Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'intérieur DFI
Office fédéral de la santé publique OFSP

Utilisation de l'application SwissCovid: déclaration de confidentialité de l'Office fédéral de la santé publique

Version : 24 juin 2020

Dans la présente déclaration de confidentialité, l'Office fédéral de la santé publique (OFSP) explique dans quelle mesure il traite les données personnelles en lien avec l'utilisation de l'application SwissCovid (ci-après « l'application ») en suisse. Il ne s'agit pas d'un descriptif exhaustif ; certains éléments spécifiques peuvent être réglés dans des déclarations de confidentialité supplémentaires, des documents similaires, des conditions d'utilisation ou des programmes d'application.

La législation sur la protection des données règle le traitement de données personnelles. La législation fédérale sur la protection des données s'applique au traitement des données. La déclaration de confidentialité est en outre conforme à la loi du 28 septembre 2012 sur les épidémies (LEp ; RS *818.101*) et l'ordonnance COVID-19 du 24 juin 2020 sur l'essai pilote du traçage de proximité (RS *818.101.25*).

On entend par données personnelles toutes les informations qui se rapportent à une personne identifiée ou identifiable. Par traitement, on entend toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données.

1 Responsable

Le responsable du traitement des données décrit dans le présent document est l'

Office de la santé publique OFSP
3003 Berne
Suisse
Tél. +41 58 462 69 98
recht(at)bag.admin.ch

2 Collecte et traitement de données personnelles

Tout le système de l'application est conçu de manière à ce que ses utilisateurs ne soient pas identifiables. Le traitement de données personnelles est réduit au minimum. Ainsi, aucune indication technique sur les personnes, les lieux ou les appareils n'est possible. Les géolocalisations ne sont pas enregistrées ; seules des données cryptées relatives aux contacts ayant eu lieu sont saisies. Ces données sont techniquement protégées de toute utilisation abusive. L'OFSP ne peut tirer aucune conclusion concernant les utilisateurs de l'application. Cette dernière protège les données des utilisateurs de telle sorte qu'aucun lien ne peut être établi avec une personne précise sur de longues distances. Un rattachement à un individu ne peut toutefois pas être totalement exclu. Il existe en effet une certaine probabilité qu'une personne alertée d'un possible risque d'infection puisse éventuellement tirer des conclusions sur l'identité de la personne infectée, en se remémorant les

contacts sociaux qu'elle a eus au cours des derniers jours. Cette notification inclut l'information selon laquelle la personne a pu être exposée au coronavirus, la mention du jour où ce fut le cas pour la dernière fois, l'indication que l'OFSP propose une infoline pour un conseil gratuit et les recommandations de l'OFSP. En utilisant l'application, des personnes sont donc potentiellement identifiables.

Le système de l'application se divise en deux composantes :

- un système pour gérer les données relatives aux situations de rapprochement, comprenant un logiciel que les utilisateurs installent sur leur téléphone portable ainsi qu'un *backend* (*backend* GR) ;
- un système de gestion des codes d'autorisation des notifications, comprenant un *frontend* et un *backend* web.

Les deux *backends*, en tant que serveur central, sont placés directement sous le contrôle de l'OFSP et gérés sur le plan technique par l'Office fédéral de l'informatique (OFIT). Les *frontends* de gestion des codes fonctionnent sur les appareils des professionnels autorisés à créer des codes d'autorisation (codes COVID).

L'application enregistre les données suivantes sur le téléphone portable:

- les codes d'identification (ID aléatoires) reçus des autres téléphones portables où l'application est activée,
- la puissance du signal,
- la date et la durée estimée de la situation de rapprochement.

Si l'infection d'un utilisateur est confirmée, les données suivantes sont enregistrées dans le système de gestion des codes :

- le code d'autorisation (code COVID),
- la date à laquelle les symptômes sont apparus ou, si l'utilisateur infecté ne présente pas de symptômes, la date du test,
- la date de la destruction de ces données.

Le *backend* GR est constitué de la liste de données suivantes :

- les clés privées de l'utilisateur infecté qui étaient actuelles durant la période où d'autres personnes ont pu être infectées,
- la date de chaque clé.

3 Buts et bases légales

Le système d'application exploité par l'OFSP se fonde sur la LEp et l'ordonnance COVID-19 sur l'essai pilote du traçage de proximité. L'application et le traitement des données entrantes par ce moyen servent exclusivement à informer les utilisateurs potentiellement exposés au coronavirus, tout en respectant la protection des données, et à établir des statistiques en lien avec le coronavirus à l'aide de données issues des deux *backends*.

4 Transmission des données

La liste des données du *backend* GR est mise à la disposition de l'application (ou *frontend*) dans la procédure d'appel. Si l'OFSP mandate des tiers, suisses ou de l'étranger, ces opérateurs s'engagent contractuellement à respecter les prescriptions de l'art. 60*a* LEp et de l'ordonnance COVID-19 sur l'essai pilote du traçage de proximité. En est exclue la réglementation concernant le code source en vertu de l'art. 60*a*, al. 5, let. e, LEp. L'OFSP contrôle le respect des prescriptions. Les tiers mandatés n'ont pas le droit d'utiliser à des fins personnelles les données secondaires générées durant l'exécution du contrat. Ces données sont analysées seulement par l'OFSP ou par l'OFIT (cf. ch. 8).

L'OFSP met régulièrement à la disposition de l'Office fédéral de la statistique (OFS) le stock actuel de

données existantes dans les deux *backends* sous forme anonymisée. L'OFIT gère le logiciel dans son ensemble sur mandat de l'OFSP et fournit le service de soutien technique requis. L'OFIT a uniquement accès à des données lorsque cela s'avère nécessaire pour les buts et les activités spécifiques des collaborateurs concernés. Ces derniers sont tenus à la confidentialité lorsqu'ils traitent les données.

L'application utilise une interface reliée au système d'exploitation du téléphone portable de l'utilisateur, qui nécessite le traitement des données par Apple ou Google. Les fonctionnalités des systèmes d'exploitation utilisées par l'interface doivent remplir les prescriptions de l'art. 60*a* LEp et de l'ordonnance COVID-19 sur l'essai pilote du traçage de proximité. En est exclue la réglementation concernant le code source en vertu de l'art. 60*a*, al. 5, let. e, LEp. L'OFSP veille à ce que cette prescription soit respectée, notamment en obtenant les assurances correspondantes.

5 Durée de conservation

Les données sont supprimées dès qu'elles ne sont plus nécessaires pour la notification des utilisateurs. Elles sont supprimées comme suit :

- données du système servant à gérer les données relatives aux rapprochements (aussi bien dans le téléphone portable que dans le *backend* GR) : 14 jours après leur saisie
- données du système des codes : 24 heures après leur saisie

6 Sécurité des données

Afin de protéger les données contre des accès non autorisés, des pertes ou des utilisations abusives, l'OFSP, en étroite collaboration avec ses fournisseurs d'hébergement internes et externes et avec d'autres prestataires informatiques, prend des mesures de sécurité adéquates, de nature technique (p. ex., cryptage, pseudonymisation, historique, contrôles d'accès, limitations d'accès, sécurité des données, solutions concernant la sécurité des technologies informatiques et des réseaux, etc.) et de nature organisationnelle (p. ex., directives aux collaborateurs, contrats de confidentialité, contrôles, etc.) conformément aux prescriptions de l'administration fédérale et de la législation fédérale en matière de protection des données.

7 Droits des personnes concernées

Vous avez le droit à l'information, à la rectification, à l'effacement, ou à la remise de vos données. Vous avez également le droit d'exiger la limitation du traitement des données et le droit de contester la manière dont vos données sont traitées. Par ailleurs, vous avez le droit de révoquer vos autorisations, sans que la licéité du traitement des données effectué jusque-là ne soit affectée. Ces droits s'appliquent pour autant qu'il existe des données personnelles. Le principe du « *privacy by design* », au cœur de l'application, est conçu, grâce à des méthodes cryptographiques innovantes et à un traitement décentralisé des données, pour éviter autant que possible de disposer d'informations sur des personnes identifiées ou identifiables (données personnelle). Pour cette raison, l'OFSP n'a pas la possibilité, par exemple, de fournir d'informations concernant les rapprochements enregistrés pour une personne ou de rectifier ces données. L'OFSP ne peut pas consulter ces données, étant donné qu'elles sont sauvegardées uniquement sur les téléphones portables.

L'exercice de ces droits implique que vous déclinez clairement votre identité (p. ex., au moyen d'une copie de votre pièce d'identité). Pour faire valoir vos droits, vous pouvez contacter l'OFSP à l'adresse indiquée au chiffre 1.

En cas d'infraction au droit de la protection des données, vous pouvez vous adresser à l'autorité de contrôle de la protection des données compétente ou saisir la justice en invoquant la législation sur la protection des données.

8 Autres

Des journaux des accès au *backend* GR et au système de contrôle du code source sont enregistrés pour les buts fixés aux art. 57*l* à 57*o* de la loi sur l'organisation du gouvernement et de l'administration (LOGA ; RS *172.010*). Ils peuvent être analysés à des fins statistiques. Les art. 57*i*–57*q* LOGA et l'ordonnance du 22 février 2012 sur le traitement des données personnelles liées à l'utilisation de l'infrastructure électronique de la Confédération (RS *172.010.442*) s'appliquent.

Les données relatives à l'historique sont détruites comme suit :

- par des tiers mandatés par l'OFSP : sept jours après leur saisie ;
- en outre, la destruction de ces données est conforme 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 (RS *172.010.442*).

9 Modifications

L'OFSP peut adapter la présente déclaration de confidentialité à tout moment, sans préavis. La version actuelle publiée et la version valable pour la période concernée s'appliquent. La présente déclaration de confidentialité a été rédigée en plusieurs langues. La version allemande fait foi en cas de divergences. En cas d'actualisation, les utilisateurs de l'application sont informés des changements de manière adéquate.

*****