Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Rapport final et recommandations

du Préposé fédéral à la protection des données et à la transparence (PFPDT)

du 4 août 2021

dans le cadre
de la procédure d'établissement des faits selon l'article 29
de la Loi fédérale sur la protection des données du 19 juin 1992
(LPD ; RS 235.1)

concernant
l'application « SocialPass »
de SwissHelios Sàrl, à Oberlunkhofen
et NewCom4U Sàrl, à Sierre

représentées par Lexing Switzerland, 1951 Sion
(jusqu'au 14 juin 2021)

Feldeggweg 1, 3003 Berne
Tél. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

Table des matières

1. Introduction

1.1. Remarques préliminaires

Le Préposé fédéral à la protection des données et à la transparence (PFPDT) établit les faits d'office ou à la demande de tiers lorsqu'une méthode de traitement est susceptible de porter atteinte à la personnalité d'un nombre important de personnes (erreur de système ; art. 29 LPD).

La présente procédure a pour but de permettre au PFPDT de vérifier si les principes de la protection des données tels que fixés aux articles 4 et 7 LPD et les prescriptions sanitaires en matière de traçage sont respectés dans le cadre de l'exploitation et l'utilisation du système SocialPass.

1.2. Situation de départ

Dans le but de mieux lutter contre la pandémie de COVID-19, le Conseil fédéral a prévu dans l'Ordonnance sur les mesures destinées à lutter contre l'épidémie de COVID-19 en situation particulière du 22 juin 2020 (Ordonnance Covid-19 situation particulière ; RS 818.101.26) que les exploitants d'installations ou d'établissements accessibles au public doivent collecter les coordonnées des participants ou des visiteurs. La collecte des coordonnées (données personnelles au sens de l'art. 3 lit. a LPD) a pour but de pouvoir retracer des cas d'éventuelles infections au sein d'un restaurant ou de tout autre établissement ou événement accessible au public. À cette fin, les exploitants et les organisateurs sont tenus de collecter le nom, le prénom, le domicile et le numéro de téléphone de leurs clients (ch. 4.4. lit. a de l'Annexe 1 Ordonnance COVID-19 situation particulière). L'art. 5 Ordonnance COVID-19 situation particulière précise que les personnes concernées doivent être informées de cette collecte de données et du but de l'utilisation de leurs données (traçage des contacts). Les coordonnées doivent être immédiatement transmises par voie électronique au service cantonal compétent s'il en fait la demande aux fins d'identification et d'information des personnes présumées infectées au sens de l'art. 33 de la Loi sur les épidémies (LEp ; RS 818.101). De surcroit, l'Ordonnance situation particulière fixe que les coordonnées collectées ne peuvent pas être utilisées à d'autres fins que celle du traçage et qu'elles doivent être conservées durant les 14 jours suivant la visite de l'établissement puis immédiatement détruites.

Afin de faciliter la collecte desdites données dans le cadre de la lutte contre la pandémie, les sociétés SwissHelios et NewCom4U ont développé SocialPass. Ce système est composé essentiellement de trois composants : l'application SocialPass peut être téléchargée sur l'appareil mobile des clients et visiteurs tandis que l'application SocialScan est utilisée par les établissements accessibles au public comme p.ex. les restaurants. Les données sont ensuite stockées sur une base de données centrale.

Dans le cadre de la présente procédure le terme « SocialPass » fera référence – sauf mention contraire – au système entier, englobant notamment les applications mobiles SocialPass et SocialScan ainsi que la base de données centralisée.

À partir du mois de juillet 2020, le PFPDT a reçu plusieurs demandes de citoyens ainsi que des médias suggérant que les traitements de données tels que prévus par SocialPass violeraient potentiellement le cadre légal prévu par la LPD et les prescriptions sanitaires en matière de traçage. Dans le cadre de sa fonction d'autorité de surveillance, le PFPDT a alors pris contact avec les responsables de ladite application en novembre 2020. Cette prise de contact devait permettre au PFPDT de vérifier si les critiques émanant de la société civile d'une part et de la presse d'autre part étaient fondées. Dans le but d'apporter des réponses plus précises aux questions soulevées lors de la première prise de contact en automne 2020, le PFPDT a ouvert, en décembre 2020, une procédure d'établissement des faits selon l'art. 29 LPD, d'abord à l'encontre de la SwissHelios Sàrl, puis à l'encontre de la NewCom4U Sàrl. Les deux procédures ont été formellement jointes le 4 mars 2021.

1.3. Parties impliquées

Les personnes physiques et morales ayant un rôle déterminant dans la présente procédure d'établissement des faits sont les suivantes :

Exploitants de SocialPass:

SwissHelios Sàrl, Wiesenstrasse 7a, 8917 Oberlunkhofen, agissant par M. Erwin Peter, associé et président des gérants et M. Julio Salgado, associé et gérant ;

NewCom4U Sàrl, Technopôle 3, 3960 Sierre, agissant par M. Thierry Pilet, associé et gérant ;

représentées par Me Sébastien Fanti, Me Géraldine Gianadda et Me Alexandre Staeger, avocats au sein de l'étude Lexing Switzerland Sàrl, Rue de Pré-Fleuri 8B, 1951 Sion.

Responsables du dossier auprès du PFPDT :

Nathalie Weber, Cheffe Team 1, Domaine de direction protection des données

Myriam Christ, Juriste Team 1, Domaine de direction protection des données

Fritz von Allmen, Spécialiste en sécurité informatique, Centre de compétence IT et Société numérique

Michael Burger, Spécialiste en sécurité informatique, Centre de compétence IT et Société numérique

1.4. Chronologie des événements

Juillet-Oct. 2020	**Plusieurs indices de la part de la société civile**, des médias et de la Fédération romande des consommateurs par rapport à des traitements de données effectués par l'application SocialPass potentiellement contraires au cadre légal.
23.10.2020	**Prise de contact par le PFPDT** par écrit après un échange téléphonique avec SwissHelios Sàrl le 23.10.2020, demande de précisions quant à la confidentialité et la sécurité des données et la double authentification.
03.11.2020	Courriel du PFPDT à SwissHelios Sàrl concernant la demande du 23.10.2020 restée sans réponse, questions complémentaires avec délai de réponse jusqu'au 09.11.2020.
03.11.2020	Demande de SwissHelios Sàrl de mettre le cabinet d'avocats Lexing Switzerland, Sion en copie.
09.11.2020	Courriel de Lexing Switzerland informant le PFPDT d'intervenir pour SwissHelios Sàrl, demande d'adresser toute correspondance ultérieure à Lexing Switzerland (élection de domicile en l'étude Lexing Switzerland).
09.11.2020	Courriel de SwissHelios Sàrl au PFPDT, complément aux réponses reçues par Lexing Switzerland, NewCom4U Sàrl fait sa première apparition dans la présente affaire et lit ce courriel en copie.
10.11.2020	Courriel du PFPDT à SwissHelios Sàrl, accusé de réception des réponses sommaires, reprise de contact prévue après évaluation interne des réponses reçues.
10.11.2020	Courriel de SwissHelios Sàrl d'adresser toute communication ultérieure directement à SwissHelios Sàrl.
11.11.2020	Courriel du PFPDT à Lexing Switzerland de la demande de SwissHelios Sàrl de communiquer directement avec SwissHelios.
26.11.2020	Courriel du PFPDT à SwissHelios Sàrl et NewCom4U Sàrl demandant des précisions jusqu'au 04.12.2020.
07.12.2020	Courriel du PFPDT à SwissHelios Sàrl et NewCom4U Sàrl, rappel suite à la demande du 26.11.2020 restée sans réponse, réponse par NewCom4U Sàrl faisant valoir des problèmes linguistiques.
08.12.2020	Courriel du PFPDT à SwissHelios Sàrl et NewCom4U Sàrl concernant les problèmes linguistiques mis en avant par les exploitants.
18./23.12.2020	Courrier recommandé (avec copie préalable par courriel) du PFPDT à SwissHelios Sàrl (le 18.12.2020) et à NewCom4U Sàrl (le 23.12.2020), demande

	de précisions du 26.11.2020 restée sans réponse, **ouverture de la procédure d'établissement des faits selon l'art. 29 LPD**.
11.01.2021	Courriel de Lexing Switzerland au PFPDT demandant une prolongation du délai de réponse, prolongation accordée par le PFPDT par courriel du 12.01.2021.
14.01.2021	Courriel de Lexing Switzerland au PFPDT, envoi de trois documents (*Privacy and Cookies Policy – socialpass – 14102020.docx ; Rapport technique SocialPass 14.01.2021.pdf ; Réponses aux questions – PFPDT.docx).*
15.01.2021	Courriel de Lexing Switzerland au PFPDT, envoi d'une procuration (incomplète).
26.01.2021	Courriel de Lexing Switzerland au PFPDT, envoi d'une procuration (complète) pour le compte de NewCom4U Sàrl.
29.01.2021	Échange téléphonique entre SwissHelios Sàrl et le PFPDT concernant la représentation de SwissHelios Sàrl par Lexing Switzerland.
03.02.2021	Courriel du PFPDT à Lexing Switzerland, accusé de réception des documents reçus, délai pour soumettre les documents manquants fixé au 10.02.2021.
09.02.2021	Courriers du PFPDT à Lexing Switzerland et à SwissHelios Sàrl, avis relatif à la jonction prévue des procédures, soumission de questions supplémentaires (responsables des traitements de données, détails sur le transfert des numéros de téléphone aux États-Unis), délai de réponse fixé au 17.02.2021.
11.02.2021	Courriel de Lexing Switzerland au PFPDT, soumission de deux rapports d'audit.
18.02.2021	Courrier de Lexing Switzerland au PFPDT, demande de prolongation de délai.
19.02.2021	Courrier du PFPDT à Lexing Switzerland, prolongation de délai accordée, au 26.02.2021 pour la question de la jonction de procédure, au 05.03.2021 pour les réponses aux questions supplémentaires.
04.03.2021	Courriers du PFPDT à Lexing Switzerland et à SwissHelios Sàrl, avis relatif à la jonction définitive des procédures, demande de précisions, demande de divers documents manquants, questions supplémentaires sur divers aspects restés peu clairs, délai fixé au 17.03.2021 (entrant).
05.03.2021	Courrier de Lexing Switzerland au PFPDT, avec des réponses sur la question du maître du fichier (SwissHelios Sàrl) et concernant le transfert des numéros aux États-Unis.
17.03.2021	Courrier de Lexing Switzerland au PFPDT, confirmant d'intervenir au nom et pour le compte de NewCom4U Sàrl et de SwissHelios Sàrl (une procuration serait fournie ultérieurement), comprenant un nombre d'annexes et de réponses aux questions posées.
19.03.2021	Courriel de NewCom4U Sàrl au PFPDT, envoi du rapport Navixia.

22.03.2021	Courriel de Lexing Switzerland au PFPDT précisant que SwissHelios Sàrl estime qu'une procuration formelle n'est pas nécessaire, confirmation qu'aucun autre document était disponible.
25.03.2021	Courriel de NewCom4U Sàrl au PFPDT soumettant quelques informations actualisées sur SocialPass.
07.04.2021	Courrier du PFPDT à Lexing Switzerland, **recommandation provisoire** d'adapter au plus vite les possibilités de traitements de manière à ce qu'il soit possible d'exploiter l'application en conformité avec le droit fédéral (avant la réouverture des restaurants).
21.04.2021	Courriel du PFPDT à Lexing Switzerland, le courrier du 07.04.2021 (recommandations provisoires) étant resté sans retour demande de confirmer jusqu'au 26.04.2021 que les fonctions de recherches ciblées seront adaptées ainsi que comment et dans quel délai cela serait fait.
23.04.2021	Courrier de Lexing Switzerland informant le PFPDT que la **recommandation provisoire ne sera pas suivie**, soumission de divers documents.
20.05.2021	Courrier du PFPDT à Lexing Switzerland, **notification des faits établis** provisoirement et possibilité de présenter des remarques aux faits établis jusqu'au 27.05.2021 (entrant) mentionnant qu'au vu de la réouverture probable de l'intérieur des restaurants le 31.05.2021, une prolongation de délai était exclue.
21.05.2021	Courrier de Lexing Switzerland au PFPDT, demande de prolongation de délai de réponse d'au moins 30 jours.
25.05.2021	Courrier du PFPDT à Lexing Switzerland, refus de la demande de prolongation de délai notant que des remarques pourront toujours être faites dans le délai imparti.
27.05.2021	Courrier de Lexing Switzerland au PFPDT, **demande de récusation** des collaborateurs en charge du dossier.
28.05.2021	Courrier du PFPDT à Lexing Switzerland, décision de non-entrée en matière par rapport à la demande de récusation (et notification de la décision aux Commissions de gestion des Chambres fédérales en tant qu'autorité de surveillance du PFPDT).
28.05.2021	Courrier du PFPDT à Lexing Switzerland, **clôture et notification du rapport final et des recommandations**, les parties disposent d'un délai de 30 jours pour prendre position.
01.06.2021	Courriel de GastroVaud, GastroValais et les exploitants de SocialPass adressé au PFPDT, aux Préposés cantonaux vaudois et valaisans et aux Médecins cantonaux vaudois et valaisans, proposition d'une visioconférence.

07.06.2021	1ère visioconférence organisée par GastroVaud à laquelle participent, entre autres, les exploitants de SocialPass et leur avocat (agissant également en tant que Préposé valaisan à la protection des données), une représentante de la Préposée à la protection des données du canton de Vaud, les médecins cantonaux vaudois et valaisans et le Préposé fédéral, M. Adrian Lobsiger, ainsi que trois représentants de son autorité. Proposition d'une démonstration du système par les exploitants de SocialPass dans le cadre d'une deuxième visioconférence.
08.06.2021	Courrier du PFPDT à Lexing Switzerland résumant les résultats de la visioconférence du 07.06.2021.
14.06.2021	Courrier de Lexing Switzerland au PFPDT notifiant la **fin du mandat de Lexing Switzerland** dans la présente procédure.
18.06.2021	Courriel de SwissHelios Sàrl au PFPDT par rapport à une démonstration du système, demande de prolongation de délai de 30 jours pour commenter le rapport final, la **demande de récusation du 27.05.2021 est retirée**.
24.06.2021	2ème visioconférence organisée par les exploitants de SocialPass à laquelle ont participé, entre autres, les collaborateurs du PFPDT en charge du dossier, les médecins cantonaux vaudois et valaisans, la préposée cantonale vaudoise et le représentant légal de GastroVaud.
29.06.2021	Courrier du PFPDT à SwissHelios Sàrl et NewCom4U Sàrl, confirmation de la prolongation de délai jusqu'au 16.07.2021.
09.07.2021	**Soumission de la prise de position des exploitants de SocialPass**.
04.08.2021	**Clôture de la procédure d'établissement des faits** et notification du rapport final complété, avis de la publication du présent rapport sur le site internet du PFPDT.

1.5. Portée de la procédure d'établissement des faits

La présente procédure a pour but de permettre au PFPDT de vérifier si les principes de la protection des données tels que fixés notamment aux articles 4 et 7 LPD ainsi que les prescriptions sanitaires en matière de traçage sont respectées dans le cadre de la gestion de SocialPass.

Les analyses portent essentiellement sur la question de savoir quels traitements de données sont effectués par SocialPass. Il convient de distinguer ces traitements du traitement (éventuellement plus étendu) de données effectué par les établissements accessibles au public et de l'éventuel traitement ultérieur par les autorités cantonales compétentes (en cas d'infection au COVID-19).

La présente procédure porte essentiellement sur le traitement des données des visiteurs d'établissements ou d'événements ; l'application SocialScan, utilisée par les établissements, n'est

incluse dans la présente procédure que dans la mesure où elle est pertinente au regard des données des visiteurs.

Dans cette perspective, le PFPDT examine les aspects suivants du traitement des données dans le cadre de l'utilisation de l'application SocialPass :

- Quels sont les types de traitements de données effectués par SocialPass ?
- Quelles sont les catégories de données personnelles traitées dans le cadre de l'utilisation de SocialPass ?
- Qui traite les données ?
- Dans quel but les données sont-elles traitées, pour quelle durée ?
- Quelles mesures de sécurité et de protection des données ont été mises en place ?

Les traitements de données effectués lors de la visite du site web www.socialpass.ch ne font expressément pas l'objet de la présente procédure. De même, les traitements de données effectués lors du téléchargement de l'application SocialPass ou SocialScan dans l'AppStore ou dans le PlayStore ne sont pas analysés dans le cadre de la présente procédure. Les composants du système « CRM » et les sites web des deux entreprises SwissHelios et NewCom4U n'ont pas non plus été examinés en profondeur. Il est apparu, lors de l'examen initial, que ces composants ne sont pas directement impliqués dans le traitement des données des personnes concernées, respectivement qu'il n'existe pas d'interfaces ou de flux de données vers les coordonnées collectées.

1.6. Bases de l'établissement des faits

Le PFPDT s'appuie sur les sources suivantes pour la présente procédure d'établissement des faits:

- Informations accessibles au public, notamment sur le site web www.socialpass.ch et dans l'AppStore (iOS) et le PlayStore (Android) ;
- Correspondance avec les représentants de SwissHelios et NewCom4U depuis l'automne 2020 ;
- Rapports d'audits et documents supplémentaires fournis par les parties selon le tableau ci-dessous.

