspondant informatique et libertés (plus connu sous l'acronyme de « CIL »), dont la présence n'était alors que facultative, le délégué à la protection des données est un rôle nouveau apporté par le RGPD et rendu obligatoire pour toute administration. Bien souvent vu comme l'empêcheur de travailler en rond, ou à défaut lorsqu'il arrive à obtenir l'oreille attentive de ses collaborateurs, comme le « Monsieur angoisse » qui n'est là que pour faire peur en employant des mots compliqués comme « *Privacy by design* » ou « *data compliance* ». Il n'est souvent que celui à qui l'on a donné la mise en conformité au RGPD parce qu'on ne savait pas à qui la donner, faute de trouver quelqu'un d'assez disponible pour s'attaquer à cette montagne perçue comme infranchissable.

Malgré cette réputation peu

reluisante, son véritable rôle reste obscur pour toute autre personne que lui-même. Le délégué à la protection des données, également appelé « DPD » ou « DPO » (pour son appellation en anglais, langue de rédaction du RGPD, « *data privacy officer* »), est pourtant la nouvelle pierre angulaire dans les collectivités et établissements publics. Soutien de l'autorité territoriale et assistant de tous les agents dans leur utilisation des données (et donc, de leur travail, si l'on considère l'utilisation des données comme l'essentiel de leurs tâches), le DPO est un allié essentiel sur lequel tous devraient pouvoir compter, pour peu que l'on comprenne réellement son rôle.

Un couteau suisse numérique

Ses tâches, listées par l'article 39 du RGPD, sont très larges : il a ainsi essentiellement un rôle de conseil envers tous ceux qui, au sein de son administration, traitent des données à caractère personnel. Telle une assistance juridique, il est avant tout présent pour répondre aux questions de tout un chacun sur leur utilisation de données personnelles dans un cadre professionnel. Cela implique donc des connaissances tout aussi larges, qu'il s'agisse de comprendre la réglementation en faisant les recherches juridiques nécessaires, de pouvoir recommander des solutions techniques visant à garantir la sécurité des données, qu'elles soient informatiques ou sous format papier, ou encore de pouvoir recommander des mesures organisationnelles afin d'assurer un management qui permette de faire circuler les données en toute sécurité.

Ce rôle est d'autant plus complexe au sein des administrations publiques qu'à ce triptyque de fonctions en qualité de « juriste – technicien – conseiller en organisation » s'ajoute un rôle de « conseiller archiviste » en devant assurer un contrôle du respect des durées d'utilité administrative des données imposées d'un côté par les recommandations du service

Les grandes caractéristiques des DPO en 2021

- **72%** exercent leur fonction comme DPO interne (+ 4 points)
- **29%** excercent en Île-de-France, première région d'exercice (- 6 points depuis 2019)
- La représentation des femmes et des hommes au sein de la fonction est équilibrée.
- **62%** sont issus de formation supérieure, de niveau 7 et 8 (- 5 points)
- **63%** sont âgés de 40 ans et plus
- **69%** des DPO internes et mutualisés sont cadres ou cadres supérieurs (- 16 points)
- **54%** des DPO internes et mutualisés exercent dans une structure inférieure ou égale à 250 salariés (+ 17 points)
- **84%** des DPO internes et mutualisés sont en CDI ou fonctionnaires
- **65%** des DPO internes et mutualisés sont directement rattachés à la direction (+ 12 points)
- **78%** des DPO internes et mutualisés exercent leur fonction à temps partiel en plus d'une autre fonction (+ 10 points)
- **70%** des DPO internes et mutualisés à temps partiel consacrent 25% et moins de leur temps de travail à leurs missions de DPO (+ 29 points)
- **76%** travaillent seuls et sans équipe
- **74%** des DPO internes et mutualisés n'ont pas de réseau de Relais Informatique et Libertés et 60 % n'ont pas de budget
- **47%** sont issus d'autres domaines d'expertise que le domaine juridique et informatique (+ 12 points)
- **55%** ont une ancienneté dans la fonction de DPO de 2 ans et moins
- **58%** sont membre d'une association ou en lien avec d'autres DPO (- 14 points)

Source : Évolution de la fonction de délégué à la protection des données – Direction générale à l'emploi et à la formation professionnelle – Édition 2022

interministériel des archives de France, et de l'autre par le principe de limitation de la conservation des données posé par le RGPD. Jongler ainsi entre ces deux réglementations parfois (souvent) contradictoires relève ainsi de l'exploit qui rend la fonction de DPO tout autant difficile que passionnante.

