

# Le journal de la conformité RGPD

Numéro 1 - Mars 2020

## Coronavirus, confinement : quelles implications en matière de protection des données ?

### UN NOUVEL OUTIL : le questionnaire mensuel de votre délégué à la protection des données

Ressourcial est votre **délégué à la protection des données (DPD)** ? Si oui, à ce titre il est alors nécessaire que nous soyons informés de toute nouvelle actualité touchant à la protection des données dans votre organisme. Pour cela Ressourcial lance un nouvel outil : un questionnaire qui, si vous êtes concerné, vous sera adressé chaque début de mois. Il est destiné à **repérer les situations qui mériteraient que votre DPD soit associé à vos travaux et réflexions**. Il ne vous faudra jamais plus de 5 minutes pour y répondre !

### Nous contacter

#### Ressourcial

19 rue Marius Grosso  
69120 Vaulx-en-Velin  
contact@ressourcial.fr  
www.ressourcial.fr

### CELLULES DE CRISE : RESSOURCIAL EST À VOS CÔTÉS

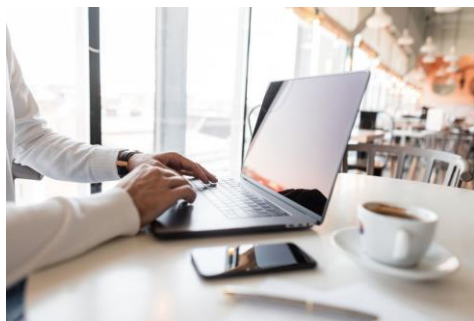
Dans le contexte particulier que nous traversons tous en ces jours de pandémie, nous vous savons pleinement mobilisés pour assurer des conditions aussi satisfaisantes que possible en termes d'accueil et de sécurité de vos usagers et de travail pour vos salariés. Gérer cette crise implique pour vous des décisions quotidiennes à prendre pour assurer la continuité de vos missions. Nous attirons votre attention sur les brèches qui risquent de s'ouvrir dans cette période troublée en termes de sécurité de vos systèmes d'information et de protection des données personnelles.

Ressourcial est pleinement à votre écoute pour vous accompagner dans cette période difficile. Dans les prochains jours, les consultants qui vous accompagnent prendront attache avec vous pour étudier la manière dont nous pouvons vous être utiles en cette période. De votre côté, à la moindre interrogation, n'hésitez pas à contacter votre consultant habituel, ou à adresser toute question à [contact@ressourcial.fr](mailto:contact@ressourcial.fr).

### UN RISQUE CYBER ACCRU EN PÉRIODE DE CRISE SANITAIRE

L'épidémie du coronavirus génère une situation de crise mondiale. Dans ce contexte, les cybercriminels sont à l'affût. D'une part les changements brusques d'organisation peuvent conduire à des imprudences dans le management des systèmes d'information, d'autre part de nouvelles cibles s'offrent à eux : les millions de télétravailleurs depuis que le gouvernement impose le confinement à domicile de millions de français.

Les pièges sont en effet multiples : des messages invitant à se connecter sur des espaces partagés frauduleux, des mails malveillants semblant venir d'organismes publics et d'autres usurpant l'identité de collègues, des fausses



*Face au risque de développement exponentiel de l'épidémie, l'employeur est invité à privilégier au maximum, lorsque cela est possible, le télétravail pour ses employés.*

demandes du service RH liées à l'organisation du travail à domicile, des faux appels téléphoniques en encore la fameuse « arnaque au président<sup>1</sup> ».

Dans ce contexte anxiogène, les citoyens ont aussi besoin de s'informer. Cependant, attention aux sources. Des experts ont par exemple identifié un logiciel malveillant des plus vicieux, *Corona-virus-Map.com.exe*, caché dans des sites Internet ou des applications pour smartphones et qui fait état de la diffusion du virus en appâtant l'internaute avec une carte de l'expansion de la pandémie, ce programme, en réalité, siphonne les données des ordinateurs (historique de navigation, mots de passe, cryptomonnaies, cookies...).

