

**Séminaire en ligne**

Jeudi 30 avril 2020

# **RGPD et sécurité informatique pendant la crise du Covid-19**

Gauthier DUCOULOMBIER

Délégué à la protection des données

Cdg59

Nicolas GILLIERS

Délégué à la protection des données

Cdg59

- I. **Contexte général: RGPD et sécurité informatique**
- II. **Contexte particulier : crise sanitaire liée au Covid-19**
- III. **Télétravail et sécurité informatique : risques et « gestes barrières »**
- IV. **Outils informatiques (visioconférence, transfert de fichiers) :  
Comment les choisir?**
- V. **Incidents informatiques (cyberattaque, panne) :  
Comment réagir?**

**Contacts et Ressources**



# I. Contexte général : RGPD et sécurité informatique



La **sécurité des données** constitue un des **pilliers essentiels de la protection des données** à caractère personnel.

Parmi les exigences fixées dans le RGPD, la nécessité de **garantir un niveau de sécurité adapté aux données à protéger.**

4

Le RGPD exige la mise en œuvre de **mesures de sécurité techniques et organisationnelles appropriées**, afin de garantir les critères « **DCIP** » pour les données à caractère personnel.



Disponibilité - Confidentialité - Intégrité - Preuve (traçabilité)



## II. Contexte particulier : Crise sanitaire liée au COVID-19



## Contexte particulier : Crise sanitaire liée au Covid-19



**Le COVID-19 : une opportunité pour les pirates informatiques !**

Les collectivités territoriales ont dû mettre en place dans l'urgence le **télétravail pour assurer la continuité du service public.**

**Elles ont dû faire des choix et abaisser le niveau de sécurité.**

7



## Contexte particulier : Crise sanitaire liée au Covid-19

### Les menaces du moment :

**Ransomware (ou rançongiciel)** : Logiciel malveillant qui chiffre les données de l'ordinateur pour demander une rançon en échange du mot de passe de déchiffrement.



**Phishing (ou hameçonnage)** : Technique destinée à obtenir des données personnelles, professionnelles ou bancaires depuis un site internet copié et falsifié.

8





## Contexte particulier : Crise sanitaire liée au Covid-19

### Les menaces du moment :



**« Arnaque au Président »**

**Faux ordres de virement**

**Chantage aux données personnelles**



### Les faits marquants de ces dernières semaines :

**14 mars 2020** : Attaque par rançongiciel de la **mairie de Marseille** et de la **métropole Aix-Marseille-Provence**. 300 ordinateurs et 90% des serveurs ont été cryptés.

**17 mars 2020** : Attaque similaire de la **mairie de Charleville-Mezières** et d'**Ardennes Métropole**.

**22 mars 2020** : Attaque par déni de service (DDOS) de l'**Assistance Publique – Hôpitaux de Paris (AP-HP)**.



10



## Contexte particulier : Crise sanitaire liée au Covid-19

### Les faits marquants de ces dernières semaines :



**6 millions d'euros de perte** dans le cadre d'une arnaque au Président : Une entreprise pharmaceutique passe une commande massive de masques et de gel à une société « fantôme ».

11

**Les fausses applications « COVID-19 »** contenant un rançongiciel qui va chiffrer les données des smartphones.

**50% des noms de domaines** liés au COVID-19, peuvent provoquer l'injection de logiciels malveillants (étude Thalès).



# Contexte particulier : Crise sanitaire liée au Covid-19

**Sujet :**Alerte: Demandez Votre Kit de confinement .  
**Date :**Wed, 22 Apr 2020 02:53:35 +0000  
**De :**Ministère de la santé <lamalal@pureandnaturalpet.com>  
**Pour :**xxxx@xxx.fr



Chers citoyens,

En application de l'état d'urgence sanitaire contre le coronavirus COVID-19, le ministre des Solidarités et de la Santé tient à protéger ses citoyens face à cette crise.

Pour cela Santé publique France souhaite équiper gratuitement tous les citoyens avec un kit de confinement.

Ce kit contient des masques médicaux FFP2, des solutions hydroalcooliques, des gants médicaux...

Dès la validation de votre demande, le kit sera livré chez vous par nos spécialistes.