Mais le rôle du DPO ne s'arrête pas à cette mission de conseil. Il dispose en effet d'autres prérogatives qui lui valent cette réputation que nous vous exposions plus tôt. L'article 39 du RGPD lui impose également de contrôler le respect de la réglementation en matière de protection des données, mais aussi des consignes internes données par l'autorité territoriale afin de protéger les données. Il peut être ainsi amené à questionner l'ensemble des agents sur leurs pratiques et les précautions prises pour veiller à la sécurité des informations détenues et traitées dans le cadre de leurs missions, tel un « ACFI* de la vie privée ».

Pourtant, visualiser le DPO comme une sorte de « père fouettard territorial » serait erroné. Il ne dispose en effet d'aucun pouvoir de sanction, et il n'est pas là pour empêcher les agents de traiter les données. Fort de son devoir de conseil, il est ainsi présent avant tout pour prévenir non seulement tout risque sur les données, mais aussi pour prévenir tout risque pouvant porter sur les agents eux-mêmes s'ils venaient hélas à traiter malencontreusement les données de manière non conforme. Il est ainsi dans l'intérêt de tout un chacun de suivre ses recommandations et de ne pas l'observer comme un ennemi. Le DPO est en effet le meilleur allié des agents afin de leur permettre de travailler en toute sécurité. Et si une violation de données venait ainsi à survenir malgré ses conseils, les agents pourraient avoir au moins la fierté d'avoir employé tous les moyens possibles pour protéger les données sous leur responsabilité.

Ainsi, s'il peut ainsi parfois être inquiétant, le DPO est toutefois une présence qui se doit d'être rassurante pour les agents des collectivités. Véritable épaule sur laquelle s'appuyer, le DPO est là pour soutenir les agents en leur recommandant des moyens de sécuriser leur travail, tant d'un point de vue technique qu'organisationnel.

Mais le rôle de soutien du DPO ne s'arrête pas à celui de conseiller. En certains cas, il endosse en effet celui peu envieux d'avocat conseil lorsque l'autorité de contrôle qu'est la CNIL est amenée à réaliser un contrôle.

En effet, en vertu des pouvoirs conférés par le RGPD, la CNIL dispose de la possibilité de contrôler le respect de la réglementation et d'en sanctionner les manquements. Le DPO aura alors la difficile tâche de coopérer et de défendre sa collectivité en fournissant à l'autorité de contrôle tous les éléments destinés à justifier de la bonne utilisation des données personnelles.

Ce rôle, qui peut l'amener à avoir quelques sueurs froides, est toutefois un rôle ingrat, puisque tout manquement sanctionné pourrait lui être reproché. « *Après tout, c'est bien lui qui s'occupe de la mise en conformité au RGPD ! C'est donc entièrement de sa faute si la réglementation n'a pas été respectée !* » entend-t-on régulièrement. Et pourtant…

Les conseilleurs ne sont pas les payeurs

Le RGPD est clair : seul le responsable des traitements (l'autorité territoriale, au sein des collectivités) est responsable en cas de manquement à la réglementation sur la protection des données. Car oui, le DPO, s'il est bien le « monsieur conformité » (ou « madame », car chacun des deux sexes est ici représenté de façon équilibrée) au sein de nos collectivités, il ne dispose d'aucun pouvoir afin de

31%

déclarent n'avoir jamais vécu de moments de tension interne ou de conflit personnel entre leur rôle de DPO et les perceptions des attentes des structures dans lesquelles ils interviennent

19%

des **DPO externes** trouvent que leur fonction est souvent ou toujours stressante

30%

des **DPO internes et internes mutualisés** trouvent que leur fonction est souvent ou toujours stressante

86%

déclarent souhaiter poursuivre leurs missions avec une forte motivation

** ACFI = Agent chargé de la fonction d'inspection, dont le rôle est de prévenir tout risque professionnel pouvant heurter la santé et/ou la sécurité de l'agent*