Audits

Tableau 1: Rapports d'audit

Nr.	Rapport d'audit	Auteur	Date
[A]	GVD7009_Recheck_SocialPass_SocialScanv1.2.pdf	Navixia	18.03.2021
[B]	iOS Mobile Application Audit Report of Social Scan v1.0.pdf	Indusface	04.11.2020

[C]	Android Mobile Application Audit Report of Social Scan v1.0.pdf	Indusface	04.11.2020

Documents supplémentaires

Tableau 2: Documents référencés complémentaires

Nr.	Document	Auteur	Date
[D]	Rapport technique SocialPass 14.01.2021.pdf	L. Miceli	14.01.2021
[E]	Fanti_Diagramme.pptx	S. Fanti	09.11.2020
[F]	SocialPass - SocialScan Uebersicht - d.pdf	SocialPass	09.11.2020
[G]	Réponses aux questions PFPDT 17032021 - scan.pdf	A. Staeger	17.11.2021
[H]	2021_03_11_QuestionnaireTechnique V1.pdf	L. Miceli	17.03.2021
[I]	Azure-Sentinel-whitepaper.pdf	Microsoft	17.03.2021
[J]	Privacy and Cookies Policy - socialpass - 14102020.docx	SwissHelios	10.10.2020
[K]	2021_03_11_QuestionnaireTechnique.docx	PFPDT	11.03.2021

À plusieurs reprises le PFPDT s'est adressé aux exploitants de l'application pour savoir si d'autres informations et documents pertinents étaient disponibles pour assurer le meilleur déroulement possible de la présente procédure. Le PFPDT souhaitait notamment savoir quels composants du système avaient fait l'objet de contrôles de sécurité, le cas échéant par des spécialistes externes, et s'il existait des résultats documentés, par exemple sous la forme d'évaluations de sécurité et de rapports de vulnérabilité.

En dehors des documents mentionnés dans ce sous-chapitre, les exploitants de l'application ont assuré le PFPDT qu'aucun examen de ce type (par exemple pour le stockage de données chez Microsoft Azure) n'a été effectué et qu'ils étaient donc dans l'impossibilité de transmettre les résultats d'un tel examen au PFPDT.

1.7. Analyses effectuées dans le cadre de la présente procédure

L'analyse technique de l'application SocialPass du PFPDT s'appuie sur les rapports d'audit des entreprises Indusface du 4 novembre 2020 et Navixia du 18 mars 2021 ainsi que sur les documents supplémentaires soumis au PFPDT par les représentants des sociétés SwissHelios et NewCom4U. Lesdits rapports d'audit ont été rédigés entre les mois d'octobre 2020 et mars 2021.

Aucune inspection des lieux en compagnie des responsables de SocialPass n'a eu lieu. Ainsi, toutes les informations – tant de nature technique que juridique – qui ont été jugées déterminantes pour l'établissement des faits ont été exigées des représentants légaux des sociétés SwissHelios et NewCom4U par écrit. Les questions du PFPDT s'appuyaient sur le cadre légal tel que prévu par la LPD

et les prescriptions sanitaires en matière de traçage, la norme ISO 27002 ainsi que sur l'Open Web Application Security Project (OWASP).

1.8. Bases légales

Les bases légales suivantes sont pertinentes dans le cadre de la présente procédure :

- Loi fédérale du 19 juin 1992 sur la protection des données (LPD), RS 235.1
- Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD), RS 235.11
- Loi fédérale sur la lutte contre les maladies transmissibles de l'homme (Loi sur les épidémies, LEp), RS 818.101
- Ordonnance sur les mesures destinées à lutter contre l'épidémie de COVID-19 en situation particulière du 19 juin 2020 (Ordonnance COVID-19 situation particulière), RS 818.101.26

1.9. Compétence du PFPDT

En vertu de l'art. 2 al. 1er LPD, la LPD régit le traitement de données concernant des personnes physiques et morales effectué par des personnes privées (physiques ou morales). La présente procédure d'établissement des faits se penche sur différents traitements de données effectués par des entités privées, notamment la collecte puis l'enregistrement des coordonnées des visiteurs effectués par les exploitants d'établissements ouverts au public dans le cadre de la lutte contre la pandémie du COVID-19. Dès lors, la collecte des coordonnées des visiteurs telle que prévue par l'Ordonnance COVID-19 situation particulière est une activité privée soumise à la LPD et par conséquent à la surveillance du PFPDT. Au contraire, le traitement des données (ultérieur) par les autorités cantonales (médecin cantonal, direction de la santé publique, équipe de traçage) tombe sous la surveillance des préposés cantonaux respectifs.

2. Faits établis

2.1. Rôles et responsabilités

Force est de constater qu'au bas du site web www.socialpass.ch consacré à l'information des citoyennes et citoyens, les coordonnées de Swisshelios Sàrl ainsi que celles de HotelPro4U (produit de marketing développé par la société NewCom4U Sàrl) sont mentionnées. Ainsi, sur le site web, les deux sociétés apparaissent comme co-éditrice de l'application SocialPass. Le fait qu'il s'agit d'une coédition semble être confirmé par les conditions générales SocialPass et SocialScan (cf. https://www.socialpass.ch/termes-et-conditions/, version du 17 avril 2021, ch. 1). En vertu du ch. 3 de

la déclaration de confidentialité – également disponible sur le site web1 – NewCom4U Sàrl est l'unique société responsable du traitement et maître du fichier.

De surcroît, et dans l'AppStore et dans le PlayStore, SwissHelios GmbH est mentionné comme unique distributeur de SocialPass.

Enfin, dans leur courrier du 26.04.2021, les représentants des exploitants de SocialPass font référence à plusieurs documents selon lesquels les exploitants de SocialPass ont été mandaté par le canton du Valais et GastroVaud respectivement. Sur la base de la documentation à notre disposition, GastroVaud aurait mandaté SwissHelios Sàrl alors que le canton du Valais aurait mandaté NewCom4U Sàrl pour l'exploitation de SocialPass.

2.2. Composants et fonctions

2.2.1. Aperçu

Le système SocialPass se base essentiellement sur une application pour les entreprises (SocialScan, cf. chapitre 2.2.3), une application pour les utilisateurs (SocialPass, cf. chapitre 2.2.4) et une base de données centrale (cf. chapitre 2.2.5). Un aperçu du fonctionnement de SocialPass sous forme d'un schéma est à disposition sous https://www.socialpass.ch/comment-cela-fonctionne/ (état au 08.05.2021).

Les exploitants de l'application SocialPass ont mis à disposition du PFPDT la figure 1. Cette figure a servi de base pour l'analyse technique. Par la suite, notamment en raison du développement de l'application, l'illustration a été complétée.

Pour la collecte des coordonnées des visiteurs, le système SocialPass prévoit deux possibilités :

- Grâce à l'application SocialPass le visiteur scanne un code-QR imprimé.
- L'exploitant de l'établissement accessible au public scanne le code-QR des visiteurs. Le schéma suivant illustre la deuxième possibilité de collecter les coordonnées des visiteurs.

[1] https://www.socialpass.ch/mentionslegales/

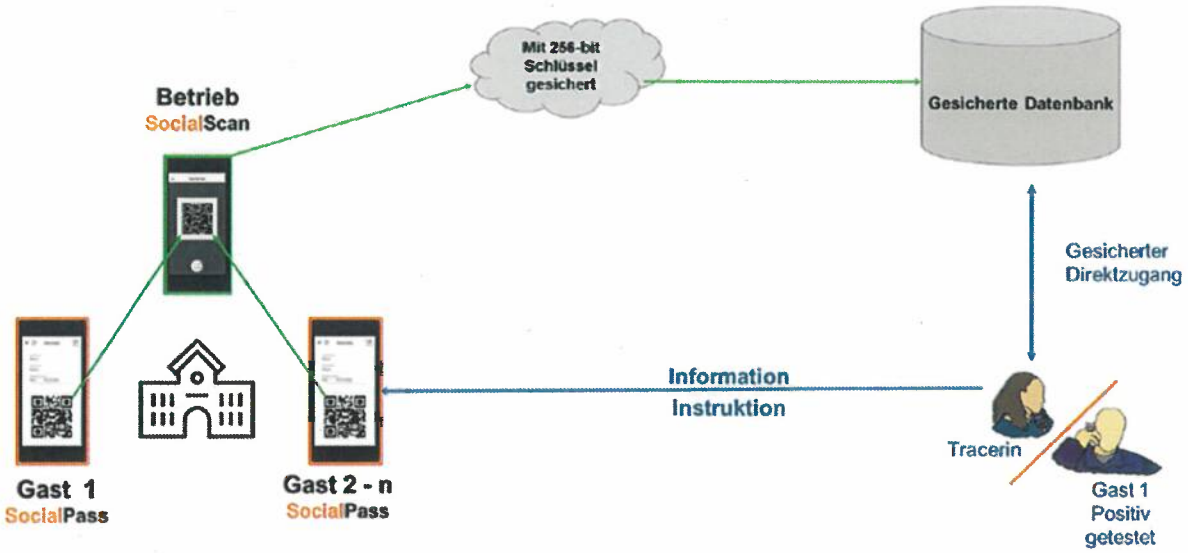

Figure 1: Schéma tel que figurant dans le document SocialPass-SocialScan Uebersicht-d.pdf

2.2.2. Description du processus d'enregistrement

(1) Après avoir installé l'application, celle-ci est ouverte et après avoir sélectionné la langue appropriée (allemand, anglais, français, italien ou espagnol), les conditions d'utilisation, y compris la déclaration de confidentialité, apparaissent. Celles-ci peuvent être soit acceptées soit rejetées.

(2) Après avoir accepté les conditions d'utilisation, l'utilisateur doit saisir son numéro de téléphone. Ensuite, un masque d'enregistrement apparaît, dans lequel il doit impérativement indiquer son nom, son prénom et son code postal. Il importe peu que les données soient correctes ou non, à l'exception du numéro de téléphone.

(3) En cliquant sur « inscription », les données spécifiées sont envoyées à « Twilio » (service tiers américain). Au cours de ce processus, un code QR est généré et stocké sur l'appareil mobile de l'utilisateur. Cela signifie qu'un visiteur d'un établissement (par exemple d'un restaurant) peut soit faire scanner ce code QR par le personnel du restaurant (possibilité 2), soit scanner un code QR sur la table (avec le numéro de la table) – processus qui correspond à la première possibilité décrite ci-dessus. Il est également possible d'enregistrer des personnes qui n'ont pas l'application SocialPass via la saisie manuelle (cf. chapitre 2.4.1), par exemple parce qu'elles n'ont pas d'appareil mobile.

(4) Les données sont ensuite cryptées et transférées directement vers une base de données SQL centrale (Microsoft Azure), qui est hébergée par Microsoft en Suisse. Cela permet aux traceurs autorisés d'accéder directement aux données afin de prévenir les personnes potentiellement infectées.

(5) Le fait de quitter un établissement (saisi par un autre scan) est également enregistré et transféré dans la base de données.

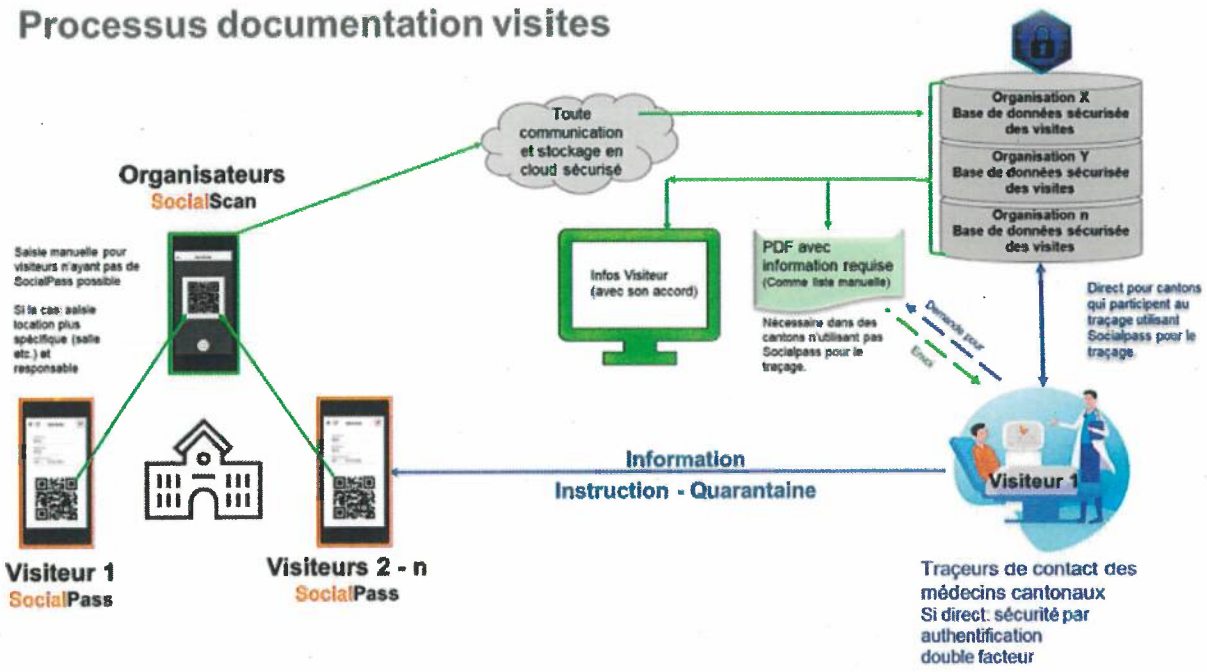

Figure 2: Schéma actualisé du mode de fonctionnement de SocialPass

(6) La figure 2 montre qu'un traceur peut accéder directement aux informations des visiteurs potentiellement infectés sur la base de données en utilisant une authentification à deux facteurs. En outre, les autorités cantonales ont un accès direct aux données enregistrées dans la base de données Azure lorsque l'utilisation de l'application SocialPass est rendue obligatoire par ces autorités (cf. chapitre 2.2.5.b).

(7) La figure 2 montre également que l'accès des médecins cantonaux aux données diffère d'un canton à un autre. Selon le modèle choisi, les exploitants d'établissements accessibles au public peuvent demander une liste d'informations sous forme de fichier Excel/PDF et la transmettre aux traceurs ou si les traceurs peuvent accéder directement aux coordonnées des visiteurs.

2.2.3. *Fonctions de SocialScan*

Le composant SocialScan est utilisé par un établissement accessible au public (par exemple un restaurant) pour enregistrer les coordonnées des visiteurs et peut être installé sur les plateformes iOS et Android.

Lors de l'enregistrement d'un établissement dans SocialScan dans le but de créer un compte, les données suivantes sont collectées (les champs obligatoires étant marqués par un *) :

- «Organisation»*: restaurant, événement, religion, prestations de service, restaurant Berne, sport, général – simple, famille, chantier de construction, centre de formation, EMS ou organisation partenaire
- Nom*
- Adresse*
- Code postal*
- Ville*
- E-Mail*
- Téléphone*
- Nom de la personne responsable*
- Mot de passe*

L'adresse mail et le mot de passe sont utilisés pour créer un compte d'utilisateur.

Les données des établissements sont traitées à deux fins différentes. D'une part, lors d'une visite dans un établissement accessible au public, les coordonnées des visiteurs sont complétées avec les données portant sur l'établissement, l'événement, etc. puis transmises à la base de données centrale aux fins de la collecte des coordonnées des visiteurs/à des fins de traçage (contact tracing). D'autre part, les données sont transférées dans le système de gestion de la relation client (Customer Relationship Management, CRM) de NewCom4U Sàrl. En fonction de l'abonnement conclu entre les établissements et les exploitants de SocialPass, ce système gère les processus de paiement pour l'utilisation de l'application.

2.2.4. *SocialPass : enregistrement et utilisation*

SocialPass est le composant utilisé par les clients d'un établissement. L'application est gratuite et peut être utilisée sur les appareils iOS et Android.

Après avoir téléchargé le composant SocialPass sur son téléphone mobile et accepté la déclaration de confidentialité (un document intitulé « SocialPass – SocialScan et la protection des données » consultable sous https://www.socialpass.ch/mentionslegales/; état au 10.05.2021), l'utilisateur doit

indiquer son numéro de portable qui est ensuite vérifié. La vérification se fait via le prestataire américain « Twilio » (cf. chiffre 2.5.2), toutefois l'utilisateur n'en est pas informé.

L'utilisateur reçoit un code de vérification par SMS sur le numéro indiqué et procède ensuite à « l'enregistrement du client ». A cette fin, il doit indiquer les données suivantes (les champs obligatoires étant marqués par un *) :

- Nom*
- Prénom*
- Numéro de téléphone mobile* (repris du pas précédent)
- Code postal*
- Date de naissance
- Adresse
- E-Mail

Il convient de noter que la date de naissance constituait un champ obligatoire au début de la procédure d'établissement de faits, ce qui a été adapté au cours de la procédure.

À l'exception du numéro de téléphone (voir ci-dessus), les données enregistrées par l'utilisateur ne sont pas vérifiées. Elles peuvent en outre être adaptées à tout moment. Lorsque l'utilisateur veut changer le numéro de téléphone mobile indiqué lors de l'enregistrement, il reçoit un nouveau code de vérification.

Les coordonnées collectées sont sauvegardées localement sur l'appareil mobile de l'utilisateur.

Une fois l'inscription complétée, l'utilisateur dispose d'un code QR qui peut être affiché sur son portable. Il peut ensuite montrer ce code à l'exploitant de l'établissement lorsqu'il accède audit établissement. L'exploitant scanne alors le code QR grâce au composant SocialScan.

Le client peut également scanner lui-même, à l'aide de l'application SocialPass, un code QR fourni par l'exploitant de l'établissement accessible au public et l'utiliser pour s'enregistrer. Il convient de noter que dans cette deuxième hypothèse, il n'est pas possible de vérifier si le code QR mis à disposition par l'exploitant de l'établissement ne renvoie pas à un contenu dangereux, puisque l'application ne demande pas de reconfirmation avant de transmettre les données après le scan du code QR.