[Faites votre demande](#)



**CYBERMALVEILLANCE.GOUV.FR**  
Assistance et prévention du risque numérique



## Demander votre kit de confinement COVID-19

Santé publique France met à disposition des Kits de confinement gratuitement contre l'épidémie de COVID-19 contenant des masques FFP2, Gel Hydroalcoolique, Gants Médicaux, Kit de Secours...

[Demander votre kit](#)



**Attention !  
ARNAQUE**

x10 Masques FFP2

Masques médicaux avec un très haut niveau de filtration.

x10 Gel Hydroalcoolique

Le gel hydroalcoolique est une solution idéale, rapide et efficace contre les bactéries.

x200 Gants Médicaux

Gants médicaux jetables et antistatiques de qualité professionnelle.

2x Trousse de secours

Les trousses de secours sont indispensables dans votre maison.

x50 Spray antibactérien

Le Lotion spray antibactérien mains et surfaces, désinfecte immédiatement les mains.

x1 Thermomètre

Un thermomètre portable électronique pour prendre la température.

© 2020 Santé publique France





# Questions – réponses avec les participant.es



# III. Télétravail et sécurité informatique : Risques et « gestes barrières »



## Quels sont les risques accentués en raison de la crise ?



- **Abaissement global de la sécurité** suite au déploiement massif du télétravail
- **Négligence ou erreur de l'agent.e**
- **Absence de moyens de détection** du piratage et du monitoring
- **Absence de procédure** en cas de cyberattaque
- **Fuite de données suite à une utilisation perso/pro** de l'ordinateur de l'agent en télétravail
- **Utilisation d'outils de visioconférence ou de transfert de fichiers peu adaptés**

15



Les gestes barrières de la collectivité pour réduire les risques : les moyens techniques



Sauvegardez régulièrement l'ensemble des données en local ET en externe

La **sauvegarde** est l'**unique solution** pour récupérer les données en cas de rançongiciel



Installez des logiciels de sécurité (antivirus, anti-spams...)



Installez des logiciels permettant l'échange d'informations de manière sécurisée (messaging, VPN, ...)





**Les gestes barrières de la collectivité pour réduire les risques : les moyens humains ou organisationnels**



**Sensibilisez à la sécurité informatique vos agent.es en télétravail.**



**Appliquez les derniers correctifs de sécurité aux équipements et logiciels utilisés**



**Utilisez des protocoles garantissant la confidentialité et l'authentification du serveur destinataire (https pour les sites web, SFTP pour le transfert de fichiers)**



## Les gestes barrières de l'agent.e



**Ne désactivez pas l'antivirus et scannez vos équipements**



**Restez vigilant sur les usages du matériel informatique :  
Ne mélangez pas « Pro et Perso »**



**Appliquez impérativement les mises à jour et correctifs  
Windows**



**Ne faites pas en télétravail ce que vous ne feriez pas au  
bureau**



## Les gestes barrières de l'agent.e



**Renforcez la sécurité de vos mots de passe**



**N'utilisez pas d'outils de stockage ou de transferts de fichiers dans le cloud**

Privilégiez les plateformes  
d'échange sécurisés préconisés par  
l'ANSSI



**Ne connectez pas de périphériques externes (USB ...)**



## La bonne conduite de l'agent.e dans la gestion des emails :

**Un courriel vous paraît suspect : n'y répondez pas et supprimez le !**

**Ne cliquez pas sur les liens présents dans le message !**

**Comment détecter un courriel suspect ?**

- Expéditeur inconnu ou inhabituel
- Esthétique graphique ou orthographe douteuse
- Expéditeur, objet ou pièce jointe inhabituels
- Demande d'informations personnelles et/ou sensibles



20



# Questions – réponses avec les participant.es

# IV. Outils informatiques (visioconférence, transfert de fichiers) : Comment les choisir ?

# IV. Outils informatiques (visioconférence, transfert de fichiers) : comment les choisir ?

Les outils de visioconférence ou de transfert de fichiers sont beaucoup plus utilisés dans le contexte pandémique.