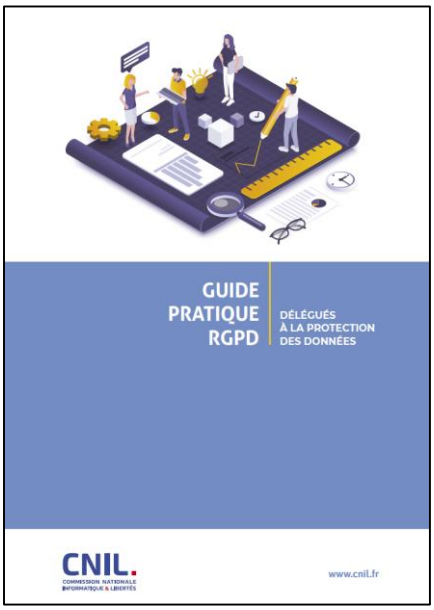
décider des finalités ou des moyens par lesquels les données seront traitées, car seul le responsable des traitements dispose d'un tel pouvoir, et le DPO ne peut pas intervenir sur les traitements de données lui-même.

Afin d'illustrer ce propos, l'on peut prendre en exemple un garagiste expertisant un véhicule au cours d'un contrôle technique : s'il va lister tous les points défaillants, il ne va pour autant pas prendre la décision de procéder aux réparations, ce pouvoir revenant au seul propriétaire du véhicule.

La mise en conformité au RGPD suit ainsi la même logique : le DPO va conseiller les agents et l'autorité territoriale. Si, pour autant, ses conseils ne sont pas suivis, il ne saurait être tenu pour responsable.

Mais cette vision du DPO « conseilleur mais pas payeur » ne doit pas faire oublier qu'il reste avant tout une aide indispensable pour tout responsable de traitements.

Le DPO est comme tous les spécialistes : il est là avant tout pour intervenir dans un domaine complexe et aider à la prise de décision. Il est là pour protéger et sécuriser, même si cela revient parfois à devoir mettre en œuvre des mesures impopulaires. Lorsque la ceinture de sécurité a été rendue obligatoire dans les véhicules, nombreuses ont été les voix pour s'élever contre ce qui semblait être une mesure liberticide et inutile. Pourtant, qui reviendrait aujourd'hui sur cette mesure salutaire ayant sans doute sauvé de nombreuses vies ? Ainsi, il convient de ne pas voir le DPO ni comme un ennemi, ni comme un magicien qui viendrait résoudre tous les problèmes d'un coup de baguette magique. Il faut savoir le prendre comme il est : un élément indispensable pour toute organisation qui cherche à prendre les meilleures décisions afin de rendre un service de qualité envers ses usagers qui comptent de plus en plus sur l'Administration comme un pilier dans un monde en perpétuel mouvement et ou la vie privée est de plus en plus chahutée ■



Pour vous aider, la CNIL a publié un guide du délégué à la protection des données. Pour le retrouver, cliquez sur l'image ci-dessus

Mon archiviste, cette héroïne !

Les frais de conservation des archives communales constituent une dépense obligatoire pour les communes (Code Général des Collectivités territoriales, article L.2321-2, second alinéa).

La conservation et la communication des archives demeurent sous la responsabilité civile et pénale du maire (Code du patrimoine, articles L.214-3 et L.214-4).

Les collectivités territoriales et les groupements de collectivités territoriales sont propriétaires de leurs archives. Elles en assurent elles-mêmes la conservation et la mise en valeur sous le contrôle scientifique et technique de l'État (Code du Patrimoine, article L.212-6-1). Les conserver, les protéger et les valoriser permet de sauvegarder l'histoire de votre collectivité, autant d'un point de vue juridique qu'historique.

Créé en 2000, le service « Archives » du centre de gestion du Gard propose aux collectivités et établissements publics du département des prestations d'archivage et conseils de gestion des archives.

Beaucoup de structures déplorent :

- Un manque de place
- Une perte de temps dans la recherche documentaire
- Un patrimoine méconnu du grand public

Les prestations proposées permettent non seulement de satisfaire aux obligations légales en matière d'archives publiques, mais également de remédier aux problématiques de gestion documentaire et de mise en valeur des documents.

Pour cela, le centre de gestion du Gard met à disposition des collectivités qui le souhaitent un archiviste qualifié, afin de répondre aux difficultés et aux besoins de celles-ci.

