# Télétravail : quelles sont les bonnes pratiques de sécurisation des données à adopter ?

## Novembre 2020

Le 29 octobre dernier, le gouvernement a durci le ton sur le recours au télétravail en annonçant que ce dernier, loin d'être une simple « option », était désormais « une obligation » et qu'il devait être porté à 100 % pour les activités compatibles.

Parmi les difficultés pratiques que sa mise œuvre suscite, le télétravail constitue un véritable challenge en matière de protection des données personnelles des salariés, et contraint les entreprises à renforcer les mesures techniques et organisationnelles afin de garantir la sécurité des traitements et des échanges.

En effet, ce mode d'organisation à distance doit nécessairement être encadré et s'accompagner de mesures de sécurité renforcées afin de garantir la sécurité des systèmes d'information et des données traitées à distance par les collaborateurs de l'entreprise.

Afin d'accompagner les entreprises dans la mise en place du télétravail et leurs démarches de sécurisation des données personnelles, la CNIL a publié une série de recommandations en avril dernier. **La sécurité informatique et l'adoption de bonnes pratiques en matière de cybersécurité sont indispensables au déploiement par l'employeur du télétravail**.

Rappelons que la mise en place du télétravail, de la sécurité des données et des systèmes d'informations relève de la **responsabilité de l'entreprise**, en sa qualité de **responsable de traitement**.

**Check liste des recommandations de la CNIL** sur les mesures qui doivent être prises concrètement par les entreprises afin de sécuriser les données traitées en télétravail, les consignes de sécurité, et recommandations à prodiguer aux salariés :

### QUELLES SOLUTIONS DOIVENT ETRE DEPLOYEES PAR LES ENTREPRISES ?

#### Edicter des pratiques et des consignes claires :

– Communiquer aux salariés une charte de sécurité informatique intégrant les règles à suivre dans le cadre du télétravail et détaillant notamment les règles de protection des données ainsi que les sanctions encourues en cas de non-respect de celles-ci. Il est par ailleurs recommandé de conférer à cette charte une force contraignante (ex. en l'annexant au règlement intérieur). Dans certaines circonstances, la violation par le salarié des recommandations de cette charte, pourra justifier une sanction disciplinaire pouvant aller jusqu'au licenciement (ex : Cour d'appel, Limoges, Chambre sociale, 4 Février 2019 – n° 17/01419).

*=> A ce titre, avez-vous mis à jour la charte informatique de votre entreprise sur ce point ?*

– Mettre à disposition des salariés une liste d'outils de communication et de travail collaboratif appropriés au travail à distance, garantissant la confidentialité des échanges et des données partagées.

➔ En particulier, il est fréquent en télétravail d'utiliser des outils de discussion et de visioconférence. La CNIL a ainsi publié le 9 avril dernier une communication destinée à prévenir des risques que peuvent comporter ces outils lorsqu'ils n'offrent pas les garanties de protection suffisantes. La CNIL recommande notamment de :

✓ utiliser des applications pour lesquelles l'éditeur indique clairement comment les données traitées sont réutilisées (dans l'application elle-même ou sur son site web, par exemple) ;

✓ lire les commentaires des utilisateurs relatifs à ces applications ;

✓ vérifier que l'éditeur a mis en place des mesures de sécurité essentielles, comme le chiffrement des communications de bout en bout.

**Rappel : l'utilisation dans le cadre du télétravail de ces outils de communication et de vidéo-conférence, ainsi que la sécurité des données traitées via ces outils, relève de la responsabilité de l'entreprise, en sa qualité de responsable de traitement.**

### Préparation des postes de travail

Equiper les postes de travail des salariés d'un pare-feu, d'un anti-virus et d'un outil de blocage de l'accès aux sites malveillants.

Mettre en place un VPN (Virtual Private Network) pour éviter l'exposition directe de vos services sur Internet.

## QUELLES SONT LES RECOMMANDATIONS A TRANSMETTRE A VOS SALARIES ?

### Utilisation des appareils fournis et contrôlés par l'entreprise

Il est recommandé de favoriser leur utilisation et ainsi de :

- sensibiliser les salariés sur la nécessité d'utiliser autant que possible le VPN mis à disposition par l'entreprise ;
- privilégier l'échange de données à travers les stockages disponibles depuis le VPN plutôt que par la messagerie électronique ;
- se connecter au moins une fois par jour au VPN de l'entreprise pour appliquer les mises à jour ;
- désactiver le VPN uniquement lorsque le salarié utilise des services consommateurs de bande passante, comme le streaming vidéo, qui ne nécessitent pas de passer par le réseau de son entreprise.