Quand le code QR de l'utilisateur est lu par un appareil de l'exploitant ou que l'utilisateur scanne le code QR mis à disposition par l'établissement, les coordonnées des visiteurs enregistrées, complétées par les données relatives à la visite dans l'établissement (« détails de présence dans une organisation ») sont alors transférées dans une base de données SQL (Microsoft Azure, cf. chapitre 2.5.3).

2.2.5. *Base de données centralisée*

a. *Généralités*

Lors d'une visite, les coordonnées du visiteur (nom, adresse, email, numéro de téléphone, etc.) sont combinées avec les données de l'établissement accessible au public (nom, emplacement, table, etc.) et le moment de la visite (checkin / checkout) pour former un ensemble de données. Cet ensemble de données (coordonnées du visiteur / données de l'établissement / heures de présence) est ensuite transmis de manière cryptée et stocké dans la base de données centrale d'Azure (Suisse Nord / Zurich). Les interfaces de programmation API (Application Programming Interfaces) sont utilisées pour la transmission des données.

D'une manière générale, les accès aux API sont protégés par l'utilisation de jetons de sécurité du type JWT encrypté à l'aide d'algorithmes AES 256. Les API sont aussi déployés dans le cloud Azure Suisse.

Le tableau suivant récapitule, à titre d'exemple, l'ensemble des données qui sont transférées à la base de données centrale en tant que « détails de présence dans une organisation » aux fins de la collecte des coordonnées des visiteurs en vertu des dispositions légales en vigueur :

PresenceDataID	4016282
OrganizationID	17800
LastName	Doe
FirstName	John
PhoneNr	+41791234567
ReservationDate	2021-01-28
Field1_Value	Table 2
City	Berne
PostalCode	3003
Canton	Berne
Arrival	2021-01-28 10:32:00.000
Departure	2021-01-28 11:45:00.000
DateOfBirth	1999-01-01
Adress	Feldeggweg 1

Les détails des présences dans une organisation peuvent être transmises soit par SocialPass ou par SocialScan, selon la variante utilisée (cf. chapitre 2.4).

Malgré les demandes explicites du PFPDT, il n'a pas été possible d'établir quelles étaient les mesures de protection des données dans Azure et si les données sont stockées sous forme cryptée ou non (data at rest protection).

Les détails de présence dans une organisation sont supprimés après 14 jours. À cette fin, une tâche planifiée a été exécutée à l'aide de la fonction « WebJobs » ; le script fonctionne en continu et supprime automatiquement, deux fois par jour, les enregistrements de données de plus de 14 jours.

Le stockage des détails de présence dans une organisation transmises est centralisé, c'est-à-dire que le stockage desdits détails de présence n'est ni physiquement ni logiquement séparé, il n'y a pas de ségrégation (séparation) des données par canton ou par établissement accessible au public. En d'autres termes, il n'y a qu'une seule base de données centrale pour toutes les données relatives aux visiteurs de tous les établissements participants au système SocialPass dans toute la Suisse.

b. Accès des autorités cantonales aux coordonnées des clients

Il y a deux possibilités d'accès aux données centralisées lors d'un cas d'infection : la remise d'une liste à l'autorité compétente par l'établissement ou un accès direct par les autorités en charge de la santé publique (cantons de Valais et Vaud).

Dans la variante « remise d'une liste » l'établissement peut, si les autorités compétentes le lui demandent pour l'identification des personnes présentes, télécharger une liste des coordonnées des visiteurs pour une période donnée et la mettre à la disposition de l'autorité cantonale.

Dans la variante « accès direct par les autorités sanitaires » les autorités cantonales compétentes, comme p.ex. les médecins cantonaux, peuvent obtenir un accès direct à la base de données Azure. Chaque canton peut, s'il le souhaite, demander un accès direct sur la base de données centralisée. Les médecins cantonaux sont alors dans le rôle du « power user » qui leur permet de créer des logins pour leurs collaborateurs. Actuellement (état au 10.05.2021), seuls les autorités sanitaires des Cantons de Vaud et Valais ont la possibilité d'accéder directement aux bases de données centralisées. Par le biais de cet accès direct à la base de données, les autorités cantonales peuvent effectuer de multiples traitements de données.

Le schéma suivant illustre les fonctions que les autorités sanitaires peuvent utiliser :

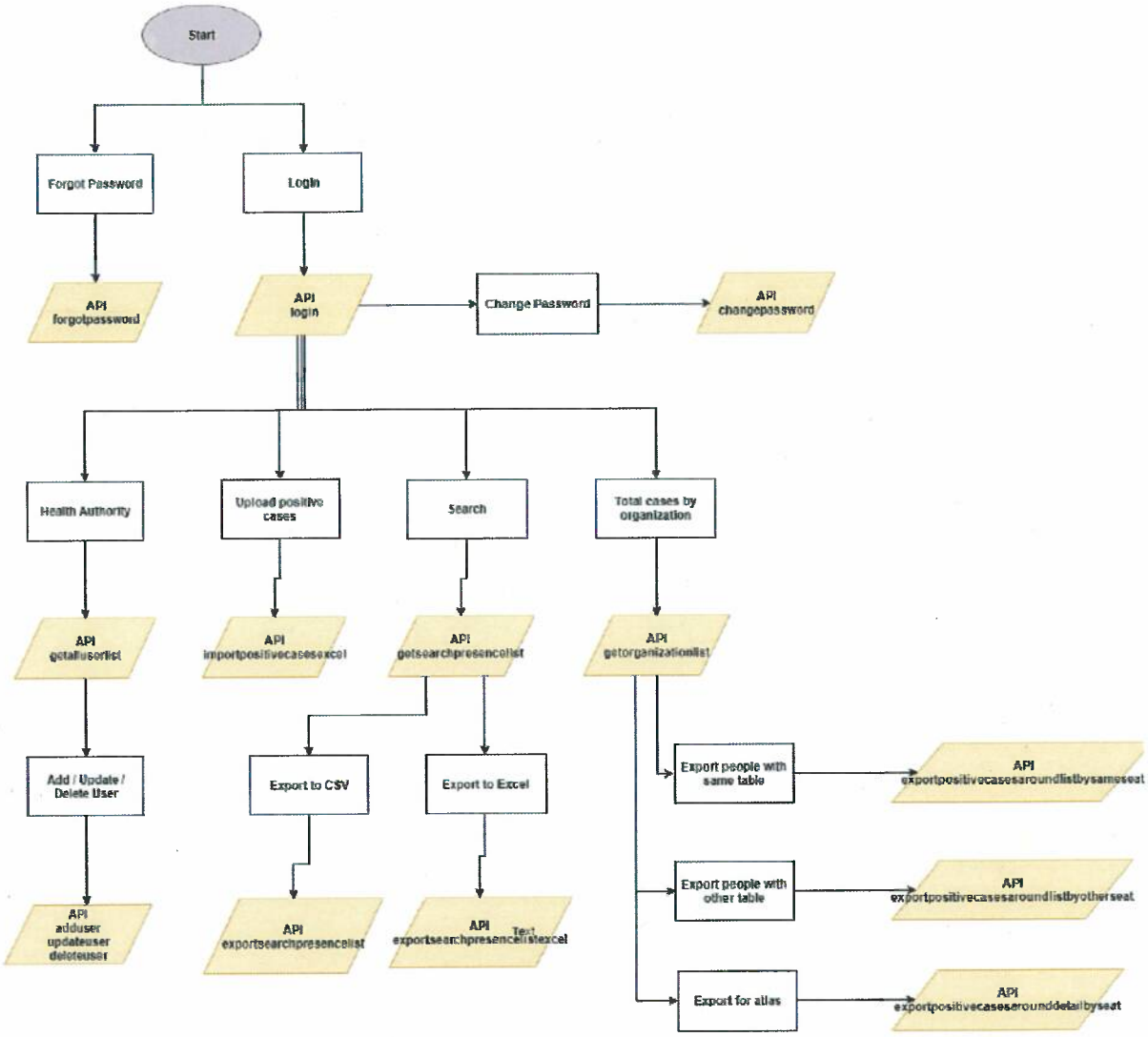

Figure 3: Backoffice Health Authority – Diagramme logique du flux de données, dans : Rapport technique (Document [D]), p. 17

Le système SocialPass met à disposition plusieurs fonctions pour traiter les données des visiteurs. Ainsi, les autorités sanitaires disposent des fonctions suivantes en fonction de leurs permissions :

- Gestion des collaborateurs (cf. Health Autority dans le schéma ci-dessus)
- Chargement du fichier des cas positifs (cf. Upload positive cases dans le schéma ci-dessus)
- Recherche (cf. Search dans le schéma ci-dessus)
- Total des cas par organisation (cf. Total cases by organization dans le schéma ci-dessus)

La première fonction est accessible aux personnes disposant d'un droit d'administrer les collaborateurs. Trois types de droits sont disponibles :

- Primary (permet d'administrer)
- Power (permet d'importer/exporter)
- Normal (permet de visualiser)

Le type Primary est défini par l'équipe de support de SocialPass. En général c'est le compte du Médecin Cantonal. Un canton spécifique est indiqué pour le Primary. Le type Power et Normal est défini par l'utilisateur de type Primary. Le canton ne peut être changé, ainsi, par exemple, si un

Primary est rattaché au canton de Vaud, le Power et le Normal le seront également. L'ancrage à un canton limite par la suite la capacité de la recherche à ce seul canton. Il en découle, par exemple, que les collaborateurs du canton de Vaud n'auront pas accès aux données des personnes résidantes dans le canton du Valais.

Selon les informations soumises par les représentants de SocialPass, aucune autre partie que les certains exploitants déterminés en amont et les autorités sanitaires n'ont accès à la base de données centralisée.

Les représentants légaux n'ont fourni aucune information à propos de l'enregistrement des accès, bien que le PFPDT leur ait adressé plusieurs questions à ce sujet. Ainsi, sur la base de la documentation disponible, le PFPDT n'a pas pu procéder à une conclusion claire en la matière.

La deuxième fonction (Upload positive cases) permet de charger la liste des cas ayant été testé positifs au Covid-19.

La troisième fonction (Search) permet de rechercher des présences dans des organisations (établissements accessibles au public) en utilisant plusieurs filtres. Lors de requêtes différents champs de données peuvent être utilisés (voir la capture d'écran ci-dessous). Ce mode de recherche permet de spécifiquement rechercher des personnes individuelles (nom, prénom), des numéros de téléphone ou des codes postaux. La recherche peut être limitée dans le temps et/ou à des établissements spécifiques (filtre). Les requêtes permettent d'effectuer des recherches avec des caractères génériques, ce qui permet d'obtenir un grand nombre de résultats.

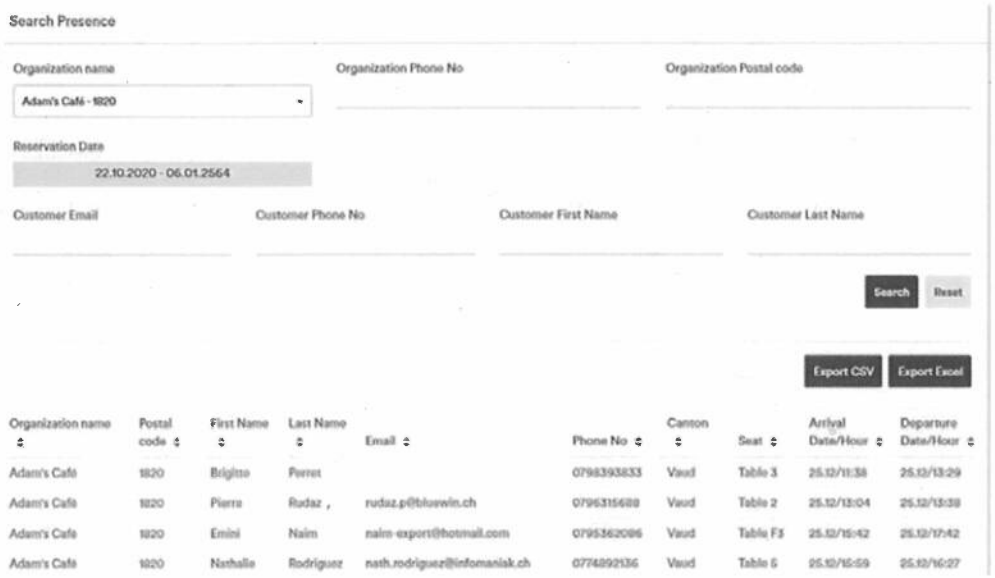

Figure 4: Options de recherches pour les autorités sanitaires, dans : Rapport technique (Document [D]), p. 75

La quatrième fonction (Total cases by organization) permet de retrouver les organisations (établissements accessibles au public) dans lequel des cas positifs ont effectué une visite. Les options de recherche suivantes sont alors disponibles :

• Voir les cas positifs

• Exporter la liste des cas positifs, y compris les personnes en contact direct avec la personne infectée

• Exporter la liste des personnes ayant fréquenté le même établissement que les cas positifs

• Exporter uniquement les numéros de téléphone des personnes en contact direct avec les cas positifs (option « Atlas » spécifique au canton du Valais).

À partir de la recherche des cas positifs dans les organisations on peut obtenir l'identification de ces cas. À partir de la recherche précédente on peut obtenir la liste des personnes ayant été en contact direct avec les cas positifs. Pour cette option de recherche, la restriction sur le canton ne s'applique pas. Tous les contacts du cas positif sont identifiés.

2.3. But de la collecte des données

Selon le ch. 7 de la déclaration de confidentialité[2], qui trouve son fondement dans l'Ordonnance Covid-19 situation particulière, la collecte des données se fait uniquement dans le but de les transmettre aux autorités publiques en cas d'infection confirmée de COVID-19 au sein de l'établissement accessible au public.

[2] Document « SocialPass – SocialScan et la protection des données », https://www.socialpass.ch/mentionslegales/, état au 10.05.2021 ; identique au document « Privacy Policy – SocialPass et SocialScan », annexe n° 1 au courrier du 26.04.2021

2.4. Description des différents modes de fonctionnement

2.4.1. SocialScan : saisie manuelle (enregistrement des clients réguliers)

Lorsque l'exploitant de l'établissement accessible au public enregistre les coordonnées du client manuellement (saisie manuelle), le client devrait, en principe, pouvoir choisir d'ajouter ses données à la liste des « clients réguliers », d'imprimer un code QR ou de continuer sans rien faire. En pratique toutefois, le choix entre ces différences options appartient à l'utilisateur de SocialScan. En effet, c'est l'utilisateur de SocialScan, c'est-à-dire l'exploitant de l'établissement accessible au public qui dispose de l'appareil sur lequel SocialScan a été téléchargé.

Si le choix porte sur l'inscription sur de la liste des clients réguliers, les données sont stockées localement sur l'appareil de l'utilisateur de SocialScan, c'est-à-dire de l'exploitant de l'établissement accessible au public. Les coordonnées peuvent ensuite être réutilisées lors d'une nouvelle visite via la fonction « saisie manuelle ». Lorsque la fonction « saisie manuelle » est choisie, la liste sur laquelle figure toutes les coordonnées des « clients réguliers » enregistrés s'affiche lorsqu'est sélectionnée la fonction « choisir un client ». L'utilisateur de SocialScan peut accéder à cette liste à tout moment. Toutes les coordonnées s'affichent alors en texte clair. Sur la base des informations soumises au PFPDT, aucune fonction permettant de supprimer à nouveau les données enregistrées ne semble exister. En outre, aucune information sur la durée de conservation des données des « clients réguliers » ne figure dans la documentation soumise dans le cadre de cette procédure.

La liste des « clients réguliers » peut également être exportée à des fins de « synchronisation » avec d'autres appareils de l'exploitant de l'établissement accessible au public (p.ex. lorsque l'équipe de service est composée de plusieurs collaborateurs). L'ensemble des données des « clients réguliers » peut être affichée sous forme d'un code QR. Ce code QR peut ensuite être lu directement à partir d'un autre appareil (importation) ou imprimé (puis lu par les appareils des différents collaborateurs).

Enfin, il convient de noter que lorsque les coordonnées d'un « client régulier » sont enregistrées, le numéro de téléphone de ce client n'est pas vérifié – contrairement à ce qui est prévu lors du téléchargement de l'application SocialPass.

