CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Missions de vérification de la CNIL portant sur la conformité à la règlementation de tout traitement accessible à partir de l'application « TousAntiCovid » ou portant sur des données à caractère personnel collectées à partir de cette application (octobre 2020-juillet 2021)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Le 22 octobre 2020

Décision n° 2020-270C de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, notamment ses articles 8-2° g), 10 et 19 ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2019-021 du 28 février 2019 portant délégation de pouvoirs de la Commission nationale de l'informatique et des libertés à sa présidente et à sa vice-présidente déléguée ;

Considérant qu'il importe de vérifier la conformité à la loi du 6 janvier 1978 modifiée, au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et à la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016, de tout traitement accessible à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, ou portant sur des données à caractère personnel collectées à partir de cette application ;

Décide de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de portant sur ces traitements, le cas échéant, en tout lieu susceptible d'être concerné par leur mise en œuvre.

La Présidente,

M-L. Denis

Marie-Laure DENIS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Le 03/11/2020

ORDRE DE MISSION

Le secrétaire général de la Commission nationale de l'informatique et des libertés ;

Vu la convention du Conseil de l'Europe n° 108 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ;

Vu le code de la sécurité intérieure, notamment ses articles L. 251-1 et suivants ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, et notamment ses articles 8-2° g), 10 et 19 ;

Vu le décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la décision du 6 avril 2020 portant habilitation de certains agents de la Commission nationale de l'informatique et des libertés à effectuer les visites ou les vérifications portant sur les traitements relevant de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° 2019-021 du 28 février 2019 portant délégation de pouvoirs de la Commission nationale de l'informatique et des libertés à sa présidente et à sa vice-présidente déléguée ;

Vu la délibération n° HAB-2020-002 du 23 juillet 2020 habilitant des agents de la CNIL à procéder à des missions de vérification ;

Charge, [redacted] de procéder, dans les conditions prévues à l'article 19 de la loi du 6 janvier 1978 modifiée, aux vérifications décidées par la Présidente dans sa décision n°2020-270C du 22 octobre 2020.

Le secrétaire général,

Louis DUTHEILLET de LAMOTHE

Service des contrôles

MONSIEUR LE MINISTRE
MINISTERE DES SOLIDARITES ET DE LA SANTE
14 AVENUE DUQUESNE
75350 PARIS

Paris, le 18 NOV. 2020

N/Réf : [redacted] Décision n°2020-270C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 001 8447 8

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle ayant eu pour objet de procéder à la vérification sur place de la conformité de tout traitement accessible à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, ou portant sur des données à caractère personnel collectées à partir de cette application, aux dispositions du règlement (UE)2016/679 du Parlement européen et du Conseil du 27 avril 2016 et de la loi n°78-17 du 6 janvier 1978 modifiée. Ce contrôle s'est déroulé dans les locaux de l'INRIA, situés 2 rue Simone Iff, à PARIS (75012)

En application de l'article 31 du décret n° 2019-536 du 29 mai 2019, vous trouverez ci-joint copies de la décision et de l'ordre de mission relatifs à ce contrôle ainsi que des procès-verbaux établis à cette occasion.

La Commission ne manquera pas de vous tenir informé des suites qui seront apportées à ce contrôle.

Je vous prie d'agréer, Monsieur Le Ministre, mes salutations distinguées.

[redacted]

P.J. : Décision n° 2020-270C
Ordre de mission
Procès-verbal n°2020-270-2
Procès-verbal n°2020-270-3

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

MONSIEUR LE MINISTRE
MINISTERE DES SOLIDARITES ET DE LA SANTE
14 AVENUE DUQUESNE
75350 PARIS

Paris, le 25 novembre 2020

N/Réf : [redacted] Décision n° 2020-270C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 1311 6

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés (CNIL) est habilitée, aux termes de l'article 19 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, à procéder à des contrôles qui peuvent s'effectuer en ligne. Sur ce fondement, un contrôle de l'application « TousAntiCovid » a été opéré.

