TaylorWessing

Télétravail et données personnelles

Vademecum

Juin 2020

« *Le télétravail désigne toute forme d'organisation du travail dans laquelle un travail qui aurait également pu être exécuté dans les locaux de l'employeur est effectué par un salarié hors de ces locaux de façon volontaire en utilisant les technologies de l'information et de la communication* »[1].

Dans le contexte d'urgence créé par la crise sanitaire, les entreprises ont dû s'équiper d'outils logiciels de télétravail sans évaluer ou encadrer leur mise en place, faute de temps.

Or, la mise en place de tels outils implique le respect de règles applicables non seulement en matière de droit du travail (détaillées dans notre guide dédié à ce sujet) mais également en matière de données personnelles.

La sécurité des systèmes d'information et le respect de la vie privée des salariés sont en effet des éléments clé de la mise en place des outils de télétravail.

Pour vous accompagner dans la mise en place ou la mise à niveau de vos outils logiciels de télétravail, nous vous proposons une méthodologie en deux étapes.

Sommaire

[1] L. 1222-9 du Code du travail.

Etape 1 : Analyse et évaluation des outils

1.1 Contrôle de proportionnalité du traitement

Les outils de télétravail impliquent des traitements de données personnelles des salariés de l'entreprise.

Conformément au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (le RGPD), **pour être licite, tout traitement de données doit être proportionné,** c'est-à-dire respecter les principes suivants :

- **Finalités limitées :** les données personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes ;
- **Données limitées :** les données personnelles traitées doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ;
- **Durée de conservation limitée :** les données doivent être conservées pendant une durée n'excédant pas celle nécessaire au regard des finalités ;

En pratique, l'employeur doit, pour chaque nouvel outil informatique, **analyser les traitements de données personnelles** impliqués par l'utilisation d'un tel outil afin de s'assurer de leur proportionnalité (Cf. Fiche F3). C'est l'un des aspects du principe de Privacy by Design.

Dans certains cas, **le RGPD impose de documenter cette analyse.**

- Les **traitements susceptibles d'engendrer un risque élevé** pour les droits et libertés des personnes concernées doivent faire l'objet d'une Analyse d'Impact relative à la Protection des Données (AIPD) (Cf. Fiche F2) ;
- **Lorsqu'un traitement est fondé sur l'intérêt légitime** du responsable de traitement, (ce qui sera la plupart du temps le cas pour les traitements de données personnelles de salariés en matière de télétravail (Cf. fiche F1)), le responsable du traitement doit effectuer un test de balance des intérêts en question et des droits et libertés des personnes concernées.

Dans tous les autres cas, nous recommandons aux responsables de traitement de documenter également cette analyse à titre de bonne pratique.

F1. Consentement & salariés

Le consentement n'est pas une base légale envisageable pour les traitements de données relatifs au télétravail.

Pour rappel, Si un traitement de données peut reposer sur le recueil du consentement de la personne concernée, celui-ci n'est valable que s'il est notamment donné librement, ce que la CNIL estime ne pas être le cas dans le cadre de la relation employeur salarié en raison du lien de subordination existant.

F2. Comment déterminer si un traitement doit faire l'objet d'une AIPD ?

Une AIPD est requise si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

L'évaluation d'un tel risque peut se faire de deux manières :

- ✓ Soit, le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une AIPD[1].
- ✓ A noter que cette liste prévoit que les « *traitements ayant pour finalité de surveiller de manière constante l'activité des employés concernés* » doivent obligatoirement faire l'objet d'une AIPD.
- ✓ Soit, le traitement remplit au moins deux des neuf critères listés dans les lignes directrices de l'EDPB[2]. A noter que ces critères comprennent (i) la surveillance systématique, (ii) l'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles et (iii) les traitements de données concernant des personnes vulnérables comme c'est le cas pour les traitements de données de salariés.

F.3 Attention à la surveillance excessive des salariés !

Le télétravail peut inciter l'employeur à installer des outils sur l'ordinateur de ses salariés dans le but de contrôler leur activité. Comme tout traitement de données personnelles, cette surveillance et les traitements en résultant doivent être proportionnés.

L'employeur peut contrôler et restreindre les outils informatiques mis à disposition de ses salariés (internet, messagerie, etc.) afin de limiter les risques d'abus d'une utilisation trop personnelle de ses outils (ex : consultation de sa messagerie personnelle, achats de produits en ligne, discussions sur les réseaux sociaux, etc.) mais ce contrôle ne doit pas être excessif ou illicite.