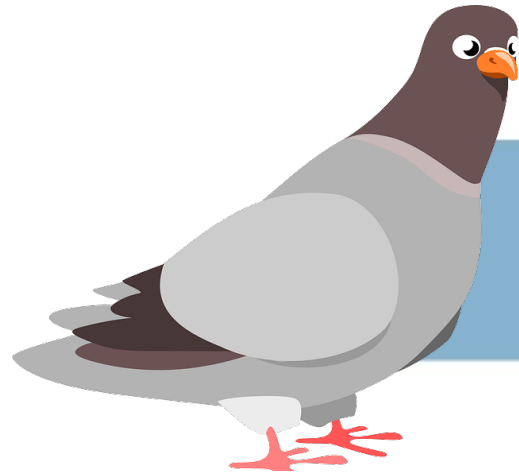


## Comment les choisir ?

Vérifier dans **les conditions d'utilisation** :  
Comment seront utilisées **vos données personnelles** ?

Utiliser des outils de transfert de fichiers garantissant que vos **données sont hébergées en France**.

# IV. Outils informatiques (visioconférence, transfert de fichiers) : comment les choisir ?



Si c'est gratuit, vous êtes le "produit" !





# V. Incidents informatiques (Cyberattaque, panne) : Comment réagir ?

# V. Cyberattaque : comment réagir ?



## En cas d'incident :

**Déconnectez immédiatement votre poste de l'internet**  
Faites rapidement **intervenir le service informatique de la collectivité** ou votre **prestataire informatique**.



Contactez votre **Délégué à la Protection des Données**

**Déposez plainte** (police, gendarmerie, procureur de la République)

**Alertez votre assureur** si vous avez un contrat « Cyber »



# Concepts clés à retenir

## Concepts clés à retenir :

La crise sanitaire est une **aubaine** pour les pirates informatiques

**Sauvegardez** régulièrement vos données et **mettez à l'abri une copie** des vos données !

**Sensibilisez et former** les personnels aux **risques informatiques**

28



## Questions – réponses avec les participant.es

# Contacts et ressources

## Le service RGPD du Cdg59 :

### Délégués à la Protection des Données :

Gauthier DUCOULOMBIER 03.59.56.88.51 [ducoulombier.g@cdg59.fr](mailto:ducoulombier.g@cdg59.fr)

Nicolas GILLIERS 03.59.56.88.50 [gilliers.n@cdg59.fr](mailto:gilliers.n@cdg59.fr)

Cellule administrative et organisationnelle : [rgpd@cdg59.fr](mailto:rgpd@cdg59.fr)

Marlène VERBEKE 03.59.56.88.18 [verbeke.m@cdg59.fr](mailto:verbeke.m@cdg59.fr)

Nathalie CAVAGNA 03.59.56.88.80 [cavagna.n@cdg59.fr](mailto:cavagna.n@cdg59.fr)

Nous contacter par voie électronique : [www.cdg59.fr/contacts/](http://www.cdg59.fr/contacts/)



## Cybermalveillance.gouv.fr : renforcement des mesures de sécurité informatique durant la crise du COVID-19

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite>



## Guide CNIL de sensibilisation au RGPD pour les collectivités territoriales

<https://www.cnil.fr/sites/default/files/atoms/files/cnil-guide-collectivite-territoriale.pdf>



## Liste des logiciels certifiés CSPN de l'ANSSI

<https://www.ssi.gouv.fr/administration/produits-certifies/cspn/produits-certifies-cspn/>



## Comment choisir son outil de webconférence par la DGAFP et la DINUM

<https://www.numerique.gouv.fr/produits-services/organiser-webconference-outils-agents-etat/>



## Infographies de l'ANSSI sur les rançongiciels et les bonnes pratiques numériques


<https://www.ssi.gouv.fr/particulier/precautions-elementaires/infographies-2/>



Merci de votre attention

## FAQ

# RGPD et sécurité informatique pendant la crise du Covid-19

Le CdG59 autorise la réutilisation de ses informations et documents dans les libertés et les conditions prévues par la licence  LICENCE OUVERTE  
OPEN LICENCE sous réserve d'apposer la mention :

«Source : CdG59, titre et lien du document ou de l'information et date de sa dernière mise à jour»