



# Ordonnance sur l'essai pilote du système suisse de traçage de proximité visant à informer les personnes potentiellement exposées au nouveau coronavirus (COVID-19)

## (Ordonnance COVID-19 essai pilote traçage de proximité)

du 13 mai 2020

---

*Le Conseil fédéral suisse,*

vu l'art. 17a, al. 1 et 3, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)<sup>1</sup>,  
vu l'art. 78, al. 1, de la loi du 28 septembre 2012 sur les épidémies (LEp)<sup>2</sup>,  
vu l'art. 25, al. 1, de la loi du 9 octobre 1992 sur la statistique fédérale<sup>3</sup>,  
*arrête:*

### Art. 1           Objet

La présente ordonnance règle l'essai pilote du système suisse de traçage de proximité (*Swiss Proximity-Tracing-System*, SPTS) visant à informer les personnes (art. 31, al. 2, et 33 LEp) qui ont potentiellement été exposées au coronavirus pendant la durée de l'essai pilote. Elle règle l'organisation, l'exploitation, les données traitées et l'utilisation du SPTS.

### Art. 2           But de l'essai pilote

<sup>1</sup> L'essai pilote sert à tester et à évaluer le SPTS en vue de sa mise en exploitation définitive.

<sup>2</sup> Les aspects suivants doivent en particulier être testés et évalués:

- a. les dernières solutions développées concernant la décentralisation du traitement des données et des méthodes de cryptographie;
- b. la stabilité de l'exploitation;
- c. la sécurité face aux manipulations involontaires ou non autorisées;
- d. la convivialité;

RS .....

- 1   RS **235.1**
- 2   RS **818.101**
- 3   RS **431.01**

- e. la clarté des informations pour les participants et les professionnels au bénéfice d'un droit d'accès.

**Art. 3** But du SPTS et des données traitées

<sup>1</sup> Le SPTS et les données qu'il permet de traiter servent les buts suivants:

- a. informer les participants potentiellement exposés au coronavirus, tout en respectant la protection des données;
- b. établir des statistiques en lien avec le coronavirus.

<sup>2</sup> Ils ne peuvent pas être utilisés à d'autres fins, en particulier ils ne peuvent servir aux autorités cantonales pour ordonner ou évaluer des mesures au sens des art. 33 à 38 LEp.

**Art. 4** Rapport avec l'ordonnance sur les épidémies

L'art. 60 LEp et les dispositions de l'ordonnance du 29 avril 2015 sur les épidémies<sup>4</sup> relatives au système d'information qu'ils visent ne sont pas applicables au SPTS.

**Art. 5** Structure du SPTS

<sup>1</sup> Le SPTS est composé des éléments suivants:

- a. un système de gestion des données relatives aux situations de rapprochement (GR), composé d'un logiciel que les participants installent sur leur téléphone portable (application) et d'un *back-end* (*back-end* GR);
- b. un système de gestion des codes, composé d'un *front-end* en ligne et d'un *back-end*.

<sup>2</sup> Le *back-end* GR et le système de gestion des codes sont exploités comme serveurs centraux par l'Office fédéral de la santé publique (OFSP).

**Art. 6** Participants à l'essai pilote

<sup>1</sup> Le cercle des participants potentiels à l'essai pilote se limite aux groupes de personnes suivants:

- a. les membres de l'armée suisse en service d'instruction, en service d'appui ou en service actif;
- b. les collaborateurs de hautes écoles;
- c. le personnel des hôpitaux et des cliniques;
- d. les employés des administrations cantonales et de l'administration fédérale;
- e. les membres d'associations voulant contribuer à l'amélioration du système.

<sup>4</sup> RS 818.101.1

<sup>2</sup> L'OFSP met à la disposition des participants, via ces institutions et associations, les informations nécessaires et l'accès technique par lequel les personnes visées à l'al. 1 peuvent télécharger l'application.

#### **Art. 7** Caractère volontaire

- <sup>1</sup> Les participants installent l'application et utilisent le SPTS sur une base volontaire.
- <sup>2</sup> Les participants sont informés qu'ils ont potentiellement été exposés au coronavirus uniquement si la personne infectée y a expressément consenti.