A ce titre, la CNIL pose les règles suivantes :

- ✓ l'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés ;
- ✓ l'enregistrement à distance de toutes les actions accomplies sur un ordinateur (« keylogger ») n'est possible qu'en cas de circonstance exceptionnelle liée à un fort impératif de sécurité ;
- ✓ les logs de connexion ne doivent pas être conservés plus de 6 mois.

La question de la surveillance des salariés se pose d'autant plus lorsque l'employeur a préconisé l'utilisation du matériel informatique personnel du salarié (« *Bring Your Own Device* »).

Dans ce cas, la CNIL rappelle que l'employé ne peut pas prévoir de mesures ayant pour effet d'entraver l'utilisation d'un équipement (ordinateur ou smartphone) dans un usage privé, au motif que cet équipement est susceptible d'être utilisé pour accéder au système informatique de l'entreprise. De la même manière, un employeur ne peut accéder ou encore s'arroger le droit d'effacer à distance des éléments relevant de la vie privée stockés sur l'équipement en question.

[2] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf

[3] https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

1.2 Revue des contrats conclus avec les prestataires fournissant les outils de télétravail

Quel contrat en matière de données personnelles ?

Dans le cadre de sa prestation de service, le prestataire fournissant l'outil peut être amené à traiter des données personnelles de salariés de l'entreprise.

En fonction de la qualification des parties, plusieurs types de contrat encadrant les traitements de données effectués par le prestataire doivent être conclus conformément au RGPD.

- **Cas de figure 1 : Le prestataire traite au nom et pour le compte de l'employeur les données personnelles des salariés et selon ses instructions.**

  Dans ce cas, le prestataire est qualifié de « sous-traitant » de l'employeur, lequel agit comme « responsable de traitement » au sens du RGPD.

  L'employeur et le prestataire doivent alors conclure **un contrat de sous-traitance de données personnelles** comportant l'ensemble des mentions prévues à l'article 28 du RGPD (Cf. Fiche F4).

- **Cas de figure 2 : L'employeur et le prestataire déterminent conjointement les finalités et les moyens du traitement de données concerné.**

  Dans ce cas, l'employeur et le prestataire sont qualifiés de « co-responsables de traitement ».

  Ils doivent alors conclure **un contrat de co-responsabilité** qui définit de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences de la législation applicable, conformément à l'article 26 du RGPD (Cf. Fiche F5).

- **Cas de figure 3 : Le prestataire traite les données personnelles pour son propre compte, c'est-à-dire qu'il détermine seul les finalités et les moyens du traitement.**

  Dans ce cas, le prestataire agit comme « responsable de traitement » au sens du RGPD pour ses propres finalités, au même titre que l'employeur.

  Si le RGPD n'impose pas la conclusion d'un contrat spécifique, nous recommandons dans ce cas de conclure **un contrat de partage de données** pour encadrer l'utilisation des données collectées via l'outil par le prestataire pour son propre compte (Cf. Fiche F6).

F4. Clauses à insérer dans un contrat de sous-traitance de données personnelles

Caractéristique du traitement objet de la sous-traitance : Objet, durée, finalités, types de données traitées, catégories de personnes concernées.

Les droits et obligations des parties et en particulier du sous-traitant qui (article 28 du RGPD) :

- ✓ ne doit pas traiter les données personnelles en dehors des instructions du responsable du traitement ;
- ✓ doit veiller à ce que les personnes autorisées à traiter les données s'engagent à en respecter la confidentialité ou soient soumises à une obligation légale de confidentialité ;
- ✓ prend les mesures de sécurité appropriées conformément à l'article 32 du RGPD ;
- ✓ ne recrute un sous-traitant ultérieur qu'avec l'autorisation écrite préalable du responsable de traitement et s'engage à conclure avec le sous-traitant ultérieur un contrat prévoyant les mêmes obligations que celles prévues au contrat qu'il a conclu avec le responsable de traitement ;
- ✓ doit assister le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice de droit adressées par les personnes concernées ;

- ✓ doit assister le responsable de traitement dans le respect de ses obligations en matière de sécurité, de notification à l'autorité compétente et/ou aux personnes concernées en cas de violation de données, de conduite d'analyse d'impact relative à la protection des données et de consultation préalable de l'autorité compétente le cas échéant ;
- ✓ doit supprimer l'ensemble des données personnelles ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes ;
- ✓ met à disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect de ses obligations et doit permettre la réalisation d'audits par le responsable du traitement (ou un auditeur mandaté par celui-ci).

F5. Clauses à insérer dans un accord entre responsables conjoints du traitement (contrat de co-responsabilité)

Conformément à l'article 26 du RGPD, l'accord conclu entre les responsables conjoints du traitement doit définir leurs obligations respectives afin de s'assurer du respect du RGPD.

