

# CENTRE DE GESTION

DU GARD



## COLLECTIVITES TERRITORIALES ET PROTECTION DES DONNEES



CENTRE DE GESTION  
DE LA FONCTION PUBLIQUE TERRITORIALE  
DU GARD



Délégué à la protection  
des données



# Sommaire

<b>Le RGPD expliqué</b>	<b>05</b>
<b>Les bons réflexes</b>	<b>19</b>
<b>Le télétravail</b>	<b>29</b>
<b>En cas de problème</b>	<b>35</b>





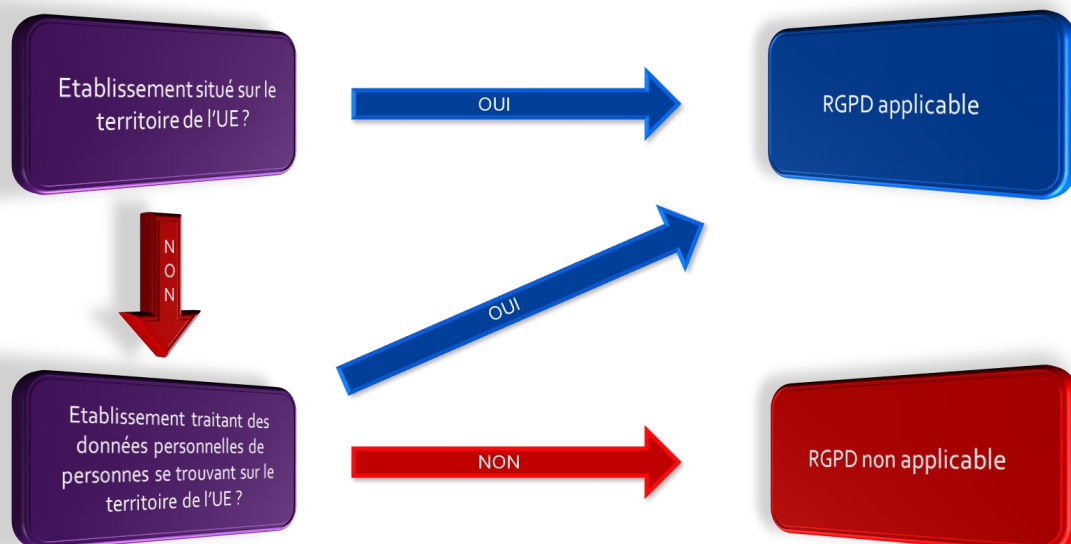
# Le RGPD expliqué

<b>Le RGPD à la loupe</b>	<b>06</b>
<b>Les risques</b>	<b>10</b>
<b>Les acteurs du RGPD</b>	<b>12</b>
<b>La mise en conformité</b>	<b>16</b>



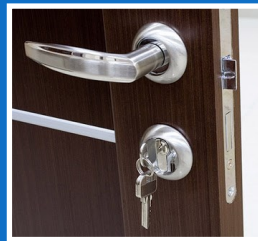
# Le RGPD à la loupe

- **Qu'est-ce que le RGPD ?**
  - Il s'agit d'un règlement européen s'appliquant aux collectivités territoriales, aux établissements publics, mais aussi aux entreprises privées entré en vigueur le 25 mai 2018
  - Son objectif est de **renforcer la protection de la vie privée** des citoyens européens en contraignant les entreprises et administrations à **prendre des mesures de protection** des données relatives aux citoyens européens
  - Son application est contrôlée par la CNIL, autorité de référence pour la France
- **A qui s'applique-t-il ?**
  - A tout établissement public ou privé et à toutes collectivités territoriale traitant des données de citoyens européens, que ce traitement se fasse ou non sur le sol européen
    - *Ainsi, Google, bien que société américaine ayant son siège aux Etats-Unis, est soumise au RGPD, car traitant des données de citoyens européens*



# Le RGPD à la loupe

- **A quoi sert ce RGPD ?**
  - Son but premier est de protéger la vie privée des citoyens européens, soit contre les usages abusifs de données, soit en renforçant la sécurité de données souvent mal protégées et pouvant être facilement dérobées par des personnes malveillantes



## (Mauvais) exemple :

*Patrick, en visite dans la collectivité, a réussi à se soustraire à la vigilance des agents de l'accueil. Impatient d'accéder à son dossier, il se rend dans le bureau le plus proche pour le chercher. Le bureau n'étant pas verrouillé, il peut entrer et accéder à tous les dossiers, y compris ceux qui ne le concernent pas.*