## **TÉLÉTRAVAIL : MAÎTRISER LES RISQUES EN ADOPTANT DE BONNES PRATIQUES**

En vertu de l'article L 4121-1 du Code du travail, l'employeur est responsable de la santé et de la sécurité des salariés. De ce fait, face au risque de développement exponentiel de l'épidémie, il est invité à privilégier au maximum, lorsque cela est possible, le télétravail pour ses employés.

Le Code du travail (Article L-1222-9) définit le télétravail comme 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. Le risque épidémique peut justifier la mise en œuvre du télétravail sans l'accord du salarié (Art. L1122-11 du Code du Travail).

Dans la mesure où l'article L.4121-1 du Code du travail indique que l'employeur est responsable de la santé et de la sécurité des salariés, il doit mettre en œuvre des actions de prévention des risques, des actions d'information et de formation, et une réorganisation du travail adapté à la crise sanitaire.

Le recours au télétravail est donc encouragé mais il ne faut pas pour autant oublier les règles de prudence concernant la collecte et le traitement de données personnelles sensibles.

Certains des salariés du secteur social et médico-social aujourd'hui en situation obligée de télétravail n'ont pas été préparés à ce mode d'activité. Or, les employeurs et toute la chaîne de management, pris au dépourvu, ne sont pas toujours en mesure de définir un cadre pratique clair. Dans l'urgence, de nombreux actes et omissions peuvent présenter des risques au titre de la protection des données.

Le télétravail présente en effet des risques : des outils d'échange de données, gratuits, et non sécurisés peuvent être utilisés (WhatsApp, Facebook, Messenger, Skype, Google Hangouts, etc.). Cela ne permet pas de garantir une sécurité suffisante des données des usagers et contrevient donc aux règles en matière de protection des données.

Le télétravail risque également d'entraîner l'utilisation de périphériques non contrôlés (clés USB, disques durs, appareils personnels non sécurisés, présence d'enceintes connectées au domicile du salarié, confusion entre les outils professionnels et personnels, etc.). Cela met en péril la sécurité et confidentialité des données personnelles.

Face à ces risques, nous vous proposons de vous référer aux recommandations émises par les autorités européennes et françaises. Ainsi, l'agence européenne de cybersécurité, l'ENISA, a formulé une série de recommandations à l'intention des entreprises qui se tournent vers le télétravail du fait de l'épidémie de Covid-19<sup>2</sup>. De même, le gouvernement communique des bonnes pratiques à adopter dans ce contexte pour lutter contre la cyber-malveillance et souligne les pièges à éviter<sup>3</sup>.

<sup>1</sup> <https://www.economie.gouv.fr/dgcrf/professionnels-agents-publics-attention-a-larnaque-au-president>

<sup>2</sup> <https://www.zdnet.fr/pratique/teletravail-conseils-de-cybersecurite-pour-les-travailleurs-a-distance-39900759.htm>

<sup>3</sup> <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite>  
<https://www.cert.ssi.gouv.fr/actualite/CERTFR-2020-ACT-002/>

### Quelques conseils (liste non exhaustive) :

- Utiliser une solution d'accès de type VPN (*Virtual Private Network*, réseau privé virtuel) propre à l'entreprise,
- Se méfier des messages ou appels téléphoniques d'origine inconnue ou inattendus,
- Ne télécharger des applications que depuis des sites officiels,
- Vérifier la fiabilité des sites visités,
- Être vigilants face à l'afflux de fausses informations,
- Se méfier des appels aux dons frauduleux,
- Appliquer les mises à jour de sécurité sur les équipements connectés lorsqu'elles sont disponibles,
- S'assurer que la connexion Wi-Fi utilisée est sécurisée et employer le matériel et la connexion sécurisée fournis par l'employeur quand cela est possible (accès à distance, visioconférence),
- S'assurer que l'anti-virus est mis à jour,
- Sauvegarder régulièrement tous les fichiers importants,
- Ne pas utiliser d'appareils personnels pour le travail et ne pas transférer de données professionnelles sur ces appareils,
- Débrancher les assistants vocaux (Google assistant, Alexa, etc.) durant le travail,
- Verrouiller le poste de travail en cas d'absence et protéger la confidentialité des données,
- S'isoler pour travailler sur des données sensibles, sans la présence d'autres personnes,
- Sécuriser ses documents papiers et les dossiers que l'on a été autorisé à emporter à domicile,
- Ne pas se connecter aux réseaux sociaux avec le matériel professionnel confié.