Les deux captures d'écran suivantes montrent le point de menu pour la saisie manuelle des données des « clients réguliers » dans Socialscan et les données à saisir et à transmettre :

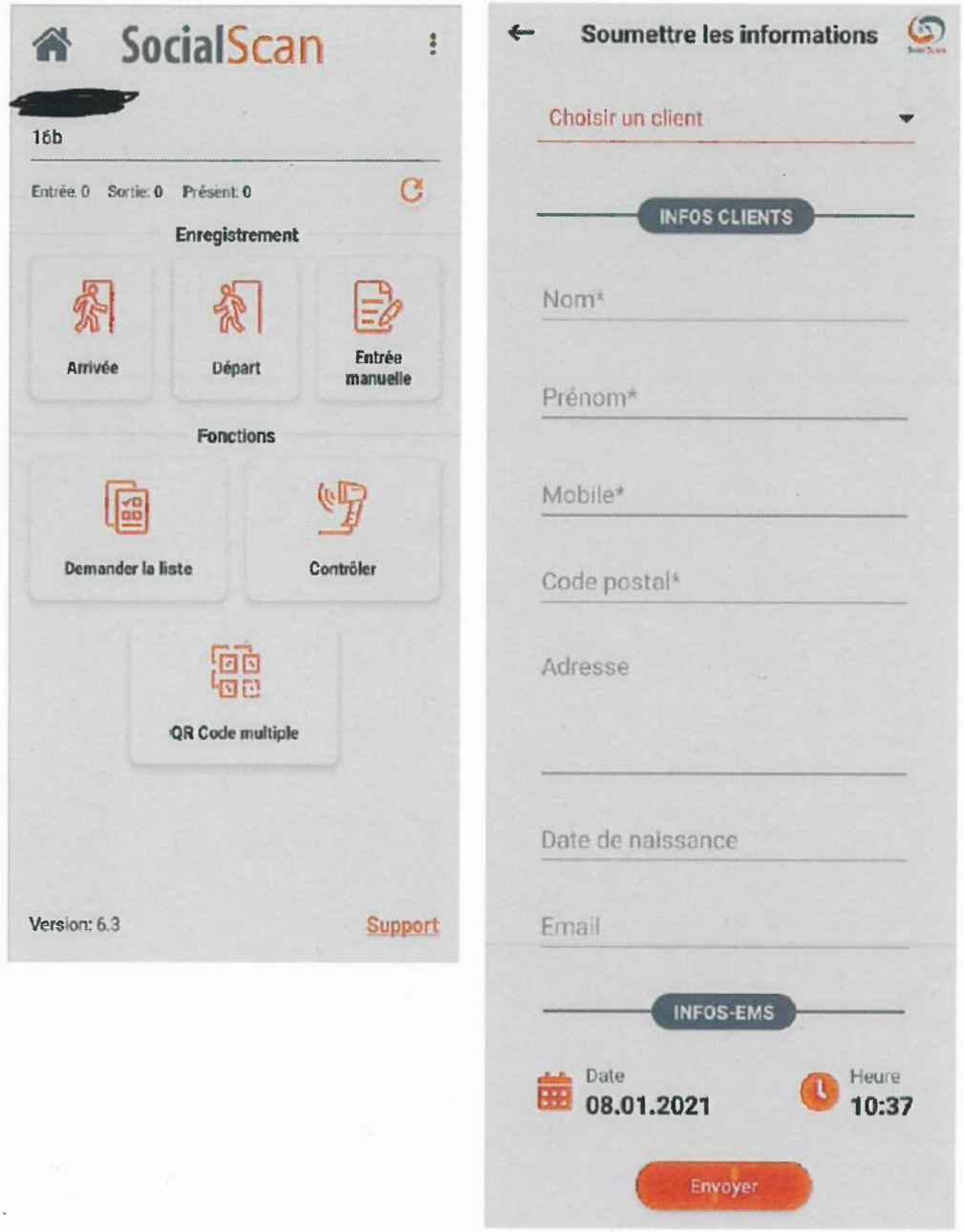

Figure 5 : écrans de SocialScan, dans : Rapport technique (Document [D]), p. 61ss.

À noter : la fonction était appelée « entrée manuelle » dans la version 6.3 et a été renommée « saisie manuelle » dans la version actuelle.

2.4.2. *Stockage des numéros de téléphone mobile issus du processus d'enregistrement*

Au cours du processus d'enregistrement, le numéro de téléphone mobile est traité dans le but de vérifier l'authenticité du numéro indiqué. Avant de déclencher la vérification par SMS grâce aux services Twilio, il est vérifié si le numéro de téléphone indiqué a déjà été utilisé une fois pour l'inscription dans SocialPass. À cette fin, tous les numéros de téléphone mobile utilisés précédemment sont stockés de manière centralisée sur Microsoft Azure. Lorsqu'un nouvel enregistrement est effectué, ces données sont interrogées.

Il n'y a aucune indication que les numéros de téléphone sont supprimés après une certaine période de temps. En outre, l'utilisateur n'est pas informé de ce stockage permanent lors de la procédure d'enregistrement. Il n'y a pas non plus d'indication sur la manière dont l'utilisateur peut faire supprimer ces données.

Il est important de noter que le traitement du numéro de téléphone répond à deux objectifs différents. D'une part, le numéro de téléphone est traité afin de procéder à sa vérification de ce numéro par l'envoi d'un SMS et, d'autre part, pour répondre aux exigences légales qui fixent que la collecte du numéro de téléphone est obligatoire afin de permettre le traçage (contact tracing). Ce sous-chapitre se penche sur le traitement des données tel que prévu par le premier objectif décrit ci-dessus.

2.5. Services de tiers

2.5.1. *Infomaniak*

Le site www.socialpass.ch sert principalement de portail d'information pour la plateforme SocialPass et est hébergé par Infomaniak en Suisse. Infomaniak est un hébergeur suisse dont les centres de données sont situés exclusivement en Suisse. À l'origine, le site www.socialpass.ch était hébergé par un fournisseur en France. Après le premier audit de la société Navixia SA en novembre 2020, l'hébergement a été confié à Infomaniak en Suisse.

Le fonctionnement du site web et le traitement des données associé ne sont pas examinés dans le cadre de cette enquête. Sur la base des informations à notre disposition, il n'y a pas d'échange de données entre le site web et les applications SocialPass ou SocialScan ; au moment de la présente enquête, le site web est uniquement utilisé à des fins d'information.

2.5.2. *Twilio*

Twilio est une entreprise américaine basée à San Francisco, aux États-Unis. Elle exploite une plateforme de communication en nuage en tant que « Platform as a Service ».

Après l'enregistrement initial auprès de SocialPass, Twilio permet l'envoi du SMS aux utilisateurs de SocialPass. En recevant le SMS, la validité du numéro du client est confirmée. À la fin du processus de vérification, une clef unique est renvoyée par ce service si le processus a pu être achevé correctement. Force est de constater que lors de l'utilisation du service Twilio des données personnelles au sens de la LPD, notamment les numéros de téléphone des visiteurs, son transférées aux US. Toutefois, sur la base de la documentation à notre disposition, nous constatons que les opérateurs de SocialPass n'ont pas vérifié si des mesures autres que celles prévues dans les clauses contractuelles étaient nécessaires et, le cas échéant, si elles avaient été mises en place.

La finalité de la collecte et du traitement des numéros de téléphone ne ressort pas clairement des documents soumis au PFPDT ; toutefois, sur la base des informations dont nous disposons, ces données ne semblent pas être traitées en tant que coordonnées, mais sont traitées afin de vérifier l'authenticité du numéro de téléphone indiqué.

2.5.3. Microsoft Azure (base de données SQL)

Une base de données Azure SQL de Microsoft, hébergée en Suisse, est utilisée pour stocker les données tel que décrit ci-dessus. Les rapports de test [B] et [C] qui nous ont été fournis ne concernent que le composant SocialScan pour Android et iOS. Ils ne contiennent aucune information sur le composant SocialPass ou les services de fournisseurs tiers, tels que Twilio ou Microsoft Azure. Afin de permettre au PFPDT de mieux évaluer le traitement en termes de sécurité et de protection des données, des réponses spécifiques supplémentaires ont été demandées à SwissHelios dans le document [K]. Dans ce contexte, la question a été posée de savoir si Azure était configuré conformément à la Baseline, par exemple. Cette question est restée sans réponse jusqu'à ce jour. Le document [I] a été soumis à titre d'information. Toutefois, il ne contient aucune information sur les mesures prises pour sécuriser le système ni sur la mise en œuvre effective et le contrôle de ces mesures. Dans la réponse (4-c) du document [H], les exploitants de SocialPass expliquent que la fonction d'audit est activée sur Azure, qui enregistre les accès à la base de données. Elle précise ensuite que l'infrastructure AZURE dispose de toutes les fonctions de sécurité, de journalisation et de traçage. Il n'est pas expliqué si et comment ceux-ci sont utilisés et donc activés. Dans ce cadre se pose également la question de savoir si des identificateurs et/ou d'autres données personnelles ont été enregistrés dans Azure en plus des données des visiteurs/clients (=présence) et si oui, lesquelles.

2.6. Information et droits des personnes concernées

2.6.1. Information des utilisateurs

Au cours de la procédure d'établissement des faits, la déclaration de protection des données et d'autres informations publiquement accessibles, à savoir les informations disponibles sur le site web www.socialpass.ch, ont été considérablement modifiées. Actuellement (état au 10.05.2021), tant les

liens dans l'AppStore (Apple/iOS), dans le PlayStore (Google/Android) que dans les applications SocialPass et SocialScan renvoient à la déclaration de protection des données sur le site www.socialpass.ch/mentionslegales/, ce qui était encore incohérent au moment de l'ouverture de la procédure.

2.6.2. Droits des personnes concernées

a. Exercice du droit d'accès

Le document « SocialPass – SocialScan et la protection des données »[3], accessibles via l'application, les AppStores et le site web sous le titre « Protection des données », indique une adresse de contact pour les utilisateurs (info@socialpass.ch; état au 10.05.2021).

En outre, la déclaration de protection des données contient des informations sur les droits des personnes concernées (cf. ch. 6).

b. Exercice du droit à l'effacement des données

L'effacement se fera de façon automatisée après la durée de conservation de 14 jours prévue par l'Ordonnance Covid-19 situation particulière.

Par contre, lorsque la fonction « Saisie manuelle » (cf. chapitre 2.4.1) est utilisée, les coordonnées des « clients réguliers » restent enregistrées sur l'appareil de l'établissement. Sur la base de la documentation soumise au PFPDT, aucune possibilité d'effacer les données des « clients réguliers » des appareils des établissements accessibles au public ne semble avoir été prévue par les exploitants de SocialPass.

Aucune information n'est disponible sur la question de savoir si une sollicitation à l'adresse des utilisateurs de supprimer l'application, et donc toutes les données personnelles détenues sur les appareils, est prévue lorsque les dispositions pertinentes fondées sur l'Ordonnance COVID-19 Situation particulière ne seront plus en vigueur.

2.7. Aspects de sécurité des données

2.7.1. Organisation de la sécurité de l'information

Le PFPDT a demandé aux opérateurs de l'application, au moyen d'un questionnaire, comment les responsabilités en matière de sécurité de l'information et de protection des données sont définies, documentées et attribuées entre les deux exploitants de l'application. Dans leur réponse à ce

[3] https://www.socialpass.ch/mentionslegales/

questionnaire technique, les exploitants de l'application ont indiqué que la répartition des responsabilités en matière de sécurité de l'information et de protection des données n'a pas pu être fixée (ni par oral ni par écrit), notamment en raison des modifications constantes de l'application au niveau cantonal ainsi qu'en raison des développements rapides, mais que peu prévisibles de la pandémie.

2.7.2. Login avec double-authentification

Sur la base des informations soumises au PFPDT, il n'est pas clair si et, le cas échéant, quels composants du système de SocialPass sont sécurisés au moyen d'une authentification à deux facteurs.

2.7.3. Identifiants de l'utilisateur

Selon le chapitre [D] "8.11 - Device - Structure des données", différents identifiants d'utilisateur sont utilisés. Outre le numéro de téléphone, il convient de mentionner explicitement l'utilisation de l'IMEI (International Mobile Equipment Entity, un numéro de série à quinze chiffres unique au monde de l'appareil) et d'un numéro d'utilisateur unique UID (Unique ID) de Google Firebase. Aucune autre donnée pseudonymisée servant à identifier de manière unique les personnes concernées n'a été mentionnée, même après des demandes explicites du PFPDT.

2.7.4. Géolocalisation

SocialPass n'utilise pas la géolocalisation.

2.8. Analyse de l'audit de Navixia SA

Les composants « SocialPass » et « SocialScan » ont fait l'objet d'un test de vulnérabilité par Navixia SA, pour le compte de GastroVaud, aux dates suivantes. Cela vaut pour les systèmes d'exploitation iOS et Android.

Date	Processus
18 mars 2021	Rapport, y compris Management Summary v.1.2
12 au 18 mars 2021	Test du cryptage mis en oeuvre
7 décembre 2020	Rapport, y compris Management Summary v.1.1
4 décembre 2020	Vérifications 2 et 3
16 au 18 novembre 2020	Kick-Off et test

Selon le rapport « Analyse de sécurité (recheck) Applications SocialPass & SocialScan v.1.2 » daté du 18 mars 2021, tous les éléments des applications susceptibles d'être pertinents pour la sécurité ont été

examinés. Cela comprend le stockage des données, la confidentialité, la cryptographie, l'authentification, la communication réseau et les paramètres de construction.

Pour analyser les applications mobiles, Navixia SA suit une méthodologie basée sur l'évaluation des risques OWASP. Cette approche suit un processus structuré et rend les résultats obtenus comparables entre eux. À cette fin, pour chaque élément identifié, la vulnérabilité est décrite et son degré de risque est cartographié sur la base du système normalisé CVSS (Common Vulnerability Scoring System). Les résultats sont évalués selon les critères suivants :

- **Exploitabilité** : les vecteurs d'accès, la complexité de l'accès et l'authentification évaluent comment un attaquant peut accéder à une vulnérabilité et quelles conditions supplémentaires, le cas échéant, doivent être remplies pour qu'elle soit exploitée.
- **Implications** : Les indices de protection des données, d'intégrité du système et de disponibilité mesurent la manière dont une vulnérabilité peut avoir un impact direct sur l'infrastructure informatique une fois exploitée.

Dans le CVSS, le score total d'une vulnérabilité résulte de la combinaison d'une série d'évaluations isolées d'aspects individuels (métriques), en tenant compte des pondérations enregistrées dans la formule de calcul.

Les indices de mesure à cet effet sont indiqués ci-dessous avec les valeurs attribuées correspondantes.

Cet indice évalue le niveau d'autorisation qu'un attaquant doit avoir afin d'exploiter avec succès la vulnérabilité.

	Disponibilité
Haut:	L'attaquant dispose de privilèges qui lui donnent accès à des rôles administratifs importants.
Moyen:	L'attaquant dispose de privilèges d'utilisateur de base qui peuvent affecter les paramètres et les fichiers d'un utilisateur.
Faible:	L'attaquant n'a pas besoin d'être authentifié.

Ici, l'évaluation est basée sur l'impact d'une vulnérabilité sur la confidentialité des données traitées.

	Confidentialité
Haut:	Il y a une perte totale de confidentialité et un attaquant obtient l'accès à toutes les ressources du composant affecté.
Moyen:	Un attaquant peut accéder à certaines données.
Faible:	Il existe un faible risque d'accès aux données au sein du composant concerné.

Cet indice décrit l'impact d'une vulnérabilité sur l'intégrité du système.

	Intégrité
Haut:	Il en résulte une perte totale d'intégrité. Par exemple, l'attaquant peut modifier n'importe quel fichier (ou ensemble de fichiers).
Moyen:	La modification de données est possible dans une mesure limitée. Cependant, la modification des données n'a pas d'impact significatif sur le composant concerné.
Faible:	Il y a un faible risque de perte d'intégrité.

Le degré de danger est évalué dans le rapport de Navixia SA sur la base des éléments ci-dessus sur une échelle de 0 à 10.

- Score entre 9,0 et 10: critique
- Score entre 7,0 et 8,9: haut
- Score entre 4,0 et 6,9: moyen
- Score entre 0,1 et 3,9: faible
- Score 0: à titre d'information

Du point de vue du PFPDT, les interprétations suivantes doivent servir de référence, en fonction de l'indice d'évaluation, afin de prévenir les risques de violation de la protection des données.

Critique:	Cette vulnérabilité représente un risque inacceptable. L'application ne doit pas être mise en ligne ; si elle l'est déjà, elle doit être désactivée immédiatement.
Haut:	Cette vulnérabilité doit être corrigée immédiatement, éventuellement dans le cadre d'un correctif d'urgence. D'autres mesures de minimisation des risques doivent être envisagées jusqu'à ce que le correctif soit en place.
Moyen:	Cette vulnérabilité doit être corrigée, même si elle entraîne des coûts supplémentaires (modérés) ou d'autres inconvénients (modérés).
Faible:	Le correctif peut être inclus dans la planification des versions sur une base régulière.

Par la suite, les conclusions du document « GVD7009_Recheck_SocialPass_SocialScan_v1.2 » sont décrites.

2.8.1. Interaction avec la plateforme (6.2.6 et 6.3.6[4])

Actuellement, le serveur ne vérifie pas les métacaractères. Le cross-site scripting (XSS) n'est souvent que le précurseur d'attaques plus graves. Actuellement, aucune vérification des données n'a lieu avant leur exécution par le serveur.

[4] Les chiffres se réfèrent aux chapitres du document [A] « GVD7009_Recheck_SocialPass_SocialScan_v1.2 »

2.8.2. *Qualité du code et packaging (6.3.7)*

Comme décrit dans le rapport d'audit, un attaquant peut modifier l'APK (paquet Android) afin qu'il contienne une ancienne version d'une bibliothèque externe sans que cela soit détecté par la signature. Toutefois, si cette ancienne bibliothèque contient des vulnérabilités, l'APK peut être installé sur un téléphone mobile, par exemple, sans briser la signature existante. Il est ainsi possible d'exploiter les failles de sécurité des anciennes bibliothèques.

En outre, les versions intégrées des bibliothèques tierces ont été examinées au cours de l'audit. Il a été constaté que toutes les bibliothèques ne sont pas de la dernière version. En fait, les bibliothèques tierces obsolètes sont souvent affectées par des failles de sécurité.

2.8.3. *Descripteur (7.1)*

Le descripteur d'API utilisé par les applications mobiles est accessible au public. Cela permet à un attaquant de détecter toutes les méthodes disponibles. D'après le rapport, le descripteur d'API n'est plus visible dans l'environnement de test UAT (User Acceptance Test), mais peut toujours être consulté en production. Un attaquant peut en tirer des informations pour attaquer l'environnement UAT. Le problème ne peut donc être résolu que si l'information n'est pas du tout visible.