- **Le RGPD a-t-il d'autres utilités ?**
  - Oui ! Le RGPD permet de mieux gérer ses données, de remettre à plat son organisation dans la gestion des données et parfois de découvrir de nouvelles méthodes de travail, plus efficaces et plus rapides
  - La protection de la vie privée étant un sujet d'actualité de plus en plus important pour les citoyens, mettre en avant la prise en compte des règles de la protection des données permet de **garantir une image de sérieux et de fiabilité** auprès de la population qui se sentira plus en sécurité dans un monde où la vie privée est de plus en plus menacée

# Le RGPD à la loupe

- **Qu'est-ce qu'une donnée à caractère personnel ?**
  - Il s'agit d'une **information permettant d'identifier une personne physique** :
    - Un nom, un prénom, une adresse
    - Un numéro de téléphone, de sécurité sociale...
    - Des données GPS permettant de suivre les déplacements d'une personne (véhicules de service, etc.)
  - Mais ce peut être également des informations plus générales, voir sensibles, qui une fois regroupées au sein d'un fichier, vont permettre d'identifier une personne par recoupement d'informations :
    - Des données de santé
    - Des informations sur les habitudes de vies, la situation familiale ou le niveau de revenus
    - Des informations sur l'apparence physique (couleur des yeux, couleur de cheveux, tenue vestimentaire, etc.)



## Exemple :

*Martine, agent du service de l'urbanisme de sa Mairie, reçoit aujourd'hui une demande de permis de construire. Grâce aux plans annexés montrant une maison avec 4 chambres, 2 garages et une piscine, elle peut en déduire que la dame qui lui a apporté le dossier est mère de famille et bénéficie d'un train de vie confortable*



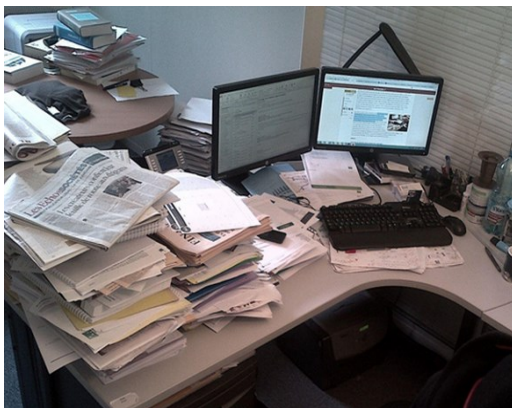
# Le RGPD à la loupe

- **On parle de traitements de données, qu'est-ce que c'est ?**
  - C'est tout simplement l'utilisation de ces données dans un but précis :
    - *Inscrire les enfants à l'école*
    - *Gérer les dossiers du personnel*
    - *Lister les personnes à inviter aux cérémonies*
    - *Etc.*



Un traitement peut résulter d'une obligation légale ! La loi peut vous imposer de traiter des données. Le RGPD vous impose alors seulement de mettre en place les mesures de sécurité appropriées

- **Petite précision utile :**



- Le RGPD n'est pas qu'un « truc d'informaticien »
- Le RGPD s'impose également aux données contenues dans les dossiers papier
- Ce qui compte dans un traitement, ce n'est pas le support (informatique ou papier), mais la donnée

# Le RGPD à la loupe

- **Le RGPD a été mis en place afin de lutter contre la multiplication des risques pesants sur notre vie privée :**
  - **La destruction, la perte ou le vol de données :** Certaines données étant nécessaires, le risque est de voir l'activité du service impactée sévèrement
  - **L'accès aux données par une personne malveillante :** Cette personne pourra alors les utiliser à son profit (démarchage abusif, voir chantage)
- Les objectifs des personnes malveillantes peuvent être multiples : simple défi, faire du profit (utilisation commerciale, chantage), militantisme politique...



