

# COVID-19 : PROTECTION DE DONNÉES ET CORONAVIRUS : FOIRE AUX QUESTIONS POUR LES EMPLOYEURS

**Categories :** COVID-19

**Date :** 06-04-2020

Dans le cadre de la pandémie de coronavirus, les entreprises mettent en œuvre des mesures exceptionnelles pour protéger la santé et la sécurité de leurs employés et clients. En raison de ces mesures extraordinaires, les employeurs sont amenés à collecter de nouveaux types de données personnelles, notamment pour savoir si les collaborateurs présentent des symptômes du virus.

Le Comité Européen de la Protection des Données (« EDPB ») et la CNPD ont publié récemment des recommandations<sup>[1]</sup> relatives à la collecte de données personnelles dans un contexte de crise sanitaire. Tenant compte de ces recommandations, nous avons élaboré une liste de questions-réponses pour vous accompagner dans vos démarches de mise en conformité.

- **Quelles données puis-je collecter en cas de suspicion de coronavirus dans mon entreprise et sur quelle(s) base(s)?**

Si une suspicion de coronavirus est signalée dans l'entreprise vous pouvez, dans le cadre de vos obligations de sécurité et de santé prévues par le Code du travail, consigner :

- la date et l'identité de la personne suspectée d'avoir été exposée au virus;
- les mesures organisationnelles prises (mesures de confinement, télétravail, prise de contact avec le service de la médecine au travail, etc.).

A la demande des autorités sanitaires, vous pouvez leur transmettre les informations relatives à la nature de l'exposition, nécessaires à une éventuelle prise en charge sanitaire ou médicale de l'employé/agent exposé.

Les traitements de données effectués par l'employeur dans ce contexte peuvent être justifiés notamment par ses obligations légales en matière de santé et sécurité au travail (Article 6.1. lit. c) du RGPD).

En ce qui concerne plus particulièrement le traitement des données de santé, l'employeur peut se fonder sur l'exécution de ses obligations en matière de droit du travail (Article 9.2. lit. b) du RGPD), sur des motifs d'intérêt public dans le domaine de la santé publique (Article 9.2. lit. i) du

RGPD) ou encore sur la nécessité de sauvegarder les intérêts vitaux de la personne concernée (Article 9.2. lit. c) du RGPD).

- **Comment gérer la communication interne relative au virus ?**

En vue d'assurer une gestion optimale de la communication sur les suspicions de coronavirus, la CNPD recommande de :

- sensibiliser et inviter les employés/agents à effectuer des remontées individuelles d'information les concernant en lien avec une éventuelle exposition, auprès d'eux ou des autorités sanitaires ;
- faciliter la transmission des informations par la mise en place, au besoin, de canaux dédiés pour garantir la sécurité et la confidentialité des données.

L'article L. 313-1. du Code du travail prévoit l'obligation de chaque salarié de prendre soin, selon ses possibilités, de sa sécurité et de sa santé ainsi que de celles des autres personnes concernées du fait de ses actes ou de ses omissions au travail, conformément à sa formation et aux instructions de son employeur. Par conséquent, les salariés doivent, en principe, informer leur employeur en cas de suspicion d'exposition au virus. Vous devez communiquer à vos collaborateurs l'existence de cette obligation.

Pour pouvoir mettre en place les recommandations susvisées, nous vous conseillons d'élaborer une procédure interne ainsi qu'une notice d'information, ou à tout le moins de mettre à jour vos notices d'information destinées à vos salariés, reprenant de manière claire les obligations des salariés en cas de suspicion d'exposition au virus (la nature des informations à fournir, les personnes autorisées à recevoir les signalements ou encore la création d'une adresse email dédiée aux déclarations de cas suspects) et de la communiquer à l'ensemble du personnel.

- **Puis-je dévoiler l'identité des collaborateurs atteints par le virus ?**

Selon les recommandations de l'EDPB, les employeurs sont tenus d'informer le personnel sur l'existence des cas de COVID-19 au sein de l'entreprise et de prendre des mesures de protection.

Dans le respect du principe de minimisation des données, les employeurs ne doivent toutefois pas communiquer plus d'informations que ce qui est strictement nécessaire à la protection de la santé des collaborateurs.

La CNPD précise que l'identité des personnes concernées ne doit pas être divulguée à des tiers ou à leurs collègues sans justification claire. Il conviendra donc d'effectuer une analyse au cas par cas pour déterminer si la révélation de l'identité des personnes concernées est justifiée (par exemple, par la nécessité de mettre en quarantaine les collaborateurs/équipes ayant été en contact avec la personne concernée).