2.8.4. *Mots de passe stockés en clair (7.1)*

Dans le cadre d'interviews, les développeurs de SocialPass ont confirmé à Navixia SA que les mots de passe ne sont plus stockés en texte clair dans la base de données. Cependant, sans accès à cette base de données, il n'a pas été possible pour Navixia de vérifier si les mots de passe sont maintenant stockés correctement (salt & hash). Dès lors, le PFPDT part du principe que les déclarations faites par les développeurs dans le rapport sont correctes et que les mots de passe ne sont plus seulement stockés en texte clair, mais qu'ils sont également sécurisés par un Medium Salting.

2.8.5. *Conservation des données (8.4.1)*

La section 8.4.1 mentionne un problème de conservation des données dû à une faille de sécurité. Selon le rapport d'audit, cela a été rectifié depuis. Or, ce point ne pouvait plus être vérifié par Navixia SA sans accès à la base de données.

2.9. Analyse de l'audit d'Indusface

Le PFPDT a reçu les deux documents suivants par e-mail le 11 février 2021 par le représentant légal des exploitants de SocialPass :

Rapports d'audit
Android Mobile Application Audit Report of Social Scan v1.0.pdf SHA256 D313DCD4B4D8FBD2C142F7943C65DB4FF4155F6B474C2F5435306ADF438F26CC
iOS Mobile Application Audit Report of Social Scan v1.0.pdf SHA256 C74551665D7B221AC133DBBEDC31F6EAB277FB151879D14237D680117B6A3BD9

Les deux rapports d'audit fournis (Indusface), se réfèrent exclusivement au composant « SocialScan », dans les versions pour Android et iOS. Ils ne contiennent aucune information sur le composant « SocialPass » ou sur des services tiers tels que « Twilio » ou les systèmes back-end sur « Azure ».

Périodes d'essai	OS	Version SocialScan
22. oct. - 04. nov. 2020	Android	V6.0.1 MD5: b82a838aa9f430857581f02693ff26c0
28. oct. - 03. nov. 2020	iOS	V6.2 MD5: 0B81B1417BCD6A7CF8360B133632B241

Les conclusions des rapports « Android Mobile Application Audit Report of Social Scan v1.0 » et « iOS Mobile Application Audit Report of Social Scan v1.0 » diffèrent en fonction des systèmes d'exploitation Android et iOS.

2.9.1. Classification

La classification est basée sur les catégories ci-dessous.

Impact	Description
Critical	A vulnerability wherein an attacker might have the ability to execute commands on the server or retrieve and modify private information.
High	Security issues are defined as a risk that puts the system and / or data related to the system in immediate danger.
Medium	Findings indicate a more serious security matter that should be remedied appropriately within a short amount of time.
Low	Findings usually indicate a minor security risk that does not pose immediate or short-term danger. An observational point in the site, or detection of certain applications or web servers.
Information	An observational point in the site, or detection of certain applications or web servers.

2.9.2. *Résultats en fonction des catégories*

Les vulnérabilités détectées sont classées dans les catégories suivantes.

Android-App	iOS-App
▪ Critical: 0 ▪ High: 2 ▪ Medium: 2 ▪ Low: 21 ▪ Information: 3	▪ Critical: 0 ▪ High: 2 ▪ Medium: 1 ▪ Low: 18 ▪ Information: 1

2.9.3. *Android et iOS Mobile*

Le tableau ci-dessous reflète les résultats d'Indusface [B] et [C] pour le composant « SocialScan » pour les systèmes d'exploitation Android et iOS. Les entrées marquées d'un astérisque (*) sont considérées par le PFPDT comme pertinentes pour la protection des données. Même s'ils sont considérés comme faibles dans la classification des risques, ils peuvent développer une classification des risques différente à la suite d'interactions. Ces entrées relatives à la protection des données sont analysées au chapitre 2.9.4.

Le PFPDT utilise les notations suivantes comme critère pour atténuer le risque de violation de la protection des données.

Critical:	Cette vulnérabilité représente un risque inacceptable. L'application ne doit pas être mise en ligne ; si elle l'est déjà, elle doit être désactivée immédiatement.
High:	Cette vulnérabilité doit être corrigée immédiatement, éventuellement dans le cadre d'un correctif d'urgence. D'autres mesures de minimisation des risques doivent être envisagées jusqu'à ce que le correctif soit en place.
Medium:	Cette vulnérabilité doit être corrigée, même si cela entraîne des coûts supplémentaires (modérés) ou d'autres inconvénients (modérés).
Low:	La correction peut être incluse dans la planification des versions ultérieures sur une base régulière.

Tableau 3: Résultats trouvés dans SocialScan

Nr.	Vulnérabilités	Catégorie de risques
1*	Blind HTML Injection	High
2*	Insecure Direct Object References	High
3	Application Is Vulnerable To Email Flooding Attack	Medium

4*	Insecure Logging Of The Application (betrifft nur Android)	Medium
5*	Application Is Vulnerable To Improper Token Management	Low
6*	Application Accepts Special Character As User Input	Low
7*	Valid Account Can Be Brute Forced	Low
8*	Missing API Rate Limiting	Low
9*	Application Does Not Have A Strong Password Policy	Low
10	Application Is Vulnerable To Reverse Engineering	Low
11*	Cleartexttraffic Is Set To True (betrifft nur Android)	Low
12*	Application Is Vulnerable To Simultaneous Login	Low
13*	Application's Request/Response Reveals Sensitive Information	Low
14*	SSL Pinning Can Be Bypassed	Low
15*	Insecure Data Storage In File System	Low
16*	Insecure Content Security Policy (Csp)/X-Frame-Options	Low
17*	Missing HSTS Header	Low
18*	Information Leakage From Clipboard	Low
19*	Sensitive Data Disclosure In Recent Apps	Low
20	Default Web Page Found	Low
21*	Application Has Set Insecure Permissions	Low
22	Programming Language And Version Disclosure	Low
23	Application Displays Web Server Banner	Low
24	Using Known Vulnerable Components	Low
25	Application Works In Rooted Device	Low
26	Application Runs On Older Platform	Information
27	Printstacktrace() Function Is Used In The Application	Information

28	setAllowFileAccess Enabled	Information

2.9.4. *Conclusions de l'audit Indusface*

Le sous-chapitre 2.9.4 résume les différentes constatations du PFPDT comportant un risque de perte de données, de corruption de données ou de dommages aux données.

a. *Blind HTML Injection [1]*[5]

L'injection HTML est utilisée lorsque l'entrée dans une application n'est pas validée. Cela permet de modifier le contenu d'une page web et tous les utilisateurs qui naviguent sur cette page verront le contenu modifié. Ainsi, sur la page d'enregistrement de SocialScan, un attaquant peut injecter un HTML Payload (par exemple, une chaîne de code malveillant) dans les champs de données et réussir à l'enregistrer. L'injection HTML est exécutée avec succès dans les modèles d'email.

b. *Insecure Direct Object References [2]*

Les références directes à des objets non sécurisées (IDOR) constituent un problème de sécurité qui se produit lorsque le développeur de l'application utilise un pointeur pour accéder directement à un objet d'implémentation interne, mais ne fournit pas de contrôles d'accès et/ou de vérifications d'autorisation supplémentaires. Un utilisateur de SocialScan est lié à son numéro d'identification d'utilisateur par l'ID de l'organisation. L'attaquant, à son tour, se connecte à SocialScan et peut simplement modifier l'ID de l'organisation à volonté. Cela permet à l'attaquant d'avoir accès aux détails de l'utilisateur correspondant (numéro de téléphone mobile et mot de passe).

c. *Insecure Logging Of The Application [4]*

Dans SocialScan, les données sensibles d'un point de vue technique sont enregistrées et peuvent conduire à des fuites d'informations. Dans SocialScan, les données sensibles telles que le nom de l'utilisateur et le mot de passe sont stockées sans aucune « obfuscation ».

d. *Application Is Vulnerable To Improper Token Management [5]*

Le rapport indique que dans SocialScan, une session reste active même après la déconnexion. Cela signifie qu'une session peut être reprise et réutilisée par un autre utilisateur.

---

[5] Les chiffres entre crochets font référence au tableau 3: Résultats trouvés dans SocialScan, ci-dessus.

e. Application Accepts Special Character As User Input [6]

SocialScan accepte les caractères spéciaux (>{</ etc.). Cela peut conduire à l'exécution d'un code malveillant.

f. Valid Account Can Be Brute Forced [7]

Une attaque par force brute (Brute-Force-Attack) est une méthode d'attaque banale. La théorie est que lors d'une telle attaque, un nombre infini de tentatives sont faites pour deviner un mot de passe. À un moment donné, le mot de passe correct devrait être deviné. C'est possible avec SocialScan.

g. Missing API Rate Limiting [8]

Les interfaces d'application dont les limites de ressources et de quotas sont absentes ou mal implémentées offrent aux attaquants la possibilité de réaliser des attaques Brute-Force sur des comptes d'utilisateurs ou de provoquer un déni de service. L'exploitation de cette vulnérabilité ne nécessite souvent même pas d'authentification ; elle requiert simplement l'envoi simultané de plusieurs requêtes.

h. Application Does Not Have A Strong Password Policy [9]

SocialScan n'a pas de politique de mot de passe ou ne l'applique pas correctement. Par exemple, il est possible d'utiliser un mot de passe composé d'une seule lettre.

i. Cleartexttraffic Is Set To True [11]

Selon le rapport d'audit, le trafic de données sur la plateforme Android s'effectue sans cryptage de transport (SSL/TLS), c'est-à-dire en texte clair (HTTP).

j. Application Is Vulnerable To Simultaneous Login [12]

Il est possible d'ouvrir plusieurs sessions avec les mêmes données d'identification. Cela augmente donc la surface d'attaque, puisqu'un attaquant peut utiliser de manière transparente des données d'identification valides en même temps que l'utilisateur légitime.

k. Application's Request/Response Reveals Sensitive Information [13]

Toutes les informations sensibles d'un point de vue technique (c'est-à-dire les données personnelles et les autres données qui pourraient potentiellement compromettre la sécurité des données, par exemple le mot de passe) ne sont pas obscurcies à l'aide d'une technique appropriée telle que le Salting.

l. *SSL Pinning Can Be Bypassed [14]*

Dans SocialScan, le SSL Pinning implémenté peut être contourné en insérant JavaScript au moment de l'exécution.

m. *Insecure Data Storage In File System [15]*

Les vulnérabilités du stockage des données surviennent lorsqu'on suppose que les utilisateurs ou les logiciels malveillants n'ont pas accès au système de fichiers d'un appareil mobile et donc aux informations sensibles contenues dans la mémoire de l'appareil. Il faut donc s'attendre à ce qu'un utilisateur malveillant ou un logiciel malveillant puisse avoir accès à des données sensibles dans SocialScan. Le rootage ou le jailbreak d'un appareil mobile contourne toute mesure de protection par cryptage.

n. *Insecure Content Security Policy (Csp)/X-Frame-Options [16]*

L'en-tête de réponse HTTP de X-Frame-Options dans SocialScan peut être utilisé pour spécifier si un navigateur est autorisé ou non à rendre une page dans un <frame>, <iframe>, <embed>, ou <object>.

o. *Missing HSTS Header [17]*

SocialScan n'utilise pas d'en-tête HSTS. Cela signifie que les communications non cryptées via HTTP sont autorisées.

p. *Information Leakage From Clipboard [18]*

SocialScan permet de copier-coller à partir du presse-papiers, notamment le copier-coller de mots de passe figurant dans le presse-papiers.

q. *Sensitive Data Disclosure In Recent Apps [19]*

Au vu du rapport, aucune précaution n'est prise pour empêcher l'utilisation de données sensibles (d'un point de vue technique) par des applications tierces (par exemple, en mettant en cache des instantanés d'applications).

r. *Application Has Set Insecure Permissions [21]*

Il s'est avéré que SocialScan n'avait pas défini des droits d'accès, ce qui constitue une menace pour la sécurité pouvant entraîner des fuites de données dans le pire des cas.

3. Appréciation juridique et recommandations

Sur la base des faits établis ci-dessus, notifiés aux parties le 20 mai 2021, le PFPDT considère ce qui suit (chapitre 3). Il tient à relever que contrairement à ce que peuvent laisser entendre les documents soumis par les parties, le PFPDT ne fonde pas ses considérations sur l'« attestation de conformité » d'un audit externe telle que mentionnée dans le document intitulé « COVID-19 – Dispositifs d'identification de la clientèle dans les établissements de restauration, Procédure de vérification technique – 15 octobre 2020 ». En effet, une telle attestation, bien que mentionnée dans ledit document figurant au dossier, n'a pas été soumise au PFPDT au cours de la procédure d'établissement des faits.

3.1. Rôles et responsabilités

Tel que constaté dans le cadre de l'établissement des faits du 20 mai 2021, les informations quant aux rôles et responsabilités des parties impliquées dans la présente procédure sont restées contradictoires (cf. chapitre 2.1).

Sur la base de la documentation soumise au PFPDT et des informations disponibles au public, le PFPDT constate que les deux sociétés ont décidé d'unir leurs efforts et leurs ressources en vue d'atteindre un but commun (amélioration du traçage dans le cadre de la pandémie du COVID-19) et ont ainsi développé le système SocialPass sous forme d'une co-édition.

En vertu de l'art. 3 lit. i LPD on entend par maître du fichier la personne privée (physique ou morale) qui décide du but et du contenu du fichier. Cependant, cette notion reflète une réalité ancienne, qui ne correspond plus aux besoins d'un monde digitalisé. En effet, cette notion remonte à une époque où les fichiers étaient constitués de classeurs et de fiches. La notion est avant tout utilisée dans le but de déterminer la personne responsable du traitement. Le PFPDT partage l'opinion de certains auteurs qui proposent de renoncer à employer cette notion et proposent que la responsabilité au sens de la LPD découle des faits du traitement de données (cf. RUDIN BEAT, Kommentar zu Art. 3 DSG, N 43, in: Baeriswyl/Pärli (Hrsg.), Stämpflis Handkommentar zum DSG, 2015).

Force est de constater que les sociétés NewCom4U Sàrl et SwissHelios Sàrl ont développé le système SocialPass ensemble, elles ont décidé du but et du contenu du fichier ainsi que des droits d'accès à ce fichier et ce sont elles qui assurent les divers traitements des données. Elles doivent dès lors être considérées toutes les deux maîtres du fichier au sens de la LPD.

La qualité de maître de fichier doit cependant être distinguée de celle de mandataire au sens de l'art. 10a LPD. Trois constellations différentes sont possibles en pratique : le mandant peut également être maître du fichier, le mandant et le mandataire peuvent être maîtres communs du fichier ou alors le mandataire peut être considéré maître du fichier, notamment lorsqu'il traite des données pour le compte de son client (cf. ROSENTHAL DAVID/JÖHRI YVONNE, Kommentar zu Art. 10a DSG, N 19, in Rosenthal/Jöhri (Hrsg.), Handkommentar zum Datenschutzgesetz sowie weiteren, ausgewählten Bestimmungen, 2008).

Dans le cas d'espèce, les dispositions légales pertinentes octroient une certaine marge de manœuvre aux exploitants d'établissements accessibles au public. En effet, le ch. 4.3. de l'annexe 1 de l'Ordonnance COVID-19 situation particulière fixe uniquement que dans le cadre des plans de protection « les coordonnées peuvent être collectées à l'aide de systèmes de gestion des réservations ou des membres, ou encore au moyen de formulaires de contact ». Aucune disposition fédérale ne vient préciser quels systèmes de gestion doivent être privilégiés. Les deux sociétés ont donc proposé une solution numérique afin d'améliorer le traçage dans le cadre de la pandémie du COVID-19 (cf. chapitre 1.2). Ce faisant, elles ont proposé un traitement de données à leurs clients respectifs. En créant le système SocialPass, elles ont décidé du but et du contenu du fichier ainsi que des droits d'accès à ce fichier et ce sont elles qui assurent les divers traitements des données. Ainsi, il découle des constatations du PFPDT que dans le cas d'espèce, les mandataires communs que sont les sociétés NewCom4U Sàrl et SwissHelios Sàrl doivent être considérés maître du fichier au sens de l'art. 3 lit. i LPD.

Dès lors, la question de savoir qui est le mandant, et s'il existe, le cas échéant, plusieurs mandants (les gouvernements des cantons respectifs, les restaurateurs pris individuellement, la faîtière des restaurateurs vaudois) peut rester ouverte.

Le maître du fichier est responsable de respecter le cadre légal lors de tout traitement de données et de garantir les droits aux personnes concernées tels que consacrés dans la LPD (cf. RUDIN, Art. 3 DSG, N 49 s. et ROSENTHAL, Art. 10a DSG, N 22). Le maître du fichier est avant tout responsable de faire suite aux éventuelles demandes d'accès des personnes concernées (art. 8 LPD).

Il découle de ce qui précède que les sociétés NewCom4U Sàrl et SwissHelios Sàrl ont la qualité de maître de fichier au sens de l'art. 3 lit. i LPD. Dès lors, il leur incombe de respecter les obligations légales prévues par la LPD, la LEp et l'Ordonnance COVID-19 situation particulière. En vertu de l'art. 4 al. 4 LPD la collecte de données personnelles, et en particulier les finalités du traitement desdites données, doivent être reconnaissables pour la personne concernée (principe de transparence). Le respect du principe de transparence permet en effet aux personnes d'exercer leur droit d'accès. Etant donné que les indications dans les différents documents sont contradictoires dans la mesure où certains documents mentionnent les deux sociétés tandis que d'autres ne mentionnent que l'une des deux sociétés en tant que maître du fichier, le PFPDT constate une violation du principe de transparence tel que consacré à l'art. 4 al. 4 LPD. En effet, en l'état actuel, les personnes concernées ne sont pas en mesure de déterminer avec certitude quelle personne morale traite leurs données et à qui, le cas échéant, elles devraient adresser une demande d'accès.