## (Mauvais) exemple :

*Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Julien a cliqué sur un lien présent dans le message. Ce lien était piégé. Un virus s'est installé sur le serveur de la Mairie et a bloqué l'ensemble du système informatique, demandant une rançon en échange de la clé de déverrouillage.*

# Le RGPD à la loupe

- Les conséquences peuvent être dramatiques :
  - Perte de crédibilité pour la collectivité qui n'a pas su protéger les données de ses administrés
  - Atteinte à la réputation des administrés en cas d'atteinte à des données sensibles
    - *Cela peut conduire à des conséquences très graves (perte de travail, conflits familiaux ou de voisinage, suicide, etc.)*



## (Mauvais) exemple :

*Arthur a reçu un appel téléphonique d'une femme prétendant travailler pour la CAF. Celle-ci lui demandait des informations confidentielle sur les l'un des agents dont il s'occupe.*

*Pensant bien faire, et ne doutant pas de la parole de cette femme, Arthur lui a confié toutes les informations demandées. Quelques jours plus tard, l'agent a été victime d'une grave usurpation d'identité*

- Le RGPD prévoit donc des **sanctions** afin de responsabiliser les responsables des traitements de données :
  - Lourdes sanctions financières
    - *Jusqu'à 4% du budget ou 20 millions d'euros*
  - Lourdes sanctions pénales en cas d'infraction grave

# Les acteurs du RGPD

- **Le responsable de traitements**
  - Il s'agit de la personne qui détermine la finalité et les moyens du traitement de données à caractère personnel
  - C'est cette personne qui endossera seule l'entière responsabilité en cas de méconnaissance de la réglementation
  - Il s'agit de l'autorité territoriale (Maire/Président)



# Les acteurs du RGPD

- **Le délégué à la protection des données (DPD ou DPO)**
  - Personne désignée par l'autorité territoriale pour piloter la mise en conformité
  - Il conseille et informe le responsable de traitements sur ses obligations liées à la réglementation en matière de protection des données
  - Il effectue une veille juridique
  - Il contrôle le respect de la réglementation
  - Il peut être aidé dans sa mission par des référents dits « Informatique et Libertés » qui relayeront ses consignes et lui feront remonter toute information utile
- A noter que :
  - Le DPD n'a pas ni la légitimité, ni le pouvoir du responsable de traitements pour donner des ordres
  - Il n'est donc pas là pour « faire », mais pour conseiller

**Le délégué à la protection des données est obligatoire pour les collectivités territoriales et les établissements publics**



**Délégué à la protection  
des données**

# Les acteurs du RGPD

- **Les sous-traitants**

- Ce sont les personnes ou organisations publiques ou privées à qui le responsable de traitements va confier la gestion d'un ou plusieurs traitements de données
  - *Par exemple, un prestataire informatique, un photographe, un délégataire de service public...*
- Ces sous-traitants doivent présenter toutes les garanties nécessaires quant à leur propre respect des mesures du RGPD
  - *Le fait qu'ils traitent des données à la place du responsable de traitements **n'exonère pas** ce dernier de sa responsabilité en cas de défaillance*
  - *Le responsable de traitements doit donc s'assurer de confier ses données à un sous-traitant irréprochable*

- **Les tiers**

- Ce sont les organismes autorisés à accéder aux données sous certaines conditions :
  - *Administration fiscale*
  - *Administrations de justice, police ou gendarmerie*
  - *Huissiers de justice*
  - *Etc.*

# Les acteurs du RGPD

- **Les usagers**
  - Ce sont les personnes concernées par les traitements de données dans les collectivités territoriales et les établissements publics
  - Ces personnes disposent d'un certain nombre de droits dits « Informatique et Libertés » qu'il convient de respecter : droit à l'information, droit d'accès, de rectification des données...

Toutes ces obligations, ces risques, ces sanctions  
peuvent faire peur

**Mais pas d'inquiétude !**

Il existe une méthode simple, préconisée par la CNIL,  
pour se mettre en conformité avec le RGPD



# La mise en conformité par le Centre de Gestion

Pour vous aider dans cette lourde tâche, le Centre de Gestion du Gard propose une prestation dédiée à la mise en conformité au RGPD





## La mise en conformité par le Centre de Gestion



### Pour plus de renseignements :

Service « *Protection des données* »

Tél : 04 66 38 74 56

@ : [dpd@cdg30.fr](mailto:dpd@cdg30.fr)



### **Pour vous aider**

Le Centre de Gestion du Gard a mis en ligne des modèles de documents, de registres ainsi que divers guides de sensibilisation

**Pour plus d'informations, rendez-vous sur :**

[www.cdg30.fr](http://www.cdg30.fr)



# Les bons réflexes

<b>Sécurité physique</b>	<b>20</b>
<b>USB</b>	<b>21</b>
<b>Messagerie</b>	<b>22</b>
<b>Ingénierie sociale</b>	<b>23</b>
<b>Confidentialité</b>	<b>24</b>
<b>Poste de travail</b>	<b>25</b>
<b>Documents papier</b>	<b>26</b>
<b>Mots de passe</b>	<b>27</b>