## QUELLES PRÉCAUTIONS EN MATIÈRE DE TÉLÉMÉDECINE ?

La Télémédecine, au sens de l'article L6316-1 du code de la santé publique, est une « forme de pratique médicale à distance utilisant les technologies de l'information et de la communication ». Constituent des actes de télémédecine : la téléconsultation, la téléexpertise, la télésurveillance médicale, la téléassistance médicale (article R 6316-1 du CSP).



*La télémédecine, une pratique qui doit être encadrée car les données personnelles qui sont traitées (collectées, enregistrées, échangées et potentiellement conservées) sont des données de santé.*

La télémédecine s'est beaucoup développée ces dernières années, pour diverses raisons : manque d'effectifs de professionnels de santé, personnes fragiles ayant des difficultés à se déplacer, limitation des coûts de déplacement. Par ailleurs, dans le cadre du plan « Ma santé 2022 », le ministère de la santé a publié un guide de doctrine technique du numérique en santé incluant un chapitre sur la télémédecine, exposant les objectifs de développement de cette méthode<sup>4</sup>.

Cependant, cette pratique doit être encadrée car les données personnelles qui sont traitées (collectées, enregistrées, échangées et potentiellement conservées) sont des données de santé. Au sens du RGPD : ces données sont des données dites « sensibles » (considérant 35 et article 9 du RGPD). En vertu de leur nature sensible, ces données particulières doivent bénéficier d'une protection renforcée par rapport aux autres catégories de données.

C'est pourquoi, l'utilisation de la télémédecine doit être strictement encadrée :

- Consentement libre et éclairé de la personne - Article R. 6316-2 du CSP.
- Conditions de réalisation des actes - Article R. 6316-3 du CSP : *Chaque acte de télémédecine est réalisé dans des conditions garantissant : 1.a) L'authentification des professionnels de santé intervenant dans l'acte ; b) L'identification du patient, c) L'accès des professionnels de santé aux données médicales du patient nécessaires à*

<sup>4</sup> [https://esante.gouv.fr/sites/default/files/media\\_entity/documents/doctrine--technique-du-numerique-en-sante\\_version-2019\\_vf.pdf](https://esante.gouv.fr/sites/default/files/media_entity/documents/doctrine--technique-du-numerique-en-sante_version-2019_vf.pdf)

la réalisation de l'acte ; 2. Lorsque la situation l'impose, la formation ou la préparation du patient à l'utilisation du dispositif de télémedecine.

- Tenue du dossier patient - Article R. 6316-4 du CSP.
- Formation et compétences des professionnels - Article R. 6316-9 du CSP : *Les organismes et les professionnels libéraux de santé qui organisent une activité de télémedecine s'assurent que les professionnels de santé et les psychologues participant aux activités de télémedecine ont la formation et les compétences techniques requises pour l'utilisation des dispositifs correspondants.*
- Les flux d'échange de données doivent être sécurisés (conformité aux modalités d'hébergement des données de santé à caractère personnel - Article R. 6316 -10 du CSP).

Pour davantage de précisions, voir le lien en note de bas de page<sup>5</sup>.

