LES BONS GESTES

Dans le cadre de ses missions, une collectivité est amenée à traiter et à gérer de nombreuses données personnelles (Noms, prénoms, adresses, numéros de téléphone, données de carrière, situation familiale, données concernant la santé, etc.).

Face à la multiplication des menaces, notamment informatique, qui pèsent aujourd'hui sur ces données, il est de la responsabilité de chacun de prendre les précautions qui s'imposent pour en garantir la sécurité.

Pour rappel, le devoir de confidentialité fait parti des obligations des fonctionnaires imposé par les articles L.121-6 (secret professionnel) et L.121-7 (discrétion). Le non respect de ce devoir peut ainsi faire l'objet d'une sanction disciplinaire.

La sécurité physique

- ✓ Je veille à ne pas laisser des inconnus circuler dans les zones d'administration, et 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 et j'en active l'alarme lorsque je suis le dernier à partir

(Mauvais) exemple :

Pierre, 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.

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

SERVICE
PROTECTION DES DONNÉES

La sécurité informatique

- ✓ Je n'utilise pas ma messagerie personnelle (qui est généralement moins bien sécurisée) pour l'exercice de mes missions professionnelles
- ✓ Je ne connecte **jamais** mon matériel personnel sur mon matériel professionnel (clé USB, smartphone, etc.)
- ✓ Je n'ouvre pas les mails dont je ne reconnais pas l'expéditeur et je n'ouvre jamais les pièces-jointes suspectes
- ✓ Je ne répond pas à des demandes d'informations confidentielles par mail et je contrôle l'identité du destinataire avant d'envoyer mes mails
- ✓ Lorsque j'envoi mes mails, j'utilise les bons champs de destinataires :
  - **A :** destinataire du mail
  - **Cc :** autres destinataires mis en copie non cachée
  - **Cci :** autres destinataires mis en copie cachée

(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.

L'ingénierie sociale

- ✓ Je ne me fie jamais aux apparences et je contrôle toujours l'identité de mes interlocuteurs, que ce soit par mail, par téléphone, ou même en face à face !
- ✓ 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.

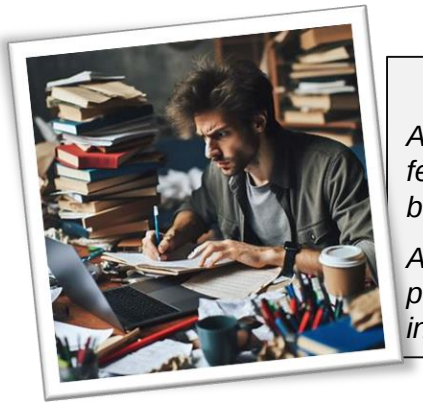
Pensant bien faire, et ne doutant pas de la parole de cette femme, Arthur lui a confié toutes les informations demandées. Quelques jours plus tard, l'agent a été victime d'une grave usurpation d'identité.

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

La sécurité du poste de travail

SERVICE
PROTECTION DES DONNÉES

- ✓ Je verrouille systématiquement mon poste de travail lorsque je m'en éloigne (même pour un court instant) aux moyens des touches ⊞ + L
- ✓ Je n'installe pas de logiciel moi-même. Je demande conseil à mon service (ou prestataire) informatique
- ✓ J'enregistre mon travail régulièrement sur un dossier réseau 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, Audrey se dit qu'une petite pause café lui ferait du bien. Elle laisse donc son ordinateur sans surveillance et son bureau ouvert.

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

La sécurité des dossiers et documents papier

- ✓ Je veille à la protection des documents sensibles par la non-transmission aux destinataires non-autorisés ainsi que par leur conservation dans des armoires et tiroirs fermés à clef
- ✓ Je range mon bureau régulièrement et je ne laisse pas traîner 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.

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86

La confidentialité des données

SERVICE
PROTECTION DES DONNÉES

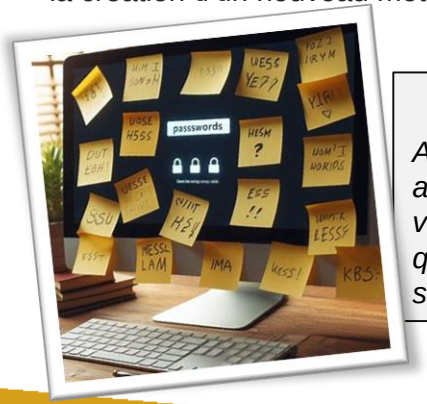
- ✓ Je veille à la confidentialité des données que je manipule
- ✓ Je récupère rapidement les documents imprimés sur le matériel d'impression
- ✓ Je détruis les documents à l'aide du broyeur lorsque cela est nécessaire
- ✓ Je n'emporte pas de dossiers à la maison, sauf exception du télétravail, et en veillant à leur chiffrement s'il s'agit de données sensibles
- ✓ Je veille à utiliser les bons outils pour assurer l'échange sécurisé des données et des documents (messageries et plateformes sécurisées hébergées sur le territoire français).

(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.

Les mots de passe

- ✓ Je choisis un mot de passe sécurisé différent pour chaque usage et composé au moins de **14 caractères** dont **un chiffre**, **un lettre majuscule**, **un lettre minuscule** et **un caractère spécial**.
- ✓ Je ne réutilise pas les mots de passe de mes comptes personnels pour les comptes professionnels
- ✓ Je ne communique jamais mon mot de passe à quiconque
- ✓ Je retiens mon mot de passe et je ne le note pas sur un papier facilement accessible à d'autres personnes (et surtout pas sur un autocollant collé sur l'écran !)
- ✓ En cas d'oubli, je n'hésite pas à contacter mon service informatique pour que celui-ci m'aide dans la création d'un nouveau mot de passe



(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.

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU GARD
Service « Protection des données »
183 chemin du Mas Coquillard – 30 900 NIMES
dpd@cdg30.fr
04 66 38 86 86