# Sécurité physique

- Je veille à ne pas laisser des inconnus circuler dans les zones d'administration
- Je ne laisse pas les personnes extérieures sans surveillance
- Je ferme mon bureau à clef lorsque je n'y suis pas
- Je veille à fermer le bâtiment lorsque je le quitte
- J'active l'alarme du bâtiment lorsque je suis le dernier à partir



## (Mauvais) exemple :

*Patrick, en visite dans la collectivité, a réussi à se soustraire à la vigilance des agents de l'accueil. Impatient d'accéder à son dossier, il se rend dans le bureau le plus proche pour le chercher. Le bureau n'étant pas verrouillé, il peut entrer et accéder à tous les dossiers, y compris ceux qui ne le concernent pas.*

# USB

- Je m'abstiens de connecter à mon poste une clef USB dont je ne connais pas la provenance
- Lorsque je n'ai pas le choix, je demande à mon service informatique de lancer une analyse antivirus avant d'ouvrir la clef USB



## (Mauvais) exemple :

*Après avoir travaillé sur un document Word chez lui, Julien a voulu transférer celui-ci sur son poste professionnel.*

*Sans le savoir, son ordinateur personnel contenait un virus qui a infecté sa clef USB. Voilà maintenant qu'à son insu, le virus s'est copié sur le serveur de la collectivité.*

# Messagerie

- Je n'ouvre pas un courriel dont je ne reconnais pas l'expéditeur
- Je n'ouvre pas les pièces-jointes suspectes
- Je ne réponds pas à des demandes d'informations confidentielles par courriel
- Je contrôle l'identité et l'adresse du destinataire avant d'envoyer mon courriel
- J'indique de manière explicite l'objet du message et son caractère confidentiel



## (Mauvais) exemple :

*Suite à la réception d'un courriel semblant provenir d'un de ses collègues, Jean-Louis a cliqué sur un lien présent dans le message. Ce lien était piégé. Sans que Jean-Louis ne le sache, son ordinateur est désormais utilisé pour envoyer des courriels malveillants.*

- Lorsque j'envoie un courriel groupé, j'utilise le bon champs de destinataires :
  - **A** : destinataire du courriel
  - **CC** : autres destinataires mis en copie non-cachée
  - **Cci** : autres destinataires mis en copie cachée

# Ingénierie sociale

- Je ne me fie jamais aux apparences et je contrôle toujours l'identité de mes interlocuteurs, par courriel ou par téléphone
- Je ne donne jamais de renseignement sensible à quiconque sans m'être assuré de son identité au préalable



## (Mauvais) exemple :

*Arthur a reçu un appel téléphonique d'une femme prétendant travailler pour la CAF. Celle-ci lui demandait des informations confidentielle sur les l'un des agents dont il s'occupe.*

*Pensant bien faire, et ne doutant pas de la parole de cette femme, Arthur lui a confié toutes les informations demandées. Quelques jours plus tard, l'agent a été victime d'une grave usurpation d'identité*

# Confidentialité

- Je veille à la confidentialité des données que je manipule
- Je récupère rapidement les documents imprimés sur le matériel d'impression
- Je n'emporte pas de dossiers à la maison
- Je ne donne de renseignements qu'aux personnes ayant le droit d'y accéder
- Je range mon bureau régulièrement et je ne laisse pas trainer de documents à la vue de tous



## (Mauvais) exemple :

*En retard sur un dossier, Céline a fait une copie des données sur sa clef USB dans le but de terminer son travail chez elle. Le soir venu, sur le chemin du retour, elle ne se rend pas compte que sa clef USB est tombée de son sac. Les données sont donc perdues et à la merci de celui qui les retrouvera.*



## Poste de travail

- Je verrouille systématiquement mon poste de travail lorsque je m'en éloigne (même pour un court instant)
- Je n'installe pas de logiciel moi-même. Je demande à mon service informatique de le faire
- J'enregistre mon travail régulièrement sur un dossier réseau (et non sur le disque-dur) afin de s'assurer de la disponibilité des données en cas de défaillance du poste
- Je reste vigilant lorsque je navigue sur internet



**(Mauvais) exemple :**

*Après un long travail acharné, Emma se dit qu'une petite pause café lui ferait du bien. Elle laisse donc son ordinateur sans surveillance.*

*Ayant pu se soustraire à la surveillance des agents de l'accueil, Patrick a pu pénétrer dans son bureau en son absence et accéder à ses données informatiques, dont des dossiers sensibles.*