En application de l'article 33 du décret n° 2019-536 du 29 mai 2019, vous trouverez ci-joint copies de la décision et de l'ordre de mission, ainsi que du procès-verbal établi dans ce cadre. Ce procès-verbal est composé d'une partie dédiée aux constatations effectuées sur l'application « TousAntiCovid » dont vous trouverez une copie papier jointe à ce courrier ainsi que trois annexes, la première présentant la recette de l'environnement technique utilisé, la deuxième, les mises à jour relatives à l'environnement technique, et la troisième, les vérifications effectuées préalablement au contrôle.

Vous trouverez joint à ce courrier un DVD-ROM contenant :

- une archive chiffrée (7-Zip) comprenant le procès-verbal de constatation, ses trois annexes, et, le cas échéant, les pièces issues du contrôle ;
- une notice explicative relative au déchiffrement de l'archive précitée ;
- les exécutables d'installation du logiciel 7-Zip.

J'invite vos services à se rapprocher du service des contrôles de la CNIL (assistantscontroles@cnil.fr) afin d'obtenir le mot de passe permettant le déchiffrement de l'archive susmentionnée.

Je vous précise que le contrôle a plus spécifiquement porté sur :

- la pertinence des données collectées (article 5-1-c du RGPD) ;
- l'information des personnes (articles 12 à 13 du RGPD) ;
- l'exercice des droits des personnes (article 15 à 21 du RGPD) ;
- la sécurité et confidentialité des données (article 32 du RGPD).

Par ailleurs, les constatations auxquelles il a été procédé n'excluent pas la faculté pour la CNIL de poursuivre le contrôle sur place ou sur convocation.

Vous pouvez présenter toute observation relative à ce procès-verbal en écrivant à Madame la Présidente de la Commission nationale de l'informatique et des libertés (3 place de Fontenoy TSA 80715 - 75334 PARIS CEDEX 07).

Pour plus d'informations sur les droits et obligations des organismes faisant l'objet d'un contrôle ainsi que sur le déroulement et les suites d'un contrôle, vous trouverez en pièce jointe une synthèse de la charte des contrôles de la CNIL. Cette charte est également disponible en intégralité sur le site internet de la CNIL (www.cnil.fr).

En tout état de cause, vous trouverez toute information utile sur le site internet de la CNIL (www.cnil.fr). [redacted]

La Commission ne manquera pas de vous tenir informé des suites qui seront apportées à ce contrôle.

Je vous prie d'agréer, Monsieur le Ministre, mes salutations distinguées.

[redacted]

P.J. : Décision n° 2020-270C
Ordre de mission
Procès-verbal n° 2020-270/1
Synthèse de la charte des contrôles de la CNIL
DVD-ROM

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

MINISTÈRE DES SOLIDARITÉS
ET DE LA SANTÉ
MONSIEUR LE MINISTRE
14 AVENUE DUQUESNE
75350 PARIS SP 07

Paris, le 180121

N/Réf. : [redacted]**CS201056**
LRAR n° 2C 156 060 2433 6
À rappeler dans toute correspondance

Monsieur le Ministre,

Conformément aux décisions **n° 2020-097C** du 28 mai 2020 et **n° 2020-270C** du 22 octobre 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué des contrôles de l'ensemble des traitements accessibles à partir de l'application mobile **StopCovid**, désormais dénommée **TousAntiCovid**, mis en œuvre par le ministère des Solidarités et de la Santé et dont les conditions de mise en œuvre sont encadrées par le décret n° 2020-650 du 29 mai 2020.

Ces contrôles ont eu pour objet de vérifier la conformité de cette application mobile aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et de la loi du 6 janvier 1978 modifiée.

À la suite d'une première série de contrôles effectuée au mois de juin 2020, le ministère des Solidarités et de la Santé a été mis en demeure, le 15 juillet 2020, de mettre en conformité le traitement des données en lien avec l'application StopCovid au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et à l'article 82 de la loi du 6 janvier 1978 modifiée.

Les mesures prises par le ministère des Solidarités et de la Santé pour se mettre en conformité avec les injonctions prononcées ont permis à la Présidente de la CNIL de procéder à la clôture de la mise en demeure par décision du 3 septembre 2020.