(1) Recommandation concernant les rôles et responsabilités :

Les sociétés NewCom4U Sàrl et SwissHelios Sàrl doivent uniformiser tous les documents (site web, appstores et app) afin de respecter leurs obligations légales en tant que maîtres du fichier au sens de l'art. 3 lit. i LPD.

3.2. Banque de données centralisée

3.2.1. Banque de données centralisée stricto sensu

La collecte des coordonnées des visiteurs (nom, prénom, numéro de téléphone, NPA) trouve son fondement dans l'art. 5 de l'Ordonnance COVID-19 situation particulière, qui oblige les exploitants d'établissements accessibles au public de collecter lesdites coordonnées. Cette disposition prévoit notamment que les exploitants collectent les coordonnées des visiteurs et les transmettent aux autorités cantonales sur demande, notamment aux fins d'identification et d'information des personnes qui se trouvaient dans l'établissement au même moment qu'une personne infectée et qui sont dès lors présumées infectées au sens de l'art. 33 LEp. Les coordonnées doivent impérativement être détruites après 14 jours.

Selon le ch. 4.5. de l'annexe 1 de l'Ordonnance COVID-19 situation particulière, il incombe à l'exploitant de garantir la confidentialité des coordonnées qu'il collecte ainsi que la sécurité des données, notamment durant leur conservation. Ainsi, en vertu des diverses dispositions applicables, il a été prévu que les coordonnées collectées restent chez les exploitants respectifs. Ce n'est qu'en cas d'infection dans un établissement déterminé que les autorités cantonales doivent avoir accès aux coordonnées des visiteurs de l'établissement concerné. En d'autres termes, il a été prévu que les exploitants des établissements gardent le contrôle sur les coordonnées qu'ils ont collectées. La disposition fédérale ne prévoit pas d'accès direct à toutes les coordonnées collectées dans tous les restaurants d'un même canton.

SocialPass doit être considéré en tant que système de gestion tel que prévu au ch. 4.3. de l'annexe 1 de l'Ordonnance COVID-19 situation particulière. En effet, cette disposition fixe que « les coordonnées peuvent être collectées à l'aide de systèmes de gestion des réservations ou des membres, ou encore au moyen de formulaires de contact ».

À la lumière de la LPD, les deux sociétés SwissHelios Sàrl et NewCom4U Sàrl doivent être considérées des tiers au sens de l'art. 10a LPD. Il découle de cette constatation que le système SocialPass ne devrait que permettre les traitements de données que le mandant serait en droit d'effectuer lui-même, c'est-à-dire que le système SocialPass, afin de tomber sous la définition du ch. 4.3. de l'annexe 1 de l'Ordonnance COVID-19 situation particulière, ne devrait que permettre d'effectuer les traitements tels que prévus dans l'Ordonnance COVID-19 situation particulière.

Cela étant, il convient de distinguer deux questions différentes qu'il convient d'analyser séparément par la suite.

Dans le cadre de ce premier sous-chapitre, il convient de se pencher sur la question de savoir si le cadre légal pertinent permet la mise en place d'une base de données centralisée. Si le cadre légal fédéral permet en effet la mise en place d'une base de données centralisée, se pose alors la question de savoir si dans le cas d'espèce, des mesures appropriées ont été mises en place afin de répondre aux exigences tenant à la sécurité de données sensibles (cf. art. 7 LPD) et aux exigences légales en matière de protection des données (notamment le principe de la proportionnalité).

Le ch. 4 de l'annexe 1 de l'Ordonnance Covid-19 situation particulière qui fixe les détails de la collecte des coordonnées n'apporte pas de précisions quant aux systèmes de gestion des réservations qui peuvent être utilisés pour la collecte (cf. ch. 4.3). Le Rapport explicatif concernant l'ordonnance COVID-19 situation particulière (y inclus grandes manifestations) du 26 mai 2021 n'apporte pas plus de précisions quant à cette question.

Les dispositions pertinentes se contentent de fixer que de tels systèmes peuvent être utilisés et que les exploitants ou les organisateurs doivent garantir la confidentialité des coordonnées qu'ils collectent et la sécurité des données, notamment durant leur conservation (cf. ch. 4.6.).

Sur la base de ces dispositions laissant une marge de manœuvre aux exploitants dans le choix du système de gestion des réservations ou des membres, le PFPDT conclut que l'Ordonnance COVID-19 situation particulière n'exclut pas, par principe, que les exploitants d'établissements accessibles au public utilisent des systèmes de gestion des réservations qui impliquent un enregistrement des données centralisé. Toutefois, cet enregistrement centralisé ne sera conforme aux exigences légales uniquement si les principes de la protection des données sont respectés et des mesures de sécurité appropriées sont mises en place en amont (cf. ch. 4.6. Ordonnance COVID-19 situation particulière et art. 7 LPD).

Le PFPDT retient dès lors que l'enregistrement des coordonnées collectées dans une base de données centralisée telle que prévue par le système SocialPass est conforme au cadre légal à condition que :

- les principes généraux de la loi sur la protection des données selon l'art. 4 ss. LPD sont respectés ;
- des mesures de sécurité appropriées aient été mises en place en amont, conformément à l'art. 7 LPD en relation avec les art. 8 et 9 OLPD, en particulier l'art. 9 al. 1 let. g OLPD (pour une analyse des mesures de sécurité mises en place, cf. chapitre 3.7).

Dans un deuxième temps, il convient dès lors d'analyser la question de savoir si la solution d'une base de données centralisées est également conforme au cadre juridique dans sa forme concrète.

3.2.2. *Divers droits d'accès à la base de donnée centralisée / fonctions de filtres*

Dans le cadre de ses analyses, le PFPDT a constaté que le fonctionnement du système SocialPass impliquait l'existence d'une base de données centralisée (cf. chapitre 3.2.1) qui offre plusieurs options de recherches ciblées (p.ex. les personnes ayant accès à cette base de données peuvent rechercher toutes les personnes s'appelant Laure ou Christophe ayant visité n'importe quel établissement public dans le canton du Valais au long des 14 derniers jours).

Force est de constater que le droit d'accès direct à la base de données centralisée octroyé aux autorités cantonales vaudoises et valaisannes, y compris les différentes options de recherches ciblées, peut conduire à la création de profils de personnalité au sens de l'art. 3 lit. d LPD. En effet, en fonction des établissements accessibles au public visités (p.ex. une maison close) et/ou en raison des personnes rencontrées lors de ces visites (p.ex. un visiteur rencontre un avocat spécialisé en droit pénal), les données ainsi assemblées peuvent permettre d'apprécier les caractéristiques essentielles de la personnalité des personnes concernées.

Au regard des dispositions légales pertinentes du droit fédéral, ces multiples possibilités de recherches ciblées apparaissent comme excessives, voire disproportionnées.

Le cadre légal fédéral pertinent ne prévoit ni le droit, pour les autorités cantonales, d'accéder à une base de données centralisée ni la création éventuelle de profils de personnalité. Dès lors, le système SocialPass permet un traitement de données qui va au-delà de ce qui est prévu par le cadre légal fédéral.

Pour les traitements éventuellement possibles allant au-delà de ce que prévoit le cadre légal fédéral, un motif justificatif au sens de l'art. 13 al. 1er LPD doit pouvoir être invoqué par les maîtres du fichier (consentement, intérêt prépondérant privé ou public, base légale). Or, dans le cas d'espèce, il semble que le seul motif justificatif invocable par des maîtres du fichier qui offrent un produit qui permet de soutenir les établissements accessibles au public dans l'accomplissement d'une tâche légale en temps de pandémie, ne peut qu'être qu'une base légale.

La base légale entendue comme une norme générale et abstraite peut relever du droit cantonal ou fédéral. La base légale doit être applicable au cas d'espèce et ne pas être contraire à une autre norme (hiérarchiquement supérieure).

De plus, le traitement de données justifié sur la base de cette base légale doit apparaître proportionné (cf. WERMELINGER, Stämpflis Handkommentar, Art. 13 DSG N 15).

En l'espèce, le cadre légal fédéral ne prévoit pas l'accès direct, pour les autorités cantonales, sur une base de données centralisée. En effet, le droit fédéral applicable au cas d'espèce prévoit que les exploitants des établissements accessibles au public maintiennent le contrôle sur les coordonnées

collectées et ne les transmettent à l'autorité publique compétente uniquement en cas d'infections présumées dans leur établissement.

Toutefois, tant que l'accès direct à la base de données centralisée n'entraîne pas un traitement des données allant au-delà de celui qui serait effectué si les données étaient remises à l'autorité sanitaire sur demande, cet accès semble être justifié, compte tenu de l'intérêt public à lutter contre la pandémie actuelle.

La question de savoir si et dans quelle mesure les réglementations cantonales peuvent justifier un accès plus étendu peut être laissée ouverte sur la base des considérations suivantes :

En effet, le PFPDT peut se prononcer sur la question de savoir si un acte cantonal constitue un motif justificatif au sens de l'art. 13 LPD pour un traitement de données effectué entre personnes privées. Dans ce cadre il lui incombe, entre autres, de déterminer si la base légale cantonale est conforme au droit fédéral hiérarchiquement supérieur, notamment si le dispositif cantonal est conforme à la LPD.

À ce titre, il convient de distinguer la situation dans le canton de Vaud de celle dans le canton du Valais (cf. lettre du 23 avril 2021 soumise au PFPDT par Lexing Switzerland).

Dans le canton de Vaud, le Chef du Département de l'économie, de l'innovation et du sport ainsi que la Cheffe du Département de la santé et de l'action sociale vaudois ont édicté la Directive du 15 septembre 2020 COVID-19 / Coronavirus. Selon l'art. 4 lit. e de cette Directive, « un dispositif d'identification de la clientèle doit être utilisé systématiquement. Ce dispositif doit être homologué par la faîtière de la branche, en concertation avec l'office du Médecin cantonal. Le dispositif d'identification doit permettre à garantir la fiabilité des données collectées aux fins d'identification des personnes présumées infectées, en particulier le nom, le prénom et le numéro de téléphone mobile. Les données sont conservées 14 jours avant destruction. Les données recueillies doivent être rendues accessibles en tout temps aux autorités sanitaires dans un format défini par ces dernières ».

Dans le document intitulé « Covid-19 – Dispositifs d'identification de la clientèle dans les établissements de restauration – Procédure de vérification technique – 15 octobre 2020 » (dont l'auteur n'est pas identifiable), soumis au PFPDT par les représentants des parties en annexe au courrier du 23.04.2021, il a été prévu que « les dispositifs d'identification doivent répondre aux spécifications techniques suivantes : [...] – permettre l'enregistrement des données des clients et du personnel sur la base de données centralisée gérée par SwissHelios Sàrl ».

Le même document prévoit, un peu plus bas, qu'« en cas de besoin, l'OMC [office du médecin cantonal] se rend sur la base de données, entre le nom de l'établissement X à une date et une heure T et peut extraire un fichier CSV contenant la liste des clients et du personnel présents à ce moment. Pour accéder aux données, l'OMC ne doit pas avoir besoin de passer par l'exploitant de l'établissement ou par les dispositifs d'identification ». S'il est vrai que la Directive du 15 septembre 2020 est de nature

générale et abstraite, force est de constater qu'elle ne fixe que dans des termes très généraux que les restaurateurs vaudois doivent utiliser un dispositif d'identification de manière systématique et que ce dispositif doit être homologué par la faîtière de la branche, en concertation avec l'office du Médecin cantonal.

Pour le reste, et notamment pour la question de savoir si les données collectées doivent être enregistrées sur une base de données centralisée accessible directement par les autorités publiques, cette disposition prévoit que les autorités sanitaires sont libres dans le choix des traitements de données mis en place. Ainsi, l'enregistrement dans une base de données centralisée ainsi que le droit d'accès direct octroyé aux autorités sanitaires a été prévu dans le document « Covid-19 – Dispositifs d'identification de la clientèle dans les établissements de restauration – Procédure de vérification technique – 15 octobre 2020 ».

Cet extrait de document, dont la nature juridique reste peu claire, ne constitue clairement pas la nature d'une norme générale et abstraite qui pourrait justifier l'accès dépassant le cadre de la législation fédérale pertinente des autorités sanitaires. Le PFPDT ne saurait donc admettre que l'accès direct sur la base de données centralisée permettant des recherches ciblées presque indéfinies octroyé au Médecin cantonal vaudois se fonde sur une base légale au sens de l'art. 13 al. 1er LPD.

En ce qui concerne un éventuel intérêt public prépondérant comme motif justificatif au sens de l'art. 13 LPD, il convient de relever que la lutte contre la pandémie est une tâche publique et non une tâche qui incombe aux personnes privées, pour quelque raison que ce soit, elle est régie par le droit public. Le fait que la base légale pertinente du Conseil fédéral ne prévoit pas d'accès direct doit également être considéré comme une indication que des droits d'accès aussi étendus n'ont pas été jugés nécessaires pour lutter contre la pandémie, et montre qu'il s'agit d'un traitement de données inutile et donc disproportionné.

Dans le canton du Valais, l'usage du système SocialPass a été rendu obligatoire par Décision du Conseil d'Etat du 2 décembre 2020 qui se lit comme suit : « la mise en œuvre de l'application électronique de traçage SocialPass est obligatoire (à défaut une liste exhaustive de tous les clients ». Par ailleurs, les détails de la mise à disposition du système SocialPass en Valais ont été définis dans le cadre d'une convention passée entre l'Etat du Valais, représenté par le Chef de son Service de la santé publique, et la société NewCom4U Sàrl, à la fin de l'année 2020. L'art. 2.1. dudit contrat oblige la société NewCom4U Sàrl à fournir une « base de données pour le traçage via scan ou autoscan de l'ID SocialPass ». Dans ce cadre, les SocialPass scannés dans les établissements sont stockés dans la base de données gérée par le mandataire et hébergés dans les serveurs Microsoft Azure localisés dans le canton de Zurich ». La même disposition contractuelle prévoit, un peu plus bas, que « [l]e mandataire développe, d'entente et sur la base d'un cahier des charges de l'Office du médecin cantonal, et supporte la base de données consultable par le Médecin cantonal et ses collaborateurs ; le mandataire assure à

cet effet le respect des exigences du Service cantonal de l'informatique pour permettre la consultation des données par le Médecin cantonal et ses collaborateurs depuis le réseau informatique de l'administration cantonale ».

La convention conclue entre la société NewCom4U Sàrl et l'Etat du Valais, représenté par le Chef de son Service de la santé publique, ne constitue pas une norme générale et abstraite pouvant justifier un traitement de données au sens de l'art. 13 al. 1er LPD. Dans ce cadre également, il n'existe donc pas de base juridique suffisante qui pourrait justifier un droit d'accès aussi étendu octroyé aux autorités sanitaires.

Il découle de ce qui précède que l'accès direct sur la base de données centralisée sous sa forme actuelle (prévoyant des possibilités de recherches ciblées), octroyé aux autorités cantonales, dépasse le traitement de données tel que prévu et justifié par le droit fédéral actuellement en vigueur et qu'il n'est pas justifié par une base légale cantonale au sens de l'art. 13 al. 1er LPD (norme générale et abstraite) et s'avère comme disproportionné.

Les responsables de SocialPass doivent donc limiter l'accès des autorités sanitaires susmentionnées aux données nécessaires pour une collecte légale des coordonnées.

(2) Recommandations :

La possibilité d'accès direct à la base de données centrale doit être limitée à ce qui est strictement nécessaire à la collecte légale des coordonnées, de sorte qu'elle soit proportionnée ; en particulier, la possibilité de rechercher des personnes doit être éliminée de cette manière.

Suite à l'élaboration puis à la notification du rapport et des recommandations dans leur version du 28 mai 2021, deux modifications du cadre légal tel que décrit au chapitre 3.2.2 doivent être relevées. Ces modifications mettent en évidence l'absence de base légale justifiant les possibilités de recherches ciblées telles que contestées dans la recommandation (2) de sorte qu'aucune modification de cette recommandation n'est indiquée.

D'une part, il convient de noter que lors de la visioconférence du 7 juin 2021, le PFPDT a été informé que la Directive du 15 septembre 2020 COVID-19 / Coronavirus du Chef du Département de l'économie, de l'innovation et du sport ainsi que de la Cheffe du Département de la santé et de l'action sociale vaudois a été abrogée en janvier 2021 bien que les représentants légaux de SocialPass aient justifié le traitement en invoquant cette base légale dans leur courrier du 23 avril 2021. Dès lors, les développements juridiques figurant au chapitre 3.2.2 du présent rapport ne sont plus pertinents. En d'autres termes, dans le canton de Vaud, le traitement de données tel que prévu par le système SocialPass n'est plus qu'encadré par le droit fédéral. Ainsi, en ce qui concerne un éventuel intérêt public

prépondérant comme motif justificatif au sens de l'art. 13 LPD, il convient de réitérer que la lutte contre la pandémie est une tâche publique et non une tâche qui incombe aux personnes privées. Pour quelque raison que ce soit, cette tâche est régie par le droit public. Dans les cantons où une disposition cantonale fait défaut, cette tâche est exclusivement régie par le droit public fédéral. La base légale pertinente du Conseil fédéral ne prévoit pas d'accès direct à une base de données centralisée. Les droits d'accès aussi étendus que ceux prévus par le système SocialPass n'ont donc pas été jugés nécessaires pour lutter contre la pandémie et ne sont dès lors par justifiés sur la seule base légale pertinente dans le canton de Vaud.