# Documents papiers

- Je veille à la protection des documents sensibles
- Je range mon bureau régulièrement et je ne laisse pas trainer de documents à la vue de tous
- Je procède à un tri régulier afin de déterminer quels documents me sont encore utiles et quels sont les documents à archiver
  - Je prends contact avec mon archiviste pour procéder au versement des documents à archiver vers le local dédié



## (Mauvais) exemple :

*Nadine reçoit un rendez-vous dans son bureau, malgré le désordre. Au cours de l'entretien, son téléphone portable sonne et elle sort donc du bureau pour répondre, laissant la personne reçue seule. Sans qu'elle ne s'en rende compte, son dernier bulletin de paie était resté visible de tous sur son bureau. Son rendez-vous avait donc accès, entre autres, à ses données bancaires, ses revenus et son numéro de sécurité sociale.*

# Mot de passe

- Je choisis un mot de passe complexe différent pour chaque usage que je change au moins une fois par an
  - Minimum 12 caractères, dont deux chiffres, deux majuscules, deux minuscules et deux caractères spéciaux
- Je ne communique jamais mon mot de passe à quiconque
- Je retiens mon mot de passe et je ne le note nulle part
- En cas d'oubli, je n'hésite pas à contacter mon service informatique pour que celui-ci m'en communique un nouveau



## **(Mauvais) exemple :**

*Afin de ne pas oublier son mot de passe, Corinne l'a noté sur un autocollant apposé sur son écran. Après avoir laissé son poste, pourtant verrouillé, pendant quelques minutes, elle se rend compte à son retour que quelqu'un a ouvert sa session et a pu accéder à des données sensibles.*



# Télétravail

<b>Sécurité physique</b>	<b>30</b>
<b>Sécurité informatique</b>	<b>31</b>
<b>Confidentialité</b>	<b>32</b>
<b>Poste de travail</b>	<b>33</b>
<b>Documents papier</b>	<b>34</b>



# Sécurité physique

- Je veille à ne pas laisser quiconque accéder à mon ordinateur professionnel
  - Dans la mesure du possible, j'installe mon bureau dans une zone isolée ou je puisse travailler tranquillement
- Je ferme mon bureau à clef lorsque je n'y suis pas
- Je veille à ranger l'ordinateur du mieux que possible (notamment s'il s'agit d'un ordinateur portable)
- Je ne laisse pas mes animaux s'approcher des documents ou du poste informatique



**(Mauvais) exemple :**

*Finissant son petit déjeuner, Emma, en télétravail depuis la veille, se décide à rejoindre son bureau ou l'attend son ordinateur.*

*Arrivant sur place, elle manque de lâcher sa tasse de café : l'écran de l'ordinateur est renversé, les dossiers papier éparpillés, tandis que son chat la regarde d'un œil curieux en baillant, tranquillement couché sur le clavier de cette nouvelle machine qu'il ne connaissait pas et avait très envie de découvrir.*

# Sécurité informatique

- J'utilise **uniquement** le poste informatique fourni par ma collectivité pour travailler
- Je ne me connecte au réseau interne de ma collectivité que grâce à un VPN
- Je ne connecte **jamais** mon matériel personnel avec mon matériel professionnel
- Je n'utilise que ma propre connexion internet (dont je suis responsable et sur laquelle j'ai seul la maîtrise) que j'ai préalablement sécurisé convenablement



## (Mauvais) exemple :

*Plus habitué à son ordinateur personnel sous Windows 7 qu'à son nouveau poste professionnel utilisant Windows 10, Julien préfère travailler sur son outil personnel. Devant transférer ses derniers travaux sur le serveur de sa collectivité, il se connecte à son réseau interne, sans prendre garde à l'absence de VPN sur son ordinateur.*

*Sans s'en rendre compte, il vient d'ouvrir l'accès à ce serveur aux cybercriminels qui avaient auparavant infectés son ordinateur personnel.*

# Confidentialité

- Je veille à la confidentialité des données que je manipule
- Je récupère rapidement les documents imprimés sur le matériel d'impression
  - Si je peux, j'installe l'imprimante à portée de main
- Je ne dévoile pas d'informations professionnelles à quiconque, y compris ma famille
- Je range mon bureau régulièrement et je ne laisse pas trainer de documents à la vue de tous



## (Mauvais) exemple :

*Recevant un samedi soir des voisins pour l'apéritif, Céline ne prend pas garde à la bonne tenue de son bureau. Après tout, ses invités resteront dans le salon !*