Les **prestations** proposées par Sarah, notre archiviste itinérante, sont les suivantes :

- **Diagnostic :** visite du local archives et rédaction d'un rapport mettant en évidence les solutions proposées, au libre choix de la collectivité
- **Tri et élimination :** repérage des éliminables et rédaction du bordereau légal
- **Classement :** classement des archives anciennes, modernes et contemporaines selon la réglementation en vigueur, rédaction d'un inventaire complet et opérations de maintenances annuelles
- **Conseils et sensibilisation :** conseils aux agents désignés comme « référents archives » pour l'archivage, la conservation, la communication, l'aménagement de locaux et d'espaces de consultation des archives

Pour plus d'informations, n'hésitez pas à la contacter aux coordonnées ci-dessous :

LE BON GESTE

L'UTILISATION DES COOKIES ET AUTRES TRACEURS

Qu'est-ce qu'un cookie ?

Non, il ne s'agit pas de ce délicieux biscuit garni de pépites de chocolats dont nous raffolons tous tant.

Un **cookie**, aussi appelé « témoin de connexion » est un petit fichier déposé sur le disque dur à l'insu de l'internaute, lors de la consultation de certains sites web, et qui conserve des informations (nombre de visites, nombre de pages vues, etc.) en vue d'une connexion ultérieure.

Les cookies ont de multiples usages : ils peuvent servir à mémoriser votre identifiant client auprès d'un site marchand, le contenu courant de votre panier d'achat, la langue d'affichage de la page web, un identifiant permettant de tracer votre navigation à des fins statistiques ou publicitaires, etc. Certains de ces usages sont strictement nécessaires aux fonctionnalités expressément demandées par l'utilisateur ou bien à l'établissement de la communication et donc exemptés de consentement. D'autres, qui ne correspondent pas à ces critères, nécessitent un consentement de l'utilisateur avant lecture ou écriture.

Pourquoi dois-je faire attention ?

Les cookies sont déposés à l'insu des utilisateurs. Or, certains cookies ne sont pas strictement nécessaires au bon fonctionnement du site. L'accord de l'utilisateur doit donc être demandé avant leur installation.

L'article 82 de la loi « Informatique et Libertés » vient préciser que le recueil de cookies :

- Doit faire l'objet d'un consentement préalable de l'utilisateur avant le stockage d'informations sur son terminal ou l'accès à des informations déjà stockées sur celui-ci
- **Sauf** si ces actions sont strictement nécessaires à la fourniture d'un service de communication en ligne expressément demandé par l'utilisateur ou ont pour finalité exclusive de permettre ou faciliter une communication par voie électronique

Ainsi, tous les cookies n'ayant pas pour finalité exclusive de permettre ou faciliter une communication par voie électronique ou n'étant pas strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur nécessitent le consentement préalable de l'internaute (par exemple les cookies permettant une publicité personnalisée ou liés aux réseaux sociaux).

Recette pour de bons cookies

Ingrédients

- Un ordinateur
- Un site internet hébergé en France
- Une personne en charge de la maintenance du site internet

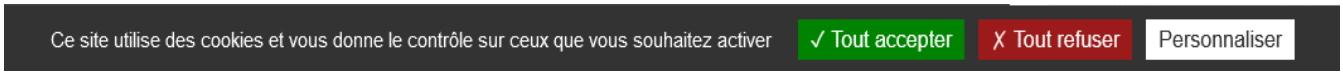
Difficulté : **Facile**

1 - Recueillir le consentement de l'utilisateur *préalablement* au dépôt ou à la lecture du cookie

- Tant que la personne n'a pas donné son consentement, les cookies ne peuvent pas être déposés ou lus sur son terminal.
- Il doit être requis à chaque fois qu'une nouvelle finalité nécessitant le consentement vient s'ajouter aux finalités initialement prévues.

2 - Informer l'utilisateur de manière claire et sans équivoque

- L'information doit être **visible**, **mise en évidence** et **complète**. Elle doit être rédigée en des termes simples et compréhensibles par tout utilisateur.
- Elle doit permettre aux internautes d'être parfaitement informés notamment s'agissant des différentes finalités des cookies et de l'identité des responsables du ou des traitements.



3 - Assurer un choix réel pour l'utilisateur

- L'utilisateur doit pouvoir accepter ou refuser le dépôt et/ou la lecture des cookies avec le même degré de simplicité. Autrement dit, un bouton «**je refuse**» doit être présent aux côtés du bouton «**j'accepte**».

4 - Permettre à l'utilisateur de retirer son consentement

- Il doit être aussi simple de retirer son consentement que de le donner.
- Des solutions permettant aux utilisateurs de retirer leur consentement doivent être mises à la disposition de l'utilisateur. Elles doivent être accessibles à tout moment.