### Attention à l'usage d'appareils et d'équipements personnels !

L'entreprise doit s'assurer que soit mis en en œuvre par les salariés :

- ✓ l'installation d'un antivirus et d'un pare-feu ;
- ✓ l'utilisation d'un compte personnel avec des droits limités, protégé par un mot de passe fort et non partagé avec d'autres personnes ;
- ✓ la mise à jour régulière du système d'exploitation et des logiciels utilisés, notamment le navigateur web et ses extensions ;
- ✓ la sauvegarde régulière du travail réalisé de préférence sur les infrastructures de l'entreprise.

De la même façon, si les salariés utilisent leurs téléphones mobiles personnels, il est nécessaire :

- ✓ d'éviter d'y enregistrer des informations confidentielles : codes secrets, codes d'accès, coordonnées bancaires, etc. ;
- ✓ d'activer le code PIN du téléphone et de mettre en place un délai de verrouillage automatique du téléphone ;
- ✓ d'activer le chiffrement des informations sur leur téléphone lorsque c'est possible ;
- ✓ de noter le numéro « IMEI » du téléphone pour le bloquer en cas de perte ou de vol ;
- ✓ de n'installer des logiciels que depuis les plateformes officielles et d'éviter les applications de sources inconnues**.**

### Sécuriser et protéger vos données : rôle de formation de l'entreprise à l'égard de ses salariés

**L'accès et la protection de vos données passe par la création d'un mot de passe qui ne puisse pas être piraté :**

Vous pensez avoir un mot de passe robuste ? Faites le test de la CNIL et vérifiez ici si vous êtes dans les standards de sécurité et de robustesse attendus : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide.

### Savoir identifier les tentatives d'hameçonnage : prévention et formation

Les salariés doivent être vigilants en cas de contact avec :

- ✓ des personnes que le salarié ne connait pas, en particulier si l'émetteur invite le salarié à cliquer sur des liens ou à ouvrir un fichier ;
- ✓ une personne connue envoyant au salarié une communication inhabituelle. Cette information doit alors être vérifiée par un autre canal (téléphone, SMS, mail) ;
- ✓ des personnes cherchant à créer un sentiment d'urgence ou de danger. Le cas échéant, il est nécessaire de toujours utiliser un autre canal pour vérifier les informations communiquées.

### Assurer la sécurité des communications.

Éviter de transmettre des données confidentielles via des services grand public de stockage, de partage de fichiers en ligne, d'édition collaborative ou via des messageries ;

Privilégier des outils de communication chiffrés, si l'entreprise ne fournit pas d'outils de communication sécurisé et éviter les applications gratuites qui offrent peu de garanties en termes de sécurité.

**Enfin, rappelons que l'ANSSI (Agence nationale de la sécurité des systèmes d'information) recommande la désignation d'un correspondant/référent pour la sécurité informatique de chaque entreprise. Cette désignation est indispensable pour coordonner la sécurité informatique de votre entreprise, et le déploiement sécurisé du télétravail.**

## QUELS AUTRES IMPERATIFS L'EMPLOYEUR DOIT-IL PRENDRE EN COMPTE ?

Le télétravail, bien que se déployant en dehors de l'enceinte de l'entreprise, ne pourra valablement être exercé que dans le respect de plusieurs libertés individuelles fondamentales des salariés telles que le droit au respect de la vie privée ou le secret des correspondances. Ce raisonnement s'applique également dans le cadre d'une démarche de sécurisation des données liée au télétravail.

Comme rappelé par le Ministère du travail dans son questions-réponses relatif au télétravail, actualisé au 10 novembre dernier, aucun dispositif ne doit ainsi conduire à une surveillance constante et permanente de l'activité du salarié.

A titre d'illustration, les « keyloggers » qui permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur sont considérées, sauf circonstance exceptionnelle liée à un fort impératif de sécurité strictement encadré, comme illicite par la CNIL.

## QUELS ACTEURS L'EMPLOYEUR PEUT-IL ASSOCIER DANS SA DEMARCHE DE PROTECTION DES DONNEES ?

La mise en place de mesures et recommandations visant à sécuriser les données personnelles des salariés implique une certaine horizontalité permettant d'associer les divers interlocuteurs de l'employeur au sein de l'entreprise.