## **Pour répondre à la crise sanitaire dans le contexte actuel (Covid 19) : un décret du ministre des solidarités et de la santé est venu assouplir, jusqu'au 30 avril 2020, les dérogations aux modalités de réalisation des actes de télémedecine.**

**Décret n° 2020-227 du 9 mars 2020 adaptant les conditions du bénéfice des prestations en espèces d'assurance maladie et de prise en charge des actes de télémedecine pour les personnes exposées au covid-19<sup>6</sup>.**

---

*« Le décret détermine, d'autre part, les conditions dérogatoires de prise en charge des actes de télémedecine pour les personnes atteintes ou potentiellement infectées par le coronavirus qui pourront en bénéficier même si elles n'ont pas de médecin traitant pratiquant la téléconsultation ni été orientées par lui ni été connues du médecin téléconsultant. Comme le prévoit la convention médicale, ces téléconsultations devront s'inscrire prioritairement dans le cadre d'organisations territoriales coordonnées. Elles peuvent être réalisées en utilisant n'importe lequel des moyens technologiques actuellement disponibles pour réaliser une vidéo transmission (lieu dédié équipé mais aussi site ou application sécurisé via un ordinateur, une tablette ou un smartphone, équipé d'une webcam et relié à internet). »*

---

Olivier Véran, ministre des Solidarités et de la Santé, a précisé qu'un patient incapable de recourir aux outils conventionnels peut "contacter par FaceTime ou WhatsApp un autre médecin qui est capable de lui faire son ordonnance, son arrêt de travail" (France Info 10 mars<sup>7</sup>). Parmi les solutions de télécommunication les plus utilisées par les particuliers au quotidien, on compte Hangouts (Google), FaceTime (Apple), WhatsApp (Facebook) et Skype (Microsoft).

Pour faire face à l'utilisation massive des solutions de télécommunication des GAFAM, gratuits, mais non adaptés à la télémedecine, **certaines plateformes de téléconsultations sont ouvertes de manière gratuites** : c'est notamment le cas de Medicam, Doctolib, Medadom, Rofim<sup>8</sup>.

**Ces dispositions dérogent aux dispositions en vigueur et ne sont valables que jusqu'au 30 avril 2020, lorsque la crise sanitaire sera terminée. En résumé, il est donc recommandé de se tourner vers des plateformes conformes et de bien veiller à ne pas pérenniser les usages dérogatoires au-delà de cette date.**

---

<sup>5</sup> [https://www.has-sante.fr/upload/docs/application/pdf/2019-07/fiche\\_memo\\_teleconsultation\\_et\\_teleexpertise\\_mise\\_en\\_oeuvre.pdf](https://www.has-sante.fr/upload/docs/application/pdf/2019-07/fiche_memo_teleconsultation_et_teleexpertise_mise_en_oeuvre.pdf)

<sup>6</sup> <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041704122&categorieLien=id>

<sup>7</sup> [https://www.francetvinfo.fr/replay-radio/8h30-fauvelle-dely/les-mesures-du-gouvernement-contre-le-coronavirus-les-consultations-a-distance-les-italiens-confines-le-8h30-franceinfo-d-olivier-veran\\_3841801.html](https://www.francetvinfo.fr/replay-radio/8h30-fauvelle-dely/les-mesures-du-gouvernement-contre-le-coronavirus-les-consultations-a-distance-les-italiens-confines-le-8h30-franceinfo-d-olivier-veran_3841801.html)

<sup>8</sup> La télémedecine se met à l'heure du coronavirus (Hospimedia, 17 mars 2020).

## COVID 19 ET TRAITEMENTS DE DONNÉES DE SANTÉ

Dans la situation de crise liée au COVID 19, Ressourcial souhaite vous rappeler les bonnes pratiques de respect de la vie privée des personnes concernées (usagers, salariés, etc.) valables même en période épidémique. Pour rappel les informations COVID 19 sont des données de santé. D'après le Code de la Santé Publique et du Code de la protection des données personnelles, une donnée de santé est toute information qui rend compte de l'état de santé d'une personne.

Le traitement de ces données particulières dites « sensibles » est par principe interdit (article 9 du RGPD). Leur utilisation est autorisée seulement dans certains cas, notamment lorsque la sauvegarde d'intérêts vitaux de personnes est concernée (art.9 2. c) et dans le cadre de l'exercice d'une mission d'intérêt public (art.9 2. g), dont la santé publique.