A ce titre, il doit notamment prévoir le rôle de chaque responsable du traitement dans le cadre de :

- ✓ la gestion des demandes d'exercice de droit adressées par des personnes concernées ;
- ✓ la communication aux personnes concernées des informations relatives au traitement requises par les articles 13 et 14 du RGPD.

Si besoin, l'accord peut désigner un des responsables conjoints comme point de contact pour les personnes concernées.

Nous recommandons également aux responsables conjoints du traitement d'insérer une description détaillée du traitement en question dans l'accord.

F6. Clauses à insérer dans un contrat de partage de données personnelles entre responsables de traitement distincts

Nous recommandons aux parties à un contrat de partage de données personnelles de prévoir dans celui-ci :

- ✓ une description détaillée des flux de données personnelles entre les parties et des traitements effectués dans le cadre du partage ;
- ✓ les rôles et obligations respectives des parties, notamment en ce qui concerne :
  - la gestion des demandes d'exercice des droits des personnes concernées par le traitement entre les parties ;
  - la communication des informations relatives au traitement requises par les articles 13 et 14 du RGPD aux personnes concernées.

En pratique, l'employeur doit analyser les traitements effectués par le prestataire fournissant l'outil afin de déterminer quel est son rôle et celui du prestataire dans le cadre du traitement de données personnelles en question et conclure le contrat adapté à la situation.

Attention : Certaines prestations de service peuvent impliquer la conduite de plusieurs traitements de données personnelles pour lesquels les parties n'ont pas toujours la même qualification. Dans ce cas, il convient de conclure autant de contrat relatif aux traitements de données personnelles qu'il y a de situation.

F7. Attention à ne pas négliger l'encadrement de la prestation de service !

L'employeur doit également encadrer dans le contrat les attentes de l'entreprise en matière de disponibilité, de confidentialité et de sécurité des outils afin d'éviter les mauvaises surprises. Ainsi, l'intégration au contrat de Niveaux de Services (SLA) ou d'une annexe Sécurité ne doit pas être négligée.

Comment encadrer un transfert des données personnelles en dehors de l'Espace Economique Européen (EEE) ?

La prestation de services fournie par le prestataire et/ou l'utilisation des outils peuvent impliquer le transfert de données personnelles en dehors de l'Espace Economique Européen. C'est par exemple le cas si les données personnelles sont hébergées par le prestataire aux Etats-Unis ou en Russie.

Dans ce cas, le RGPD exige l'encadrement du transfert par la mise en place de garanties appropriées de manière à assurer que le niveau de protection des personnes concernées garanti par le RGPD ne soit pas compromis.

Pour ce faire, il existe plusieurs outils juridiques tels que la conclusion de Clauses Contractuelles Types de la Commission Européenne, l'adhésion au Privacy Shield en cas de transfert aux Etats-Unis, les décisions d'adéquation de la Commission Européenne, etc.

En pratique, en cas de transfert des données personnelles en dehors de l'EEE, il convient pour l'employeur d'encadrer le transfert via un des outils juridiques mis à sa disposition et le prévoir dans le contrat conclu avec le prestataire.

TO-DO LIST :

☑ Déterminer le rôle du prestataire dans le cadre des traitements de données résultant de l'utilisation de l'outil ;

☑ Conclure un contrat relatif au traitement de données personnelles en fonction du rôle du prestataire :

- Relation de sous-traitance => conclusion d'un Contrat de sous-traitance de données personnelles
- Relation de co-responsabilité => conclusion d'un Contrat de co-responsablilité
- Relation de responsables de traitement distincts => conclusion d'un Contrat de partage des données personnelles

☑ Analyser si un transfert de données personnelles en dehors de l'EEE est effectué dans le cadre de l'utilisation de l'outil en question ;

☑ Le cas échéant, encadrer le transfert de données personnelles en dehors de l'EEE ;

1.3 Contrôle des mesures de sécurité mises en place

Conformément au RGPD, le responsable de traitement doit mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité des données personnelles adapté au risque.

Dans ses récentes recommandations en matière de télétravail, la CNIL indique que, si l'entreprise doit modifier les règles de gestion de son système d'information pour permettre le télétravail (changement des règles d'habilitation, accès des administrateurs à distance, etc.), il convient de mesurer les risques encourus et, au besoin, de prendre les mesures de sécurité nécessaires.

Dans le cadre de cette analyse, il convient pour l'employeur de vérifier que les mesures de sécurité mises en place par le prestataire sont suffisantes au titre du RGPD pour assurer la sécurité des données personnelles.