Dans le cas où il s'avère nécessaire de révéler le nom des employés qui ont contracté le virus, ces derniers doivent être informés à l'avance et les employeurs doivent veiller au respect de leur dignité et intégrité.

- **Dans quelle mesure je peux effectuer des contrôles pour identifier des cas suspects d'infection ?**

Il est interdit de collecter de manière systématique et généralisée, ou par le biais d'enquêtes et demandes individuelles, des informations concernant la recherche d'éventuels symptômes présentés par un employé/personne externe à l'entreprise ainsi que leurs proches.

La CNPD prohibe :

- d'exiger que les employés vous communiquent quotidiennement un relevé de leurs températures corporelles ou que ces derniers remplissent des fiches ou questionnaires médicaux, préalablement établis ; ou
- de solliciter des visiteurs ou autres personnes externes de signer une déclaration préétablie par laquelle ils certifieraient qu'ils ne présentent pas de symptôme du coronavirus ou qu'ils n'ont pas voyagé récemment dans une zone à risque, etc.

- **Comment préserver la sécurité des données dans le cadre du télétravail?**

En cas de télétravail, l'employeur reste responsable pour les incidents affectant la sécurité des données personnelles et doit mettre en place les mesures techniques et organisationnelles appropriées telles que :

- l'accès des employés au système informatique de l'employeur doit être fourni via un point d'accès sécurisé (par exemple, une connexion VPN) avec une procédure de vérification d'accès solide.

- l'employeur doit veiller à ce que les salariés respectent les mesures de sécurité minimales (ex. verrouillage de l'ordinateur après avoir quitté le poste ; appels téléphoniques confidentiels sans la présence d'autres personnes susceptibles d'entendre les conversations ; sécurisation du réseau wi-fi utilisé pour le télétravail) ;
- mise en place d'une politique de télétravail définissant les obligations des collaborateurs notamment celles destinées à préserver la confidentialité et sécurité des données ;
- l'utilisation des documents en format physique contenant des données confidentielles (dossiers, impressions) par les salariés doit être interdite ou au moins limitée ;
- l'utilisation de l'équipement informatique privé du salarié pour le télétravail doit être évitée. Si l'utilisation des équipements privés est inévitable, l'employeur doit veiller à ce qu'ils soient sécurisés de manière adéquate. Il convient de prévoir une séparation des données privées et professionnelles.

- **Surveillance des salariés en télétravail : est-ce possible ?**

Une telle surveillance est possible, mais elle strictement encadrée.

En effet, la situation exceptionnelle liée à la propagation du coronavirus ne vous autorise pas à mettre en place un système de surveillance des salariés en dehors des conditions prévues par l'article L. 261-1. du Code du travail.

Préalablement à la mise en œuvre du traitement à des fins de surveillance l'employeur doit en informer les salariés concernés, mais aussi la délégation du personnel ou, à défaut, l'inspection du travail et des mines. En outre, certains traitements doivent faire l'objet d'une codécision entre l'employeur et la délégation du personnel.

Les employeurs qui effectuent des traitements en violation de l'article susvisé peuvent encourir une peine d'emprisonnement de huit jours à un an et/ou une amende jusqu'à 125.000 euros.

- **Est-il nécessaire de mettre à jour ma politique de confidentialité ?**

Il convient de vérifier si votre politique de confidentialité et votre registre des activités de traitement contiennent les informations nécessaires concernant les catégories de données collectées et les finalités du traitement.

Si vous collectez de nouvelles catégories de données personnelles et/ou utilisez les données personnelles pour d'autres finalités, vous devez mettre à jour votre documentation pour refléter ces changements.

**L'équipe MDTP (Média, Data, Technologies & IP) de l'Etude Molitor Avocats à la Cour** se tient à votre disposition, ainsi qu'à celle de vos clients, afin de vous accompagner durant cette période particulière et vous assister pour toutes questions que vous pourriez avoir sur l'impact du coronavirus en matière de protection de données, ou sur votre activité en général.

[1] CNPD, *Coronavirus (covid-19): Recommandations de la CNPD relatives à la collecte de données personnelles dans un contexte de crise sanitaire*, <https://cnpd.public.lu/fr/actualites/national/2020/03/coronavirus.html>

EDPB, *Statement on the processing of personal data in the context of the COVID-19 outbreak*, [https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak\\_en](https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en)

**Experts :**



**Virginie LIEBERMANN**

**COUNSEL**

Avocat à la Cour, Member of Luxembourg Bar, 2008