### Les mesures à proscrire en cas de crise sanitaire :

En cas de crise sanitaire, telle l'épidémie actuelle, il est recommandé<sup>9</sup> à l'employeur de prendre des mesures de prévention, comme favoriser les modes de travail à distance, et les faciliter au maximum pour les personnes considérées à risque<sup>10</sup>, interdire ou annuler les déplacements professionnels, éviter au maximum les rassemblements, fournir le matériel d'hygiène nécessaire (gel hydroalcoolique, gants, distance à respecter) à la mise en place des gestes barrières, etc. L'employeur doit donc s'assurer que les missions et les conditions de travail n'exposent pas ses employés ou des usagers à des risques. En revanche, il ne peut pas porter atteinte au respect de la vie privée des personnes concernées (usagers/salariés) et surveiller ses usagers et/ou employés en collectant par exemple systématiquement leur température, leurs symptômes ou la condition de leur entourage (pour savoir si l'un de leurs proches présente des symptômes, par exemple). Il ne peut pas d'avantage exiger du salarié ou de l'utilisateur qu'il lui communique ses relevés de température quotidiens, ou les endroits qu'il a pu fréquenter en vacances ou dans tout autre cadre privé. Seul le médecin du travail ou le médecin traitant est habilité à collecter ce type de données, qui seront protégées par le secret professionnel. Tout usager ou tout employé a le droit de refuser tout type d'examen ou questionnaire.

Concrètement, comment les entreprises peuvent-elles protéger la santé de leurs employés et de leurs usagers tout en respectant leur vie privée ? L'employeur doit mettre en place des actions de prévention en se fondant sur les recommandations officielles (ministère des Solidarités et de la Santé, ARS, Conseil départemental, etc.) et pourra dans ce cas-recueillir uniquement certaines données, comme la date et l'identité de la personne suspectée d'avoir été exposée, les mesures prises (télétravail, congé maladie,...) et il devra communiquer aux autorités sanitaires qui le demandent les éléments liés à la nature de l'exposition, pour qu'une éventuelle prise en charge sanitaire ou médicale de la personne exposée soit mise en place.

Le ministère des Solidarités et de la Santé, dans un guide<sup>11</sup>, précise les modalités de détection du COVID-19 ainsi que les modalités d'alerte à mettre en place dans les structures médico-sociales. Afin d'organiser au mieux le circuit du patient dans la filière sanitaire appropriée, le personnel chargé de la prise en charge du patient doit informer sans délai l'ARS afin d'anticiper dès le signalement le suivi et la prise en charge des contacts étroits et des co-exposés le cas échéant.

Le repérage du patient suspect se fait en premier lieu par le personnel de l'établissement ou du service à partir des premiers symptômes (fièvre, signes respiratoires). En raison de la fragilité des résidents (âge, comorbidités, vie en collectivité), tout syndrome grippal ou rhinopharyngé doit faire l'objet d'investigations systématiques.

**Enfin, nous rappelons que tout traitement de données à caractère personnel doit être identifié et inscrit au registre de vos activités de traitement.**

<sup>9</sup> <https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles>

<sup>10</sup> Femmes enceintes / Maladies respiratoires chroniques (asthme, bronchite chronique...) / Insuffisances respiratoires chroniques / Mucoviscidose / Insuffisances cardiaques toutes causes / Maladies des coronaires / Antécédents d'accident vasculaire cérébral / Hypertension artérielle / Insuffisance rénale chronique dialysée / Diabète de type 1/insulinodépendant et diabète de type 2 / Les personnes avec une immunodépression : pathologies cancéreuses et hématologiques, transplantations d'organe et de cellules souches hématopoïétiques, maladies inflammatoires et/ou auto immunes recevant un traitement immunosuppresseur, personnes infectées par le VIH, Maladie hépatique chronique avec cirrhose / Obésité avec un indice de masse corporelle (IMC) égal ou supérieur à 40.

<sup>11</sup> <https://solidarites-sante.gouv.fr/IMG/pdf/guide-covid-19-phase-epidemie-v15-16032020.pdf>