Il convient également de mobiliser le service informatique de l'entreprise pour mettre en œuvre les mesures de sécurité supplémentaires nécessaires en interne.

Conformément au RGPD et aux recommandations de la CNIL, les mesures techniques et organisationnelles prises par l'employeur doivent être documentées dans un document spécifique.

TO-DO LIST :

☑ Analyser les risques encourus ;

☑ Déterminer les mesures de sécurité à prendre en fonction des risques ;

☑ Vérifier que les mesures de sécurité du prestataire sont suffisantes ;

☑ Documenter l'analyse des risques et les mesures prises dans un document spécifique.

Les recommandations de la CNIL en matière de sécurité

La CNIL a publié plusieurs contenus relatifs à la sécurité des données :

- Recommandations spécifiques au télétravail : https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mettre-en-place-du-teletravail
- Guide de la sécurité des données personnelles : https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle.pdf
- Recommandations spécifiques au BYOD : https://www.cnil.fr/fr/byod-quelles-sont-les-bonnes-pratiques

BILAN DE L'ETAPE 1 :

Cette étape est achevée lorsque l'employeur s'est assuré que :

i. les traitements de données personnelles sous-jacents à l'utilisation des outils sont bien proportionnés ;

ii. le rôle du prestataire dans le cadre des traitements de données est déterminé et ses obligations encadrées dans le cadre d'un contrat adapté ;

iii. les mesures de sécurité des données sont suffisantes.

Il convient alors de préparer ou mettre à jour la documentation associée aux traitements de données. C'est l'objet de l'Etape 2.

Etape 2 : Préparation et mise à jour de la documentation associée aux traitements de données impliqués par le télétravail

2.1 Notice d'information des personnes concernées

Conformément aux articles 13 et 14 du RGPD, les personnes concernées doivent recevoir une information complète, précise et transparente sur la façon dont leurs données personnelles sont utilisées.

Ainsi, il convient de vérifier que les traitements de données effectués lors de l'utilisation des outils de télétravail ont déjà fait l'objet d'une information (via la politique de confidentialité à destination des salariés par exemple).

Si ce n'est pas le cas, la fourniture d'une notice d'information spécifique ou la mise à jour de la politique de confidentialité à destination des salariés est nécessaire.

2.2 Charte informatique

L'employeur doit mettre en place au sein de l'entreprise une charte informatique dictant les modalités d'utilisation des ressources informatiques mises à disposition des salariés par l'employeur et notamment les mesures de sécurité et bonnes pratiques à suivre dans le cadre du télétravail.

A titre d'exemple, une charte informatique peut inclure les mesures de sécurité suivantes :

- Ne jamais confier son identifiant/mot de passe à un tiers ;
- Verrouiller son ordinateur dès que l'on quitte son poste de travail ;
- Ne pas accéder, tenter d'accéder ou supprimer des informations si cela ne relève pas des tâches incombant au salarié ; ou encore,
- Ne pas installer, copier, modifier, détruire des logiciels sans autorisation.

L'employeur doit s'assurer que l'installation des outils en question dans l'environnement informatique de l'entreprise ne nécessite pas l'intégration de règles d'utilisation supplémentaires dans la charte informatique de l'entreprise et la modifier le cas échéant.

2.3 Registre de traitement de données personnelles

Conformément à l'article 30 du RGPD, le responsable du traitement doit tenir un registre des activités de traitement de données personnelles effectués sous sa responsabilité.

L'employeur doit s'assurer que les traitements de données personnelles sous-jacents à l'utilisation des outils et à l'organisation du télétravail sont déjà été prévus dans le registre de traitements de données et, à défaut, les y répertorier.

2.4 Politiques internes

Conformément au RGPD, l'employeur doit mettre en place des processus internes permettant d'assurer la protection des données à tout moment.

Organiser les processus internes de l'entreprise implique notamment la rédaction et la mise en place des politiques suivantes :

- Politique pour le respect des principes de Privacy by Design et Privacy by Default ;
- Politique de mise en place de nouveaux traitements de données ;
- Politique de gestion des demandes d'exercice de droits par des personnes concernées ;
- Politique de notification et gestion des violations de données personnelles.

Ces politiques peuvent nécessiter des mises à jour afin d'intégrer les contraintes et risques liés au télétravail.

2.5 Adjonction de la documentation pertinente au Règlement Intérieur

Pour permettre à l'employeur d'appliquer des sanctions en cas de manquement aux obligations de sécurité et de bon usage prévues à la Charte informatique ou tout autre document en lien avec le télétravail, il convient de suivre la procédure d'adjonction au règlement intérieur prévue à l'article L. 1321-1 et suivant du code du travail.