Parmi ces interlocuteurs privilégiés, on retrouve, en premier lieu, les représentants du personnel.

En effet, ces mesures et leur gestion seront plus à même d'être comprises et moins susceptibles d'être remises en cause après validation des institutions représentatives.

A ce titre, une information de ces interlocuteurs permettrait de les intégrer à la démarche de sécurisation des données tout en les sensibilisant aux enjeux liés à cette dernière.

En outre, lorsque l'entreprise en est dotée, le délégué à la protection des données (DPO), dès lors que son rôle est principalement d'informer et de conseiller le responsable de traitement ainsi que ses salariés sur la protection des données, devra nécessairement être amené à collaborer avec l'employeur sur les mesures à prendre en la matière.

## QUELLES SONT LES PRINCIPALES SANCTIONS AUXQUELLES L'EMPLOYEUR S'EXPOSE EN CAS DE CARENCE ?

Comme évoqué, l'employeur, en tant que responsable du traitement des données, est astreint à une obligation de sécurité. Cette dernière n'est pas conçue de manière théorique dans la législation.

En effet, l'absence de précautions concernant la sécurité des informations relatives aux salariés est passible d'une sanction pénale de cinq ans d'emprisonnement et de 300 000 euros d'amende.

En outre, un manquement de l'employeur à ses obligations est passible de sanctions prononcées par la CNIL pouvant aller du simple rappel à l'ordre à une amende administrative.

***

**Assurer la sécurité des données dans le cadre d'un télétravail généralisé est un enjeu majeur pour les entreprises.**

**Les avocats de Grant Thornton Société d'Avocats en droit social et droit des données personnelles, ainsi que les experts Informatiques de Grant Thornton, restent pleinement mobilisés et à votre disposition pour vous accompagner et vous conseiller dans la mise en œuvre de l'ensemble de ces actions.**

## Contacts


**Caroline Luche-Rocchia**
Avocat - Associée
**E** : CLuche-Rocchia@avocats-gt.com
**T** : +33 1 41 16 27 37

**Alexis Grin**
Associé – IT Risk Services
**E** : Alexis.Grin@fr.gt.com
**T** : +33 1 41 25 91 64

**Nicolas Rémy-Neris**
Avocat, Directeur
**E** : NRemyNeris@avocats-gt.com
**T** : +33 1 41 16 27 25

**Pauline Garcia**
Avocat
**E** : PGarcia@avocats-gt.com
**T** : +33 1 41 16 27 45

**Islem Berkani**
Avocat
E: IBerkani@avocats-gt.com
T: +33 1 41 16 27 40

**Grant Thornton Société d'Avocats**
29, rue du Pont
92200 – Neuilly-sur-Seine, France
www.avocats-gt.com


***À propos de Grant Thornton Société d'Avocats***
*Grant Thornton Société d'Avocats accompagne ses clients dans toutes leurs opérations stratégiques, que ce soit dans un contexte national ou international, grâce à une expertise pluridisciplinaire reconnue dans tous les domaines du droit des affaires.*


NOTE : Cette note d'alerte est de nature générale et aucune décision ne devrait être prise sans davantage de conseil. Grant Thornton Société d'Avocats n'assume aucune responsabilité légale concernant les conséquences de toute décision ou de toute mesure prise en raison de l'information ci-dessus. Vous êtes encouragés à demander un avis professionnel. Nous serions heureux de discuter avec vous de l'application particulière des changements à vos propres cas

© 2020 Grant Thornton Société d'Avocats, Tous droits réservés. Grant Thornton Société d'Avocats est le cabinet d'avocats lié au réseau Grant Thornton en France, dont la société SAS Grant Thornton est le membre français du réseau Grant Thornton International Ltd (GTIL). "Grant Thornton" est la marque sous laquelle les cabinets membres de Grant Thornton délivrent des services d'Audit, de Fiscalité et de Conseil à leurs clients et / ou, désigne, en fonction du contexte, un ou plusieurs cabinets membres. GTIL et les cabinets membres ne constituent pas un partenariat mondial. GTIL et chacun des cabinets membres sont des entités juridiques indépendantes. Les services professionnels sont délivrés par les cabinets membres, affiliés ou liés. GTIL ne délivre aucun service aux clients. GTIL et ses cabinets membres ne sont pas des agents. Aucune obligation ne les lie entre eux.