*Devant aller aux toilettes, Corinne s'isole un instant. Passant devant le bureau sur lequel traînent de nombreux dossiers, la tentation se fait trop grande ! Corinne aura ainsi tout le loisir de raconter le lendemain à ses copines que Monsieur Deloin, le gentil voisin du bout de la rue, a fait une demande d'aide sociale suite à la demande de divorce de sa femme.*



# Poste de travail

- Je verrouille systématiquement mon poste de travail lorsque je m'en éloigne (même pour un court instant)
- Je n'installe pas de logiciel moi-même. Je demande conseil à mon service informatique
- J'enregistre mon travail régulièrement sur un dossier réseau ET sur le disque-dur afin de s'assurer de la disponibilité des données en cas de défaillance du poste ou de la connexion avec le serveur
- Je reste vigilant lorsque je navigue sur internet



## (Mauvais) exemple :

*Patrick, épuisé après un long travail, décide de rejoindre sa cuisine pour se préparer un café.*

*Sans qu'il n'y fasse attention, son fils de 5 ans s'introduit dans son bureau et, voulant aider papa, commence à toucher à l'ordinateur qui n'avait pas été verrouillé.*

*A son retour, Patrick ne peut que constater, impuissant, que tout son travail avait été perdu.*

# Documents papiers

- Je veille à la protection des documents sensibles
- Je range mon bureau régulièrement et je ne laisse pas trainer de documents à la vue de tous
- Je ne conserve que les documents utiles et je rapporte les autres à mon bureau à la première occasion
- Je ne mange pas près de mes documents papier (ni près du poste informatique)



## (Mauvais) exemple :

*Nadine, très en retard sur un dossier, s'installe à midi dans une position précaire sur son canapé, son ordinateur portable sur les genoux afin de continuer à travailler tout en dégustant un plat cuisiné rapidement réchauffé au micro-ondes et posé sur le clavier. Lors d'un mauvais mouvement, elle a le malheur de renverser un peu de sauce sur les touches de l'ordinateur.*

*Prise de panique, et voulant rattraper sa maladresse, elle multiplie les gestes brusques et fini par renverser sa bouteille d'eau sur le dossier papier qui était posé sur sa table.*

## En cas de problème

- Je garde mon calme !
- Je prends contact avec le service informatique lorsque l'incident est de nature numérique
- Je prends contact avec le service « *Protection des données* » qui pourra m'orienter sur la marche à suivre

**Service « *Protection des données* » du  
Centre de Gestion du Gard**

**Tél :** 04 66 38 74 56


**@ :** [dpd@cdg30.fr](mailto:dpd@cdg30.fr)



# Pour aller plus loin

- **Commission Nationale de l'Informatique et des Libertés (CNIL)**

 : [www.cnil.fr](http://www.cnil.fr)

 : 01 53 73 22 22

⇒ Site de référence pour trouver des informations sur la protection des données. Permet également d'adresser une plainte en cas de mauvais usage de nos données personnelles

- **Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)**

 : [www.ssi.gouv.fr](http://www.ssi.gouv.fr)

⇒ Site regroupant toutes les informations utiles en lien avec la cybersécurité


- **Cybermalveillance**

 : [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

⇒ Site permettant de trouver des informations et de l'aide en cas d'acte de cybermalveillance

- **Commission d'Accès aux Documents Administratifs (CADA)**

 : [www.cada.fr](http://www.cada.fr)

 : 01 42 75 79 99

⇒ Site regroupant les informations sur la communicabilité des documents administratifs

- **@docs de France Archives**

 : [francearchives.fr/@docs/choix-thematique](http://francearchives.fr/@docs/choix-thematique)

⇒ Site permettant de déterminer les droits d'accès d'une personne aux documents publics

# Pour aller plus loin

- **SecNum Académie**

🖥️ : [secnumacademie.gouv.fr](https://secnumacademie.gouv.fr)

⇒ Formation en ligne gratuite et ouverte à tous niveaux permettant de s'initier à la cybersécurité

- **DATAK**

🖥️ : [www.datak.ch](http://www.datak.ch)

⇒ Petit jeu libre sur navigateur internet permettant de se familiariser avec la protection des données personnelles

- **Educnum**

🖥️ : [www.educnum.fr](http://www.educnum.fr)

⇒ Site d'information et de sensibilisation à la culture numérique et à la sécurité des données personnelles

- **Framasoft**

🖥️ : [framsoft.org](http://framsoft.org)

⇒ Annuaire de logiciels libres

