RGPD
Coronavirus et Télétravail

CONTEXTE

En raison du confinement imposé par la règlementation dans le cadre de la pandémie au COVID-19, certains agents sont conduits à télétravailler.
Ils doivent ainsi accéder aux serveurs, applications et données depuis leur domicile, à partir de leur poste professionnel ou personnel.

Afin de pouvoir poursuivre aisément son activité à distance et éviter certains risques, voici quelques conseils, bonnes pratiques et mesures de sécurité.

CONSEILS ET BONNES PRATIQUES D'INSTALLATION

Physiques :

- ⇨ Adapter un environnement différent de celui de votre bureau professionnel.
- ⇨ Veiller à ne pas être dérangé par la présence de tiers (conjoint, enfants, visiteurs, …)
- ⇨ Distinguer le temps et l'espace de travail entre vie professionnelle et vie privée (bureau, horaires, pauses, planning, ...).
- ⇨ S'assurer que les autres personnes du domicile n'accéderont pas aux documents papiers et documents numériques (pièce fermée à clé / stockage verrouillable...)
- ⇨ Maintenir le relationnel et le contact avec les collègues en utilisant tous les outils de communication mis à disposition : mails, tchats, documents partagés, visioconférence, outils de travail collaboratif, agenda partagé (un support d'aide à l'utilisation des outils d'information et de communication fourni par l'employeur est souhaitable).
  -> Ne pas sombrer dans l'isolement : compte tenu de la situation exceptionnelle de confinement. Le fait de ne plus aller sur le lieu de travail et d'y retrouver ses collègues peut rendre le sentiment d'isolement amplifié par les difficultés matérielles rencontrées avec l'utilisation des technologies de communication et le caractère anxiogène de la situation.
- ⇨ Réguler son activité et en assurer le suivi afin de faire face à cette situation nouvelle et inconnue. Celle-ci peut générer aussi bien de l'hyper-connexion au travail du fait des nombreuses sollicitations, du besoin ressenti de se rendre utile et de ne pas se faire oublier que de l'inaction par défaut de concentration.
- ⇨ En pratique, ne jetez aucun document papier dans la poubelle sans les avoir auparavant anonymisés et déchiquetés.

Informatiques :

- ⇨ Afin d'optimiser ses connexions, placer sa box au centre du logement, dans un endroit dégagé et de préférence surélevé. Limiter les obstacles (murs épais, meubles, pièce éloignée, …) entre le Wi-Fi et l'ordinateur ou appareils nomades. Il est également recommandé de laisser un espace d'environ deux mètres entre la box et les autres équipements à émission d'ondes tels que : base de téléphone sans fil, babyphone, micro-ondes…

Attention, les usages simultanés de visioconférence et visionnage d'une bande dessinée par les enfants, streaming, …) sont consommateurs de bande passante. Idem pour les plateformes (YouTube, Netflix…) qui, si elles utilisent des mécanismes d'optimisation de vos réseaux privés virtuels (VPN), réduiront ce débit VPN pour l'exercice de votre activité principale.

En cas de difficulté, prévoir de connecter son ordinateur directement à la box avec un câble Ethernet ou utiliser la 4G mobile de son smartphone ou contacter l'administrateur qui a pour mission d'assurer le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de vos matériels professionnels. Il a accès aux logs de connexion et aux adresses IP de tout ou partie d'équipement (professionnel ou personnel) se connectant aux serveurs du service.

QUELS SONT LES RISQUES DANS LE CADRE DE LA PROTECTION DES DONNEES ?

Ce contexte de connexion et d'utilisation du matériel à distance fait peser un risque sur le fonctionnement, la sécurité et l'intégrité du système d'information, ainsi que sur la sécurité des données traitées dans le cadre de l'activité, qu'elles soient à caractère personnel ou non, sensibles ou pas.

Exemple : si vous avez à traiter de données médicales, vous devrez faire preuve de la plus grande vigilance possible concernant leur protection et veiller à ce que des tiers non autorisés n'aient pas connaissance de telles données (famille, visiteurs, …).

⇨ Ne pas communiquer des données médicales via la messagerie personnelle, les réseaux sociaux ou au moyen de plateformes de stockage en ligne, ces supports n'étant pas sécurisés.