Checklist de la documentation à préparer et/ou mettre à jour :

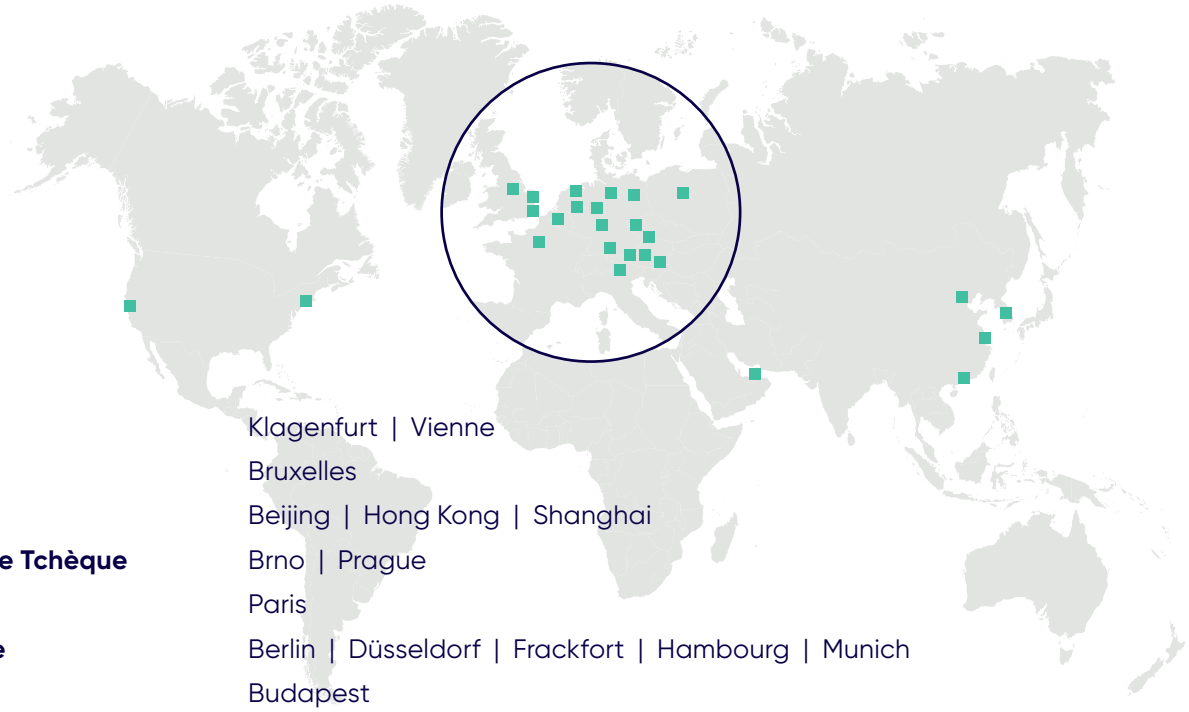
- ☑ Le cas échéant, Analyse d'Impact à la Protection des Données ;
- ☑ Le cas échéant, test de balance entre l'intérêt du responsable de traitement et les droits et libertés des personnes concernées ;
- ☑ Contrat relatif aux traitements de données personnelles conclu avec le prestataire ;
- ☑ Document répertoriant les mesures techniques et organisationnelles prises ;
- ☑ Notice d'information aux personnes concernées ;
- ☑ Charte informatique ;
- ☑ Registre des traitements de données personnelles ;
- ☑ Politiques internes :
- ☑ Adjonction des documents pertinents au Règlement Intérieur.

Contacts

Valérie Aumage
Avocat Associé IT
T +33 (0)1 72 74 18 35
E v.aumage@taylorwessing.com

Chloé Martin dit Neuville
Avocat Collaborateur IT
T +33 (0)1 72 74 03 33
E c.martinditneuville@taylorwessing.com

1000+ avocats
300+ associés
28 bureaux
16 juridictions



Autriche	Klagenfurt | Vienne
Belgique	Bruxelles
Chine	Beijing | Hong Kong | Shanghai
République Tchèque	Brno | Prague
France	Paris
Allemagne	Berlin | Düsseldorf | Frackfort | Hambourg | Munich
Hongrie	Budapest
Pays-Bas	Amsterdam | Eindhoven
Pologne	Varsovie
Slovaquie	Bratislava
Corée du Sud	Seoul*
EAU	Dubai
Ukraine	Kiev
Royaume-Uni	Cambridge | Liverpool | Londres | Londres TechFocus
Etats-Unis	New York | Silicon Valley

* En partenariat avec DR & AJU LLC