D'autre part, l'Ordonnance du Conseil fédéral Covid-19 situation particulière, qui encadre la collecte des coordonnées dans les établissements accessibles au public a fait l'objet d'une révision totale de sorte que la structure et la numérotation des articles ont changé.[6] L'art. 11 de l'Ordonnance (auparavant l'art. 5) est désormais la disposition essentielle pour la collecte des données des visiteurs. En sus des changements formels, l'obligation de collecter les coordonnées des visiteurs a été réduite : dans les restaurants, les clients doivent uniquement partager leurs coordonnées s'ils prennent place à l'intérieur. De plus, une seule personne par groupe doit communiquer ses coordonnées à l'exploitant de l'établissement. Dans les discothèques, l'obligation de collecter les coordonnées des clients a été supprimée. L'accès à ces événements est toutefois réservé aux personnes en possession d'un certificat Covid-19 (Art. 13 Ordonnance COVID-19 situation particulière). Dans les centres de sports et lors d'événements culturels, les coordonnées doivent toujours être collectées. Les changements susmentionnés sont entrés en vigueur le 26 juin 2021.

3.3. Option « saisie manuelle »

Le PFPDT constate que, d'une part, les coordonnées des clients réguliers sont enregistrées localement sur l'appareil et que, d'autre part, il est possible d'exporter ces données vers d'autres appareils au moyen d'un code QR. En outre, toutes les coordonnées des clients réguliers sont affichées sur les appareils utilisés par les établissements.

Avec la procédure choisie, la mise en œuvre de l'art. 5 LPD (exactitude des données) requiert un effort organisationnel considérable et ne permet même pas d'exclure certaines erreurs. Ainsi, les demandes d'information, de rectification ou d'effacement ne peuvent être traitées que de manière incomplète.

En outre, l'affichage de toutes les données de contact viole le principe de proportionnalité tel que consacré à l'art. 4 al. 2 LPD (d'un point de vue temporel et quantitatif), car l'établissement peut consulter

---

[6] Communiqué du Conseil fédéral du 23.06.2021 https://www.bag.admin.ch/bag/fr/home/das-bag/aktuell/medienmitteilungen.msg-id-84127.html.

à tout moment d'avantage de données sur une personne que ce qui est nécessaire pour identifier le client.

(3) Recommandation concernant la liste des clients réguliers SocialScan

SocialPass adapte les processus et les fonctions de collecte et de mise à disposition des coordonnées des personnes recourant plusieurs fois à l'application (par ex. les clients réguliers) de sorte que

- la collecte des coordonnées ne soit pas effectuée par le personnel de service,

- les coordonnées des clients réguliers que l'établissement a enregistrées puissent être effacées ou rectifiées à la demande de ces clients,

- la synchronisation de la liste des clients réguliers permette d'éviter des statuts de données différents au sein de la même structure, et que les données soient soumises à un cycle de vie axé sur la finalité,

- seules les coordonnées nécessaires à l'identification de la liste des clients réguliers puissent être consultées (principe de minimisation des données).

3.4. Transferts des numéros de téléphone aux États-Unis

Comme indiqué ci-dessus (ch. 2.5.2), les numéros de téléphone mobile des utilisateurs sont transmis au Service Twilio, et donc aux États-Unis d'Amérique dans le cadre du processus de vérification.

Les États-Unis tombe dans la catégorie des pays tiers ne disposant pas d'une législation adéquate au sens de l'art. 6 al. 1er LPD[7]. En dépit de l'absence d'une législation assurant un niveau de protection adéquat à l'étranger, l'art. 6 al. 2 LPD prévoit que des données personnelles peuvent être communiquées à l'étranger, à l'une des conditions prévues par cet alinéa. En l'espèce, aucune condition fixée à l'art. 6 al. 2 LPD n'est remplie. Le PFPDT relève avant tout que des garanties suffisantes, notamment de nature contractuelle, font défaut. Il découle de ce qui précède qu'un niveau de protection adéquat n'a pas été assuré par les responsables.

Même si l'intérêt (public) invoqué par les responsables afin de justifier la vérification des numéros semble compréhensible dans le contexte actuel, force est de constater qu'il n'est pas apparent pour quelles raisons il serait nécessaire de recourir à un service situé aux États-Unis, au lieu de mandater un service similaire ayant son siège dans un pays offrant un niveau de protection des données adéquat.

Par ailleurs, le PFPDT relève que les personnes concernées ne sont pas informées du transfert de leur numéro de téléphone aux États-Unis, ni même de l'utilisation du service Twilio. Aucune information à

[7] Liste des Etats ayant une législation assurant un niveau de protection adéquat, publié sous https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2020/staatenliste.pdf.download.pdf/20200908_Staatenliste_f.pdf

propos de Twilio n'est disponible ni sur le site internet ni dans les App-Store. Ce manque d'information constitue une violation du principe de transparence (art. 4 al. 4 LPD).

(4) Recommandation concernant le service de vérification des numéros

SocialPass apporte des garanties manifestes (p.ex. au moyen d'un accord avec Twilio) pour qu'un niveau de protection adéquat soit garanti dans le cadre du transfert des numéros de téléphone des utilisateurs au service « Twilio » aux Etats-Unis ;

Alternativement, SocialPass recourt à un service alternatif qui n'implique pas un transfert vers un pays étranger dont le niveau de protection est inadéquat.

Les utilisateurs sont informés de manière transparente sur le transfert des données au service de tiers (Twilio ou autre), des modalités d'enregistrement et des possibilités de demander l'effacement des propres données.

3.5. Stockage centralisé et permanent du numéro de téléphone mobile dans le processus d'enregistrement

Le PFPDT note que, pour que le traçage des contacts fonctionne, il est entre autres nécessaire que le numéro de téléphone mobile soit saisi dans SocialPass. Les numéros sont vérifiés au moyen du service OTP américain Twilio (cf. chapitre 2.5.2).

Les numéros de téléphone sont également enregistrés de manière centralisée dans la base de donnée Azure. Rien n'a été prévu quant à leur effacement. Les utilisateurs ne sont pas informés de manière transparente ni de l'enregistrement ni de l'utilisation que Twilio fait de leur numéro. De tels traitements de données ne répondent pas aux exigences fixées dans la LPD, notamment au principe de transparence tel que consacré à l'art. 4 al. 4 LPD. En outre, sur la base de l'art. 4 al. 2 LPD, le stockage centralisé du numéro de téléphone mobile lors du processus d'enregistrement est disproportionné (du point de vue temporel) dans la mesure où ce numéro est conservé pour une durée illimitée, c'est-à-dire une durée allant au-delà de ce qui est nécessaire pour la lutte contre le COVID-19.

(5) Recommandation concernant l'enregistrement centralisé et permanent du numéro de téléphone mobile dans le processus d'enregistrement

SocialPass adapte le processus d'inscription des utilisateurs de sorte que

- l'enregistrement centralisé du numéro de téléphone mobile soit limité au strict nécessaire pour le traitement visé, notamment en ce qui concerne la durée de l'enregistrement (au plus tard lorsque la situation particulière prend fin) ;

- les utilisateurs, avant d'installer l'application, soient informés de manière transparente quant au traitement de leur numéro de téléphone mobile ;

- les utilisateurs soient informés de leurs droits et, en particulier, de la manière dont elles peuvent exercer leurs droits pour que les données en lien avec l'enregistrement du numéro de téléphone mobile soient effacées.

3.6. Microsoft Azure (base de données SQL)

Deux des trois composants (SocialPass et SocialScan) ont fait l'objet d'une évaluation externe de la sécurité. Le troisième composant (base de données centrale sur Azure) n'a pas été audité au motif que Microsoft est responsable de la sécurité. Le PFPDT relève toutefois qu'en raison de plusieurs risques liés à la sécurité des données, comme p.ex. la possibilité d'un data breach, les responsables devraient être en mesure d'expliquer plus en détails pourquoi ils ont renoncé à un audit adéquat.L'application SocialPass communique avec une infrastructure centrale (*backend*) hébergée chez Microsoft Azure. Avec Azure, beaucoup de réglages sont prédéfinis, mais d'autres doivent être ajustés manuellement, comme les alertes et les accès utilisateurs. Pour la sécurité de la base de données Azure SQL, il est recommandé d'utiliser Azure Sentinel. Cela permet de recueillir des données sur l'ensemble des utilisateurs, des appareils, des applications et des infrastructures et de détecter et d'analyser les menaces.

Azure Sentinel ne permet toutefois pas de configurer, par exemple, des autorisations d'accès pour une base de données SQL. Or, conformément à l'art. 7 LPD, une telle configuration est obligatoire du point de vue de la sécurité des données. SocialPass n'a pas encore confirmé au PFPDT que la configuration dans Azure est mise en œuvre conformément au WhitePaper et à la Baseline[8] applicables (voir ci-dessous). Le PFPDT constate donc que les recommandations faites par Microsoft (Azure security baseline) sur la protection de la base de données SQL dans Azure sont insuffisamment mises en œuvre par SocialPass.

(6) Recommandation concernant la configuration et le renforcement de Microsoft Azure

SocialPass configure la plateforme Microsoft Azure de sorte que

a) les mesures de sécurité de la Baseline et du WhitePaper [I] de Microsoft soient mises en œuvre,
b) la vérification de l'efficacité et la mise en œuvre de ces mesures puissent être prouvées.

3.7. Divers aspects de sécurité des données

Les responsables ont affirmé que des améliorations concernant la sécurité des données ont été mises en place, sans toutefois les concrétiser. Les recommandations suivantes dans le domaine de la sécurité

[8] https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/sql-database-security-baseline (état au 21.4.2021).

des données sont donc formulées sous réserve que les vulnérabilités mises en lumière dans l'établissement des faits du 20 mai 2021 n'ont pas été corrigées entre-temps.

3.7.1. Gestion des vulnérabilités

Le PFPDT note que les audits externes ont décelé des vulnérabilités. Celles-ci ont été évaluées du point de vue de la sécurité informatique, mais pas de la sécurité des données au sens de l'art. 7 LPD en relation avec l'art. 8 OLPD. Cet aspect a fait l'objet d'une première évaluation, par le PFPDT, dans la section 2.9.4 Afin de garantir la sécurité des données conformément à l'art. 7 LPD, il faudrait classer toutes les vulnérabilités (risques élevés comme faibles) de manière décroissante selon leur dangerosité du point de vue du droit de la protection des données.

(7) Recommandation concernant la gestion des vulnérabilités

SocialPass adapte les applications SocialPass et SocialScan de sorte que

a) les vulnérabilités relevées dans les rapports d'audit [A] [B] et [C] soient éliminées en fonction des risques qu'elles représentent,
b) les vulnérabilités concernant la protection des données, en particulier, soient éliminées sans délai.

3.7.2. Mise en place d'une authentification forte

Le PFPDT constate que, sur la base des informations fournies, il n'est pas possible de savoir quels composants du système SocialPass sont sécurisés par l'authentification à deux facteurs et donc protégés contre tout accès, modification ou destruction non autorisés, si l'on se réfère à l'état actuel de la technique et à l'art. 7 LPD en relation avec l'art. 8 s. OLPD.

(8) Recommandation concernant la mise en place d'une authentification forte

SocialPass revoit l'accès à tous ses composants de sorte que ceux-ci, en fonction de l'état actuel de la technique, permettent une authentification robuste, voire y soient obligatoirement soumis si la protection des données l'exige.

3.7.3. Utilisation disproportionnée d'identifiants

Le PFPDT note que, outre le numéro de téléphone, le traitement des données dans le cadre de SocialPass englobe l'IMEI (International Mobile Equipment Identity, un numéro de série unique à quinze chiffres pour les appareils) et, dans le cas d'Android, également un UID (Unique ID) du numéro d'utilisateur provenant de Google Firebase. La saisie des données de contact en vue du traçage vise toutefois les personnes et non les appareils. Les opérateurs n'ont pas expliqué, et les informations disponibles n'indiquent pas clairement en quoi l'utilisation de ces identifiants est nécessaire.

Par conséquent, il est inutile, et par ce fait, disproportionné du point de vue de l'art. 4 al. 2 LPD, d'utiliser des identifiants spécifiques aux appareils et aux applications à cette fin. Les numéros de téléphone peuvent très bien être vérifiés sans que ces identifiants soient utilisés.

(9) Recommandation concernant le traitement des identifiants d'appareils

SocialPass renonce au traitement des identifiants qui ne sont pas nécessaires à la lumière de la finalité poursuivie, notamment IMEI, Firebase-ID et Unique ID provenant de Google Firebase.

3.7.4. Organisation et documentation relatives à la sécurité des données

Les responsables de SocialPass n'ayant pas soumis de documentation relative à la sécurité des données, dans le cadre de la présente procédure, portant sur les responsabilités en la matière, le PFPDT part du principe qu'une telle documentation fait défaut.

Le PFPDT constate en outre qu'il n'existe pas de règlement de traitement au sens de l'art. 11 OLPD incluant une stratégie de sécurité (notamment celle des données) pour SocialPass et SocialScan. Un tel règlement sert à mettre en œuvre et à documenter la stratégie de sécurité et décrit les mesures techniques et organisationnelles mises en œuvre au sens de l'art. 7 LPD.

En vertu de l'art. 11a al. 5 lit. a LPD, les responsables de la base de données ne sont pas soumis à l'obligation de déclaration d'un fichier, s'il est assumé que les données sont traitées par une personne privée en vertu d'une obligation légale. Par contre, l'art. 11 OLPD prévoit l'obligation d'élaborer un règlement de traitement pour les fichiers automatisés, y compris pour les maîtres de fichiers déliés de l'obligation de déclaration à condition que cette exception soit basée sur la lettre a de l'art. 11a al. 5 LPD.

(10) Recommandation concernant la documentation relative à la sécurité des données :

Les responsables de SocialPass se dotent d'un règlement de traitement portant notamment sur la sécurité des données et proposant une stratégie de sécurité documentée qui

a) comprenne des mesures organisationnelles et techniques relatives à la sécurité des données qui soient en phase avec l'état actuel de la technique,
b) attribue de manière claire et documentée les tâches qu'elle prévoit aux différents acteurs,
c) soit régulièrement contrôlée quant à l'efficacité de sa mise en œuvre.

4. Prises de position des parties

4.1. Remarques préliminaires relatives au droit d'être entendu

Ni l'art. 29 LPD ni l'art. 34 OLPD ne contiennent des règles spécifiques quant aux divers délais à respecter dans le cadre d'une procédure d'établissement des faits. La pratique du PFPDT en tant qu'autorité fédérale indépendante consiste à garantir un délai de réponse raisonnable aux parties afin que ces dernières puissent exercer leur droit d'être entendu. Si le PFPDT est tenu de garantir le droit d'être entendu aux parties impliquées dans une procédure d'établissement des faits, les parties elles-mêmes ont un devoir de collaboration consacré à l'art. 34 LPD.

Lorsque le PFPDT fixe les différents délais au cours de la procédure d'établissement des faits, il procède toujours aussi à une pesée des intérêts. D'une part, il prend en compte le besoin pour les parties d'avoir le temps de préparer leurs soumissions. D'autre part, il estime que les parties ont un devoir de collaborer et qu'il leur appartient de lui transmettre toute information utile au bon déroulement de la procédure, p.ex. lorsque certains éléments de faits subissent un changement en cours de procédure. Enfin, étant donné qu'une procédure d'établissement des faits n'est qu'engagée en cas d'« erreur de système », c'est-à-dire lorsqu'un traitement risque de porter atteinte à la personnalité d'une multitude de personnes, l'intérêt du public à être informé le plus tôt possible de cette erreur de système est pris en compte dans la pesée des intérêts.

La présente procédure porte sur une application numérique proposée par deux entreprises privées dans toute la Suisse pour lutter contre la pandémie actuelle. Cette application traite des données personnelles et affecte tout particulièrement la population des cantons de Vaud et Valais, notamment en raison des exigences des autorités sanitaires de ces deux cantons. Dans ce contexte, le PFPDT s'est efforcé de faire aboutir la procédure d'établissement des faits en temps utile. Toutefois, cette procédure s'est avérée exceptionnellement longue et compliquée. Lors de la fixation des délais de réponse et de l'évaluation des nombreuses demandes de prolongation de délais reçues (cf. chapitre 1.4), le PFPDT a donc, entre autres, dû tenir compte du fait que, la deuxième vague de la pandémie s'est calmée au début de l'été 2021. Cette évolution épidémiologique a eu pour conséquence que les restaurants ont pu rouvrir à ce moment-là. Ainsi, une reprise de l'utilisation de l'application SocialPass était imminente. Le PFPDT a donc estimé que la sensibilisation de la population aux risques du traitement de données était urgente.

4.2. Prise de position des parties relative aux faits établis le 20 mai 2021

Dans le cadre de la présente procédure, notamment au vu de la réouverture des terrasses des restaurants le 19 avril 2021, le PFPDT a remis des recommandations provisoires aux parties le 7 avril 2021. Le 23 avril 2021, les parties ont refusé ces recommandations par courrier de Lexing Switzerland.

Par lettre du 20 mai 2021, le PFPDT a ensuite communiqué aux parties les faits tels qu'établis au chapitre 2 afin qu'elles puissent prendre position. Au vu de la réouverture de l'intérieur des restaurants le 31 mai 2021, le PFPDT a estimé qu'un délai de réponse d'une semaine était approprié au regard des circonstances particulières de la présente affaire. Les parties ont décidé de laisser expirer le délai de réponse fixé au 27 mai 2021, notamment après que le PFPDT ait rejeté et leur demande de prolongation de délai d'au moins 30 jours et la demande de récusation des collaborateurs en charge du dossier soumise par Lexing Switzerland.