QUELLES MESURES DE SECURITE METTRE EN PLACE ?

⇨ Utilisez un mot de passe fort pour vous connecter à votre session - Ne le divulguer à aucune autre personne, même au sein de votre famille - Eviter les post-it.

⇨ N'oubliez pas que vous êtes soumis, même en télétravail, à la charte informatique de votre collectivité, si elle existe.

⇨ Si possible, utiliser le VPN ou une Box dédiée pour accéder au réseau de la collectivité.

⇨ Prévoir le verrouillage automatique du poste, tous les quarts d'heure par exemple, et le verrouiller à chaque éloignement de l'ordinateur (touches Windows et L).

⇨ Eviter la copie de fichiers professionnels sur du matériel personnel.

⇨ Détruire les documents lorsqu'ils ne sont plus nécessaires.

⇨ Sauf en cas de réelle nécessité, ne pas sauvegarder de données professionnelles sur un cloud personnel, sauvegarder les documents contenant des informations confidentielles et/ou des données à caractère personnel uniquement sur les serveurs.

⇨ Ne pas télécharger d'applications sans l'accord et sous le contrôle de votre hiérarchie sur vos matériels professionnels.

⇨ Ne pas utiliser de clés USB en-dehors de celles éventuellement attribuées par la collectivité.

⇨ Ne jamais laisser l'ordinateur fixe ou nomade sans surveillance, sur une longue période, que ce soit à l'intérieur de la maison ou à l'extérieur 'dans un véhicule par exemple le temps d'une course)

- ⇨ Si vous possédez un assistant vocal veiller à le débrancher en cas de discussion professionnelle par téléphone ou visioconférence.
- ⇨ Attention au risque de phishing (demande de virement "urgent" ou de « reset » de mot de passe ou d'envoi de documents) => Penser à bien vérifier l'identité du demandeur et ne pas cliquer sur des liens malveillants.
- ⇨ Informer, sans délai, votre autorité de tout dysfonctionnement, altération, perte, vol, destruction et autre évènement pouvant affecter les moyens informatiques et de communication électronique et votre DPD en cas de perte ou de vol de données personnelles.

Attention, en cas d'utilisation de son matériel personnel, des règles complémentaires de sécurité doivent s'appliquer :

- ⇨ S'assurer du bon fonctionnement et du bon état de santé du matériel personnel utilisé (antivirus, mise à jour, etc.)
- ⇨ Ne pas se connecter sur des réseaux sans-fils libres type « hotspot » (lieux publics, gares, ...), réseaux non fiables de par leur nature.

POUR ALLER PLUS LOIN

*** Sécuriser ses données personnelles**

La Commission nationale de l'information et des libertés (CNIL), rappelle les moyens de sécuriser vos données, même en télétravail.
https://www.cnil.fr/fr/salaries-en-teletravail-quelles-sont-les-bonnes-pratiques-suivre
https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mettre-en-place-du-teletravail

*** Se protéger de la cybermalveillance**

Le gouvernement rappelle que la cybermalveillance, n'est pas, elle, en confinement et donne 10 recommandations pour télétravailler en toute sécurité.
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

* **ANSSI** (Agence nationale des systèmes d'information)

* **ARCEP** (Autorité de régulation des communications électroniques et des postes)

* **INRS** : "Le télétravail en situation exceptionnelle" http://www.inrs.fr/risques/teletravail-situation-exceptionnelle/ce-qu-il-faut-retenir.html

* **Ministère de l'action et des comptes publics** :
https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=B1BD183E-6E4B-4FE5-B6AE-608C763442B1&filename=COVID%2019%20-%20Questions-r%C3%A9ponses%20employeurs%20et%20agents%20publics.pdf

* **SOFAXIS** : Fiches 1 & 2 Covid19 - Télétravail

* **CDG 61** : Guide « Travail sur écran »
https://www.cdg61.fr/file_manager_download.php?id=818

CONTACT/INFORMATION

Délégué à la protection des données - 2, rue François Arago – 61250 Valframbert
0233804811 - rgpd@cdg61.fr / www.cdg61.fr