#### **Art. 8** Principes du traitement des données

- <sup>1</sup> Lors du traitement des données, toutes les mesures techniques et organisationnelles appropriées doivent être prises pour éviter que les participants puissent être identifiés.
- <sup>2</sup> Les données enregistrées sur le téléphone portable d'un participant et concernant d'autres participants sont traitées et enregistrées exclusivement sur ce téléphone.
- <sup>3</sup> Aucune donnée de géolocalisation n'est créée ou traitée dans le SPTS, de quelque façon que ce soit.
- <sup>4</sup> Le code source et les spécifications techniques de tous les composants du SPTS sont accessibles au public.
- <sup>5</sup> La législation fédérale en matière de protection des données s'applique.

#### **Art. 9** Organe fédéral responsable

L'OFSP est l'organe fédéral responsable du respect de la législation sur la protection des données pour tous les composants du SPTS.

#### **Art. 10** Fonctionnement de base

- <sup>1</sup> Dans le fonctionnement de base, le *back-end* GR donne aux applications un accès en ligne à son contenu. Le contenu consiste en une liste des données suivantes:
  - a. les clés privées des participants infectés qui étaient actuelles au moment où d'autres personnes ont probablement été contaminées (période pertinente);
  - b. la date de chaque clé.
- <sup>2</sup> L'application remplit les fonctions suivantes:
  - a. elle génère chaque jour une nouvelle clé privée qui ne permet pas de remonter à l'application ou au participant;
  - b. elle envoie en permanence via Bluetooth un code d'identification qui change toutes les quinze minutes, généré à partir de la clé privée actuelle mais qui ne permet ni d'identifier la clé, ni de remonter à l'application ou au participant;

- c. elle vérifie en permanence si elle reçoit des signaux compatibles émis par d'autres téléphones portables; si un autre téléphone portable se trouve à deux mètres ou moins, l'application enregistre son code d'identification actuel, la force du signal et la date et la durée approximative du rapprochement; le rapprochement est estimé à l'aide de la force des signaux reçus;
- d. depuis le *back-end* GR, elle extrait à intervalles réguliers la liste des clés privées des participants infectés et détermine sur cette base les codes d'identification y relatifs visés à la let. b; elle compare les codes d'identification à ceux qu'elle a enregistrés localement;
- e. si la comparaison révèle qu'un téléphone portable s'est rapproché à moins de deux mètres d'au moins un participant infecté et que la durée totale de cette proximité atteint ou dépasse les quinze minutes au cours de la même journée, l'application envoie une information.

#### **Art. 11**            Fonctionnement après une infection

<sup>1</sup> En cas d'infection, les professionnels disposant des droits d'accès au système de gestion des codes génèrent un code d'autorisation unique et temporaire. En outre, ils saisissent dans le système de gestion des codes le moment où les premiers symptômes sont apparus ou, si la personne infectée ne présente aucun symptôme, la date du test.

<sup>2</sup> Les professionnels disposant des droits d'accès communiquent le code d'autorisation au participant infecté. Celui-ci peut saisir le code d'autorisation dans l'application.

<sup>3</sup> Le *back-end* de gestion des codes confirme à l'application la validité du code saisi. Il retrace au maximum trois jours de la date que le professionnel disposant des droits d'accès visé à l'al. 1 a saisie. La date qui en résulte est considérée comme le début de la période pertinente. Le *back-end* de gestion des codes communique cette date à l'application de la personne infectée.

<sup>4</sup> L'application de la personne infectée transmet au *back-end* GR les clés privées qui étaient actuelles durant la période pertinente avec les dates correspondantes.

<sup>5</sup> Le *back-end* GR place les clés privées reçues et les dates correspondantes sur sa liste.

<sup>6</sup> Après la déclaration d'une infection, l'application génère une nouvelle clé privée. Celle-ci ne permet pas de remonter à d'anciennes clés privées.

#### **Art. 12**            Contenu de l'information

<sup>1</sup> L'information comprend:

- a. une information selon laquelle le participant a potentiellement été exposé au coronavirus;
- b. une indication du jour où cela s'est produit la dernière fois;
- c. les règles de conduite recommandées par l'OFSP.

<sup>2</sup> Le SPTS ne transmet aucune prescription. Il n'informe ni sur les mesures des autorités cantonales compétentes au sens des art. 33 à 38 LEp, ni sur les possibilités d'accéder à des tests de dépistage du virus.

**Art. 13** Participation de tiers à la mise à disposition des clés privées

<sup>1</sup> L'OFSP peut charger des tiers de donner aux applications un accès en ligne à la liste contenant les données visées à l'art. 10, al. 1.

<sup>2</sup> Les tiers doivent s'engager à respecter les prescriptions de la présente ordonnance.

<sup>3</sup> L'OFSP contrôle le respect des prescriptions.

**Art. 14** Contenu du système de gestion des codes

Le système de gestion des codes contient les données suivantes:

- a. les codes d'autorisation;
- b. la date à laquelle les premiers symptômes sont apparus ou, si la personne infectée ne présente aucun symptôme, la date du test;
- c. la date de la destruction des données visées aux let. a et b.

**Art. 15** Droits d'accès au système de gestion des codes

<sup>1</sup> Les personnes suivantes peuvent émettre un code d'autorisation:

- a. les médecins cantonaux;
- b. le médecin en chef de l'armée;
- c. les autres collaborateurs des services du médecin cantonal ou du service médico-militaire de l'armée;
- d. les tiers mandatés par les services des médecins cantonaux ou par le service médico-militaire de l'armée;
- e. le médecin traitant et son personnel assistant.

<sup>2</sup> L'inscription dans le système de gestion des codes passe par le système central de gestion des accès et des autorisations de l'administration fédérale pour les applications Web. Les dispositions de l'ordonnance du 19 octobre 2016 sur les systèmes de gestion des données d'identification et les services d'annuaire de la Confédération<sup>5</sup> s'appliquent.

<sup>3</sup> L'OFSP attribue et gère les droits d'accès au système de gestion des codes. Il autorise les médecins cantonaux et le médecin en chef de l'armée à attribuer des droits d'accès à leur personnel assistant.

<sup>5</sup> RS 172.010.59

**Art. 16** Journaux accès

<sup>1</sup> Les art. 57i à 57q de la loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration<sup>6</sup> et l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération<sup>7</sup> sont applicables à l'enregistrement et à l'analyse des journaux des accès au *back-end* GR et au système de gestion des codes.

<sup>2</sup> Hormis les journaux des accès et l'enregistrement des rapprochements, le SPTS n'enregistre aucun journal des activités des *front-ends* et des applications.

**Art. 17** Communication à des fins de statistiques

L'OFSP met régulièrement à la disposition de l'Office fédéral de la statistique (OFS) les données actuelles disponibles dans les deux *back-ends*, sous forme entièrement anonymisée, à des fins statistiques.

**Art. 18** Destruction des données

<sup>1</sup> Les données du système GR sont détruites à la fois sur les téléphones portables et dans le *back-end* GR 21 jours après leur saisie.

<sup>2</sup> Les données du système de gestion des codes sont détruites 24 heures après leur saisie.

<sup>3</sup> Les données journalisées des tiers mandatés au sens de l'art. 13 sont détruites 7 jours après leur saisie.

<sup>4</sup> Pour le reste, les données journalisées sont détruites conformément à l'art. 4, al. 1, let. b, de l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération<sup>8</sup>.

<sup>5</sup> Les données mises à la disposition de l'OFS sont également détruites conformément à cet article.

**Art. 19** Désinstallation de l'application, installation de la version définitive

À la fin de l'essai pilote, les institutions et associations visées à l'al. 6, al. 1, invitent les participants concernés à désinstaller eux-mêmes l'application de leur téléphone portable ou à installer la version définitive de l'application, pour autant que le SPTS reste en exploitation et qu'ils souhaitent continuer à participer.

**Art. 20** Évaluation de l'essai pilote

<sup>1</sup> Le Département fédéral de l'intérieur informe en permanence le Conseil fédéral et l'Assemblée fédérale de l'essai pilote.

<sup>6</sup> RS 172.010

<sup>7</sup> RS 172.010.442

<sup>8</sup> RS 172.010.442

<sup>2</sup> Il fait rapport au Conseil fédéral sur l'essai au plus tard un mois après la fin de l'essai pilote.

**Art. 21**            Entrée en vigueur et durée de validité

La présente ordonnance entre en vigueur le 14 mai 2020 à 0 h 00<sup>9</sup> et a effet jusqu'au 30 juin 2020.

...

Au nom du Conseil fédéral suisse:

La présidente de la Confédération, Simonetta  
Sommaruga

Le chancelier de la Confédération, Walter  
Thurnherr

<sup>9</sup> Publication urgente du 13 mai 2020 au sens de l'art. 7, al. 3, de la loi du 18 juin 2004 sur les publications officielles (RS 170.512)