4.3. Prise de position des parties relative au rapport final et aux recommandations du 28 mai 2021

Par courrier du 28 mai 2021, le PFPDT a informé les parties de la fin de la présente procédure d'établissement des faits, leur a remis le présent rapport et les recommandations y relative dans leur version du 28 mai 2021 et les a invitées à lui faire savoir dans un délai de 30 jours, conformément à l'art. 29 al. 4 PFPDT, si elles acceptaient ou rejetaient les recommandations.

Par courrier du 14 juin 2021 au PFPDT, Lexing Switzerland a notifié la fin de son mandat dans la présente procédure. Cette fin de mandat a conduit le PFPDT à accorder une prolongation du délai de 30 jours jusqu'au 16 juillet 2021, notamment à la suite d'une demande des parties désormais agissant pour leur propre compte. Après que les parties aient révoqué la demande de récusation du personnel du PFPDT, deux visioconférences constructives ont eu lieu entre elles et le PFPDT le 7 et le 24 juin 2021, auxquelles ont également participé les autorités de santé et de protection des données ainsi que les associations de la gastronomie des cantons de Vaud et Valais. Sur la base des échanges qui ont eu lieu dans le cadre de ces deux visioconférences, les exploitants de SocialPass ont soumis, le 9 juillet 2021, une prise de position par rapport aux recommandations émises par le PFPDT dans son rapport notifié le 28 mai 2021. Le présent chapitre traite en détail des réponses reçues.

4.3.1. Recommandation (1) concernant les rôles et les responsabilités

La recommandation (1) formulée ci-dessus au chapitre 3.1 et reprise ci-dessous est la suivante:

> **(1) Recommandation rôles et responsabilités**
>
> Les sociétés NewCom4U Sàrl et SwissHelios Sàrl doivent uniformiser tous les documents (site web, appstores et app) afin de respecter leurs obligations légales en tant que maîtres du fichier au sens de l'art. 3 lit. i LPD.

Les exploitants de SocialPass confirment avoir donné suite à cette recommandation, toutefois sans apporter de précisions (l'affirmation correspondante est limitée à « fait »). En tout état de cause, le PFPDT prend note que les parties **acceptent** la recommandation (1) concernant les rôles et les responsabilités.

Le PFPDT constate en plus que, notamment dans la déclaration de confidentialité publiée sur le site web de SocialPass, seule l'entreprise NewCom4U Sàrl est mentionnée comme maître du fichier. Toutefois, cela ne correspond pas à l' appréciation du PFPDT (cf. chapitre 3.1) selon laquelle les deux sociétés doivent être considérées conjointement comme maîtres du fichier. La responsabilité commune doit être rendue transparente, c'est-à-dire que les deux maîtres du fichier doivent figurer de manière cohérente dans la documentation.

La recommandation (1) concernant les rôles et responsabilités n'a donc pas encore été complètement mise en œuvre à l'heure actuelle.

4.3.2. Recommandation (2) concernant la base de données centrale

La recommandation (2) formulée ci-dessus au chapitre 3.2 et reprise ci-dessous est la suivante :

> **(2) Recommandation**
>
> La possibilité d'accès direct à la base de données centrale doit être limitée à ce qui est strictement nécessaire à la collecte légale des coordonnées, de sorte qu'elle soit proportionnée ; en particulier, la possibilité de rechercher des personnes doit être éliminée de cette manière.

Les exploitants de SocialPass confirment avoir donné suite à cette recommandation centrale, toutefois sans apporter de précisions (l'affirmation correspondante est limitée à « fait »). En tout état de cause, le PFPDT prend note que les parties **acceptent** la recommandation (2) concernant l'accès direct à la base de données centrale et la possibilité de rechercher des personnes.

4.3.3. Recommandation (3) concernant la liste des clients réguliers SocialScan

La recommandation (3) formulée ci-dessus au chapitre 3.3 et reprise ci-dessous est la suivante :

> **(3) Recommandation concernant la liste des clients réguliers SocialScan**
>
> SocialPass adapte les processus et les fonctions de collecte et de mise à disposition des coordonnées des personnes recourant plusieurs fois à l'application (par ex. les clients réguliers) de sorte que
>
> - la collecte des coordonnées ne soit pas effectuée par le personnel de service,
>
> - les coordonnées des clients réguliers que l'établissement a enregistrées puissent être effacées ou rectifiées à la demande de ces clients,
>
> - la synchronisation de la liste des clients réguliers permette d'éviter des statuts de données différents au sein de la même structure, et que les données soient soumises à un cycle de vie axé sur la finalité,
>
> - seules les coordonnées nécessaires à l'identification de la liste des clients réguliers puissent être consultées (principe de minimisation des données).

À propos de cette recommandation, la prise de position des exploitants de SocialPass se lit comme suit:

> *« Ces informations ne sont disponibles que sur les appareils SOCIALSCAN des restaurants et pas dans la base centrale.*
>
> *a) Cette recommandation n'est pas praticable dans la perspective d'une personne âgée qui veut donner ses informations dans l'application. C'est donc au personnel que revient la tâche de saisir ces informations.*
>
> *b) Cette n'existe pas pour l'instant et nous prévoyions de l'implémenter dans une prochaine phase de développement.*
>
> *c) Le processus de synchronisation est basé sur la finalité car il permet une collecte de données conforme.*
>
> *d) Seules les informations minimales sont recueillies actuellement ».*

Le PFPDT déduit de cette réponse que les exploitants **acceptent partiellement** les recommandations (3) concernant la liste des clients réguliers SocialScan. Il prend acte des remarques quant à la praticabilité de la mise en œuvre des recommandations et décidera de la suite à donner à cette réponse dans le cadre d'éventuelles contrôles de suivi.

4.3.4. Recommandation (4) concernant le service de vérification des numéros

La recommandation (4) formulée ci-dessus au chapitre 3.4 et reprise ci-dessous est la suivante :

> **(4) Recommandation concernant le service de vérification des numéros**
>
> SocialPass apporte des garanties manifestes (p.ex. au moyen d'un accord avec Twilio) pour qu'un niveau de protection adéquat soit garanti dans le cadre du transfert des numéros de téléphone des utilisateurs au service « Twilio » aux Etats-Unis ;
>
> Alternativement, SocialPass recourt à un service alternatif qui n'implique pas un transfert vers un pays étranger dont le niveau de protection est inadéquat.
>
> Les utilisateurs sont informés de manière transparente sur le transfert des données au service de tiers (Twilio ou autre), des modalités d'enregistrement et des possibilités de demander l'effacement des propres données.

À propos de cette recommandation, les exploitants de SocialPass ont soumis au PFPDT la prise de position suivante :

> *« Twilio a établie des mesures de protection de données qui étaient approuvé par la Communauté Européenne. Binding Corporate Rules et* https://www.twilio.com/gdpr
>
> *Nous considérons que cela suffise comme garantie manifeste du niveau de protection de données.*

Twilio ne dispose seulement d'un numéro de téléphone qui n'est pas associé à un nom. Donc personne ne pourrait dire je suis xy veuillez effacer mon numéro tel. Le nom xy n'est pas dans la base de données, seulement un no. de tel. sans identifiant »

Les exploitants n'expliquent pas dans quelle mesure les mesures présentées répondent aux exigences du PFPDT en matière de garanties suffisantes au sens de la LPD[9]. Les exploitants ne se prononcent pas non plus sur l'aspect de la reconnaissabilité du traitement.

Le PFPDT déduit de cette réponse que les exploitants **n'acceptent pas** les recommandations (4) concernant le service de vérification des numéros. Il décidera de la suite à donner à cette réponse dans le cadre d'éventuelles contrôles de suivi.

4.3.5. Recommandation (5) concernant l'enregistrement centralisé et permanent du numéro de téléphone mobile dans le processus d'enregistrement

La recommandation (5) formulée ci-dessus au chapitre 3.5 et reprise ci-dessous est la suivante :

(5) Recommandation concernant l'enregistrement centralisé et permanent du numéro de téléphone mobile dans le processus d'enregistrement

SocialPass adapte le processus d'inscription des utilisateurs de sorte que

- l'enregistrement centralisé du numéro de téléphone mobile soit limité au strict nécessaire pour le traitement visé, notamment en ce qui concerne la durée de l'enregistrement (au plus tard lorsque la situation particulière prend fin),
- les utilisateurs, avant d'installer l'application, soient informés de manière transparente quant au traitement de leur numéro de téléphone mobile,
- les utilisateurs soient informés de leurs droits et, en particulier, de la manière dont elles peuvent exercer leurs droits pour que les données en lien avec l'enregistrement du numéro de téléphone mobile soient effacées.

À propos de cette recommandation, la prise de position des exploitants de SocialPass se lit comme suit:

« L'enregistrement centralisé du numéro de téléphone est limité comme recommandé. Les utilisateurs sont informés par la publication en https://www.socialpass.ch/mentionslegales/ »

[9] Cf. https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/handel-und-wirtschaft/uebermittlung-ins-ausland.html

Le PFPDT prend note que les parties **acceptent** la recommandation (5) concernant l'enregistrement centralisé et permanent du numéro de téléphone mobile dans le processus d'enregistrement.

Cependant, le PFPDT constate que la déclaration de confidentialité mentionnée ne porte que sur l'utilisation des données collectées pour le traçage des contacts. Or, la recommandation susmentionnée fait référence au stockage du numéro de téléphone au cours du processus d'enregistrement.

En raison de ce manque de clarté, le PFPDT estime que cette recommandation n'a pas été suivie de mesures concrètes et il en déduit que la recommandation n'a pas encore été mise en place complètement à l'heure actuelle.

4.3.6. Recommandation (6) concernant la configuration et le renforcement de Microsoft Azure

La recommandation (6) formulée ci-dessus au chapitre 3.6 et reprise ci-dessous est la suivante :

> **(6) Recommandation concernant la configuration et le renforcement de Microsoft Azure**
>
> SocialPass configure la plateforme Microsoft Azure de sorte que
>
> a) les mesures de sécurité de la Baseline et du WhitePaper [I] de Microsoft soient mises en œuvre,
> b) la vérification de l'efficacité et la mise en œuvre de ces mesures puissent être prouvées.

La réponse des exploitants de SocialPass à cette recommandation se lit comme suit:

« En cours d'implémentation. Disponible d'ici la fin du mois d'août. »

Le PFPDT prend note que les parties **acceptent** la recommandation (6) concernant la configuration et le renforcement de Microsoft Azure et attend les preuves correspondantes dès que la mise en œuvre de cette recommandation aura eu lieu.

4.3.7. Recommandation (7) concernant la gestion des vulnérabilités

La recommandation (7) formulée ci-dessus au chapitre 3.7.1 et reprise ci-dessous est la suivante :

> **(7) Recommandation concernant la gestion des vulnérabilités**
>
> SocialPass adapte les applications SocialPass et SocialScan de sorte que
>
> a) les vulnérabilités relevées dans les rapports d'audit [A] [B] et [C] soient éliminées en fonction des risques qu'elles représentent,
> b) les vulnérabilités concernant la protection des données, en particulier, soient éliminées sans délai.

Les exploitants de SocialPass confirment avoir donné suite à cette recommandation, toutefois sans apporter de précisions (l'affirmation correspondante est limitée à « fait »). En tout état de cause, le PFPDT prend note que les parties **acceptent** la recommandation (7) concernant la gestion des vulnérabilités.

4.3.8. Recommandation (8) concernant la mise en place d'une authentification forte

La recommandation (8) formulée ci-dessus au chapitre 3.7.2 et reprise ci-dessous est la suivante :

> **(8) Recommandation concernant la mise en place d'une authentification forte**
>
> SocialPass revoit l'accès à tous ses composants de sorte que ceux-ci, en fonction de l'état actuel de la technique, permettent une authentification robuste, voire y soient obligatoirement soumis si la protection des données l'exige.

Les exploitants de SocialPass confirment avoir donné suite à cette recommandation, toutefois sans apporter de précisions (l'affirmation correspondante est limitée à « fait »). En tout état de cause, le PFPDT prend note que les parties **acceptent** la recommandation (8) concernant la mise en place d'une authentification forte.

4.3.9. Recommandation (9) concernant le traitement des identifiants d'appareils

La recommandation (9) formulée ci-dessus au chapitre 3.7.3 et reprise ci-dessous est la suivante :

> **(9) Recommandation concernant le traitement des identifiants d'appareils**
>
> SocialPass renonce au traitement des identifiants qui ne sont pas nécessaires à la lumière de la finalité poursuivie, notamment IMEI, Firebase-ID et Unique ID provenant de Google Firebase.

La prise de position par rapport à cette recommandation se lit comme suit:

> *« Nous utilisons un identifiant qui ne correspond pas à IMEI ou FIREBASE-ID mais qui est unique et généré par l'application SocialPass ».*

Le PFPDT conclut de cette réponse que les exploitants de SocialPass **acceptent** la recommandation (9) concernant le traitement des identifiants d'appareils.

4.3.10. Recommandation (10) concernant la documentation relative à la sécurité des données

La recommandation (10) formulée ci-dessus au chapitre 3.7.4 et reprise ci-dessous est la suivante :

(10) Recommandation concernant la documentation relative à la sécurité des données :

Les responsables de SocialPass se dotent d'un règlement de traitement portant notamment sur la sécurité des données et proposant une stratégie de sécurité documentée qui

a) comprenne des mesures organisationnelles et techniques relatives à la sécurité des données qui soient en phase avec l'état actuel de la technique,
b) attribue de manière claire et documentée les tâches qu'elle prévoit aux différents acteurs,
c) soit régulièrement contrôlée quant à l'efficacité de sa mise en œuvre.

La prise de position par rapport à cette recommandation se lit comme suit :

> *« a) Nous allons nous doter d'un organigramme avec des fonctions dédiées à la sécurité des données. Il sera constitué d'un organe de direction qui veillera à l'application des normes en vigueur concernant la protection des données.*
> *b) Nous allons déléguer les tâches de documentation des processus et de l'exécution de ces processus auprès d'une compagnie externe.*
> *c) Nous allons nous doter d'un organe de vérification de l'exécution et de la maintenance des processus décrit au point b ».*

Le PFPDT conclut de cette réponse que les exploitants de SocialPass **acceptent** cette recommandation. Il attend les preuves correspondantes dès que la mise en œuvre de cette recommandation aura eu lieu.

5. Conclusion

Depuis le début de la procédure d'établissement des faits, qui s'est avérée exceptionnellement longue et compliquée, des ajustements importants ont été effectués par les responsables de SocialPass. En particulier, les exploitants de SocialPass ont affirmé avoir mis en œuvre la recommandation (2) concernant l'accès direct à la base de données centrale. Dès lors, le PFPDT suppose que les utilisateurs de SocialPass ne sont plus exposés à un accès potentiellement excessif sur leurs coordonnées de la part des autorités sanitaires (via une recherche ciblée des personnes dans la base de données centrale). De plus, les exploitants ont confirmé au PFPDT que les faiblesses techniques – en particulier celles relevées dans les recommandations (6) à (10) – ont été corrigées. Les risques d'une atteinte au droit de la personnalité des personnes concernées liés à l'utilisation de l'application SocialPass ont donc considérablement été réduits au cours de la procédure. Dans le cadre d'un éventuel suivi du contrôle,

le PFPDT reviendra sur les diverses implémentations des recommandations prévues et de manière ponctuelle sur d'autres aspects mentionnés dans le présent rapport.

Au vu de la sensibilité des données personnelles traitées et des réactions de la société civile, le contrôle du système SocialPass quant au respect des exigences de protection des données s'est avéré nécessaire et efficace. Les constatations faites et recommandations émises par le PFPDT pourront servir de marche à suivre pour d'autres exploitants privés, qui souhaiteraient développer des systèmes de gestion de réservations dans le cadre de la lutte contre la pandémie du Covid-19.

6. Suite de la procédure

La manière dont ces recommandations sont mises en œuvre en pratique relève de la seule responsabilité des exploitants de SocialPass qui sont affligés sur leurs déclarations et affirmations (art. 34 LPD). Dans le cadre de la poursuite de la coopération entre les exploitants de SocialPass et le PFPDT, notamment dans le cadre d'éventuels contrôles ultérieurs, le PFPDT se réserve le droit de contrôler le respect du cadre légal par les exploitants de SocialPass.

Dans la mesure où lesdites sociétés refusent ou ne suivent pas les recommandations, le PFPDT peut porter l'affaire devant le Tribunal administratif fédéral pour décision (art. 29 al. 4 LPD).

7. Publication de la recommandation en vertu de l'art. 30 al. 2 LPD

Pour les raisons susmentionnées, il existe un intérêt fondamental à sensibiliser le public en temps utile par rapport aux risques potentiels pour la sphère privée et le droit à l'autodétermination, qui émanent des applications numériques développées pour lutter contre la pandémie actuelle. Vu que la procédure d'établissement des faits s'est avérée exceptionnellement longue et compliquée, le 31 mai 2021 – jour de la réouverture des terrasses des restaurants – le PFPDT a donc informé le public quant aux aspects principaux de la procédure d'établissement des faits clôturée le 28 mai 2021, y compris par rapport aux recommandations principales : SocialPass: limitation des possibilités de recherche requise (admin.ch).

La publication du rapport intégral dans sa version du 4 août 2021 n'aura lieu que sous réserve que du point de vue des sociétés SwissHelios Sàrl et NewCom4U Sàrl aucune donnée confidentielle qui pourrait révéler des secrets d'affaire ou influencer la capacité concurrentielle ne figure dans le rapport.

Les sociétés SwissHelios Sàrl et NewCom4U Sàrl sont priées de vérifier que le rapport de contrôle ne contienne pas de telles informations confidentielles et de confirmer cet état de fait par écrit au PFPDT dans un délai de 10 jours.

Le Préposé fédéral à la protection
des données et à la transparence

Berne, le 4 août 2021

Adrian Lobsiger