La Commission a effectué une nouvelle série de contrôles en octobre et novembre 2020, ayant notamment pour objet de vérifier la pérennité des mesures prises suite à la mise en demeure du 15 juillet dernier ainsi que la conformité au Règlement et à la loi « Informatique et Libertés » des nouvelles fonctionnalités proposées par la nouvelle version de l'application mobile désormais dénommée TousAntiCovid.

À titre liminaire, en ce qui concerne les mesures mises en œuvre consécutivement à la mise en demeure du 15 juillet 2020, je prends note que les contrôles effectués en novembre 2020 ont permis de constater l'effectivité de l'ensemble des mesures prises par le ministère des Solidarités et de la Santé. Ces éléments n'appellent dès lors aucune observation complémentaire de ma part.

Sans préjuger des suites qui seront apportées à cette procédure de contrôle et des vérifications complémentaires que la CNIL pourrait être amenée à réaliser à l'avenir, les constatations effectuées me conduisent toutefois à vous faire part des observations suivantes.

En premier lieu, la délégation a constaté que la nouvelle version de l'application TousAntiCovid, déployée le 22 octobre 2020, permet aux utilisateurs de générer, directement dans l'application, une attestation de déplacement dérogatoire. Les données traitées dans ce cadre sont les nom, prénom, date de naissance, lieu de naissance, adresse, date, heure et motif de sortie. La délégation a constaté que l'ensemble des données traitées dans le cadre de cette nouvelle fonctionnalité est stocké localement, dans l'ordiphone de l'utilisateur, et présenté au format texte, encodé dans un QR code.

La délégation a également été informée de l'implémentation d'une seconde fonctionnalité permettant d'informer les utilisateurs, au sein de l'application TousAntiCovid, sur la circulation du virus au niveau national.

Je note que, dans une logique de minimisation des données et de protection des données dès la conception et par défaut, aucune des données traitées dans le cadre de ces nouvelles fonctionnalités, telles que mises en œuvre au moment où les contrôles de la CNIL ont été effectués en novembre 2020, ne fait l'objet d'une transmission vers le serveur central.

En deuxième lieu, depuis septembre 2020, la délégation a constaté l'intégration dans les versions iOS de l'application d'un système de « notification push ». Cette nouvelle fonctionnalité a pour but de permettre le bon fonctionnement de l'application TousAntiCovid installée sur des terminaux iOS en bénéficiant de ressources matérielles suffisantes, allouées par le système d'exploitation lors de la réception de cette notification, pour exécuter une requête « *status* » propre au protocole ROBERT. Cette fonctionnalité entraîne l'envoi de données à caractère personnel supplémentaires, au serveur central ainsi qu'au serveur de notification d'Apple, et notamment un identifiant unique, spécifique au terminal et à l'application installée sur celui-ci.

Or, je note qu'au jour des contrôles, aucune de ces données à caractère personnel transmises au serveur central n'était mentionnée dans le décret n° 2020-650 du 29 mai 2020 au titre des données traitées. Dès lors, je vous invite à procéder à la modification du décret afin de les y intégrer.

En troisième lieu, je vous rappelle que la CNIL avait demandé, dans son avis du 25 mai 2020, que l'impact effectif du dispositif sur la stratégie sanitaire globale soit étudié et documenté par le Gouvernement de manière régulière pendant toute sa période d'utilisation. Cette demande avait été réitérée dans le cadre de la mise en demeure MED-2020-015 du 15 juillet 2020.

À cet égard, je prends note de l'augmentation significative des métriques de l'application telles que le nombre d'utilisateurs déclarés positifs ainsi que ceux notifiés via l'application. En outre, si une étude visant à identifier les freins et les leviers au téléchargement de l'application StopCovid a été commandée par le ministère des Solidarités et de la Santé et une étude a été initiée par l'INSERM de sa propre initiative sur l'impact du traçage numérique des contacts et l'isolation du foyer sur la transmission de l'épidémie de COVID-19, ces mesures n'apparaissent pas pleinement suffisantes afin de documenter l'efficacité de l'application mobile dans le cadre de la stratégie sanitaire globale.

Je vous invite dès lors à poursuivre le développement d'initiatives et d'indicateurs complémentaires afin d'évaluer pleinement l'effectivité sanitaire du dispositif.

Mes services [redacted] se tiennent à la disposition des vôtres pour toute information complémentaire.

Je vous prie d'agréer, Monsieur le Ministre, mes salutations distinguées.

M.-L. D.

Marie-Laure DENIS

Copie à [redacted] Déléguée à la protection des données)

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS 3, place de Fontenoy – TSA 80715 75334 PARIS Cedex 07 www.cnil.fr	**PROCÈS-VERBAL DE CONSTATATIONS EN LIGNE**

En application des dispositions prévues par les articles 55 à 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les articles 10, 19 et 25 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, L. 251-1 et suivants du code de la sécurité intérieure, le cas échéant, et des articles 16 à 37 du décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 précitée ;

Je soussigné [redacted]
agents de la CNIL, dûment habilités dans les conditions prévues à l'article 19 de la loi précitée ;

Conformément à la décision de la présidente de la CNIL **n°2020-270C** en date du **22 octobre 2020**, la mission de contrôle a pour objet de procéder à la vérification de la conformité des traitements accessibles à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée et du règlement (UE) 2016/679 susvisés ;

Disons débuter la mission de contrôle le 28 octobre 2020, à 10h, depuis les locaux de la CNIL, situés 3, Place de Fontenoy à PARIS (75007) ;

Mentionnons utiliser un téléphone de marque Google, modèle Pixel 3 XL.

Mentionnons que le téléphone de marque Google utilisé pour le présent contrôle est réinitialisé dans ses paramètres d'usine ;

Mentionnons démarrer le téléphone de marque Google ;

Mentionnons que le système est à jour :

Votre système est à jour

Version d'Android : 11
Mise à jour de sécurité Android : 5 octobre 2020

Dernière recherche de mise à jour à 11:28

Installation de l'application « TOUS ANTI COVID » sur le téléphone de marque Google

Saisissons « tousanticovid » dans la barre de recherche du Google Play Store (voir pièces) ;

Sélectionnons le premier résultat (voir pièces) :

TousAntiCovid
Gouvernement

Installer

Cliquons sur « Coordonnées du développeur » ;

Prenons copie de l'intégralité de la page ;

Cliquons sur « A propos de l'appli » ;

Cliquons sur « À propos de l'appli → » ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur « En savoir plus » ;

Cliquons sur précédent à deux reprises ;

Prenons copie de chaque capture d'écran proposées dans le Google Play Store ;

Cliquons sur « Installer » ;

Ouvrons l'application ;

 Paraphes [redacted]

Constatons l'apparition d'une notification :

Cliquons sur cette notification et constatons l'affichage suivant :

Prenons copie de l'intégralité de la page ;

Cliquons sur « Voir tous les chiffres » ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Lire toutes les actualités » ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Où me faire dépister ? » ;

Constatons l'ouverture d'une page web au domaine « sante.fr » (voir pièces) :

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Attestation couvre-feu » ;

Constatons l'ouverture d'une page web au domaine « gouv.fr » (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Gérer mes données » ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Confidentialité » ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur « Plus d'informations sur RGPD → » ;

Constatons l'ouverture d'une page web au domaine « gouv.fr » (voir pièces) ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « À propos de TousAntiCovid → » ;

Constatons l'ouverture d'une page web au domaine « gouv.fr » (voir pièces) ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Code source de l'application → » ;

Constatons l'ouverture d'une page web au domaine « inria.fr » (voir pièces) ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur ;

Cliquons sur « Politique de protection des données → » ;

Constatons l'ouverture d'une page web au domaine « gouv.fr » (voir pièces) ;

Prenons copie de l'intégralité de la page (voir pièces) ;

Cliquons sur le bouton « précédent » du navigateur à trois reprises ;

Constatons revenir à l'écran d'accueil :

Cliquons sur « Je veux participer » ;

Cliquons sur « Continuer » ;

Cliquons sur « Accepter » et constatons l'affichage suivant :

Autoriser les "contacts Bluetooth"

TousAntiCovid a besoin d'utiliser le Bluetooth de votre téléphone pour fonctionner.
Aucune donnée de géolocalisation n'est échangée ou enregistrée.

Cliquons sur « Autoriser » et constatons l'affichage suivant :

Cliquons sur « J'AI COMPRIS » et constatons l'affichage suivant :

Cliquons sur « Lorsque vous utilisez l'application » et constatons l'affichage suivant :

Cliquons sur « Accepter » et constatons l'affichage suivant :

Cliquons sur « Autoriser » et constatons l'affichage suivant :

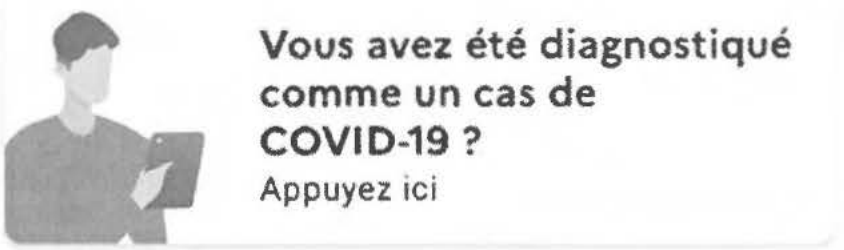
Cliquons sur « Autoriser les notifications » et constatons l'affichage suivant :

Cliquons sur « C'est noté » et constatons l'affichage suivant :

Cliquons sur « Activer TousAntiCovid » et constatons l'affichage suivant :

Renseignons « ffTY » dans le champ correspondant et cliquons sur « Confirmer » :

Constatons l'affichage suivant :

Cliquons sur « 

» ;

Cliquons sur « Saisir le code » ;

Saisissons « 654321 » et cliquons sur « Valider » ;

Cliquons sur « Aujourd'hui » et constatons l'affichage suivant :

Cliquons sur « OK » ;

Cliquons sur le bouton « précédent » à 4 reprises ;

Constatons que, le téléphone verrouillé, une notification reste visible :

Le responsable des traitements peut présenter toute observation relative au présent procès-verbal en écrivant à Madame la Présidente de la Commission nationale de l'informatique et des libertés (3, Place de Fontenoy TSA 80715, 75334 PARIS CEDEX 07) ;

La mission de contrôle s'est terminée, ce jour, à 15h ;

Signature de l'agent chargé de la mission de contrôle
[redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

INVENTAIRE DES PIÈCES DU PROCÈS-VERBAL DE CONSTATATIONS EN LIGNE

Les copies, notamment informatiques, effectuées par la délégation de la CNIL font l'objet de mesures de protection particulières destinées à assurer leur confidentialité.

Les copies numériques mentionnées ci-dessous font l'objet d'un calcul d'empreinte numérique garantissant leur intégrité et leur authenticité.

Ces empreintes numériques sont calculées par l'intermédiaire de l'algorithme SHA256.

[redacted]

 Paraphes [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Signature de l'agent chargé de la mission de vérification
[redacted]

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS 3, place de Fontenoy – TSA 80715 75334 PARIS Cedex 07 www.cnil.fr	**PROCÈS-VERBAL DE CONTRÔLE SUR PLACE**

En application des dispositions prévues par les articles 55 à 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les articles 10, 19 et 25 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, L. 251-1 et suivants du code de la sécurité intérieure, et des articles 16 à 37 du décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 précitée ;

Conformément à la décision de la présidente de la CNIL n°2020-270C en date du 22 octobre 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité de tout traitement accessible à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, ou portant sur des données à caractère personnel collectées à partir de cette application aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n°78-17 du 6 janvier 1978 modifiée ;

Nous soussignés, [redacted] agents de la CNIL, dûment habilités à procéder à des missions de vérification sur place ;

Le présent procès-verbal ainsi que les pièces annexées et celles pouvant être transmises ultérieurement sont susceptibles d'être communiquées à d'autres autorités de contrôle en application du chapitre VII section 2 du règlement (UE) 2016/679 susvisé ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 12 novembre 2020, à 9h, dans les locaux de INRIA, situés 2 rue Simone Iff à PARIS (75012) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité [redacted] a reçu et pris connaissance, au début du contrôle, de l'objet des vérifications, de l'identité et de la qualité des personnes chargées du contrôle, ainsi que des dispositions prévues à l'article 19 de la loi précitée ; le responsable des lieux a été informé au début du contrôle de son droit d'opposition et ne l'a pas exercé ;

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En introduction, [redacted] nous présente un document résumant l'ensemble des évolutions apportées à l'application StopCovid, renommée TousAntiCovid, depuis la notification de la mise en demeure.

Prenons copie du document de présentation des évolutions utilisé par INRIA en introduction du contrôle (voir pièces).

En ce qui concerne les mesures prises suite à la mise en demeure de la CNIL

La délégation est informée des éléments suivants :

Il n'y a pas eu de modification des acteurs impliqués dans le traitement de StopCovid devenu TousAntiCovid.

Demandons copie de tous les documents encadrant la relation contractuelle entre le Ministère et INRIA, ainsi qu'entre INRIA et l'ensemble des acteurs intervenants dans les traitements accessibles au sein de l'application TousAntiCovid (anciennement StopCovid).

Suite à la mise en demeure de la CNIL, les filtres de l'historique des contacts au niveau du téléphone de l'utilisateur ont été activés. INRIA a été ajouté comme sous-traitant en tant que destinataire dans les mentions d'information, les clauses relatives au RGPD ont été complétées dans les contrats de sous-traitance, la description de la solution anti-DDOS a été ajoutée dans l'analyse d'impact sur la protection des données, l'utilisation de la version 1.0. de l'application a été bloquée.

Prenons copie de la dernière version de l'AIPD et du registre de traitement.

La mise à jour forcée de l'application, de manière à supprimer toute utilisation de [redacted] ne concerne que les versions inférieures à la version 1.1. Ainsi, un utilisateur ayant installé StopCovid entre le 26 juin et le 22 octobre (1.1) peut continuer aujourd'hui à utiliser son

application dans cette version. L'utilisateur ayant téléchargé l'application entre le 22 octobre et le 3 novembre peut continuer à utiliser la version 2.0.

Sommes informés que les versions actuelles de l'application sont les suivantes :

- IOS : version 2.1.3 (3ème chiffre : correction mineure sans nouvelle fonctionnalité majeure)
- Android : version 2.1.1

En notre présence et à notre demande, [redacted] se connecte au compte développeur du panneau de visualisation de l'App Store (voir pièces).

Constatons les chiffres relatifs aux téléchargements de l'application iOS sur les périodes suivantes (voir pièces) du 2 juin au 26 juin, du 26 juin au 22 octobre, du 22 octobre au 3 novembre, du 3 novembre au 10 novembre.

Demandons les captures d'écrans sur Play Store pour les 4 mêmes périodes.

[redacted] nous informe qu'à sa connaissance les pays affichés dans le panneau de visualisation correspondent aux pays des stores initiaux des utilisateurs. Par exemple, un utilisateur ayant acheté un iPhone aux Etats-Unis et vivant en France depuis plusieurs années sera un « téléchargement américain ».

En notre présence et à notre demande, [redacted] nous présente le panneau de visualisation présentant les activations (ROBERT) des applications mobiles sur plusieurs périodes dont les quatre précitées (voir pièces).

En ce qui concerne le CAPTCHA :

La délégation est informée des éléments suivants :

La solution CAPTCHA mise en œuvre par [redacted] est la même depuis la v1.1 de l'application.

Demandons l'extrait de code responsable de l'exécution du CAPTCHA (frontend et backend) ainsi que l'URL correspondante sur le Gitlab d'INRIA.

Demandons une capture d'écran actualisée, telle que celle transmise précédemment et démontrant l'arrêt du webservice lié au [redacted]

En ce qui concerne la solution anti- DDOS :

La délégation est informée des éléments suivants :

La solution anti-DDOS mise en œuvre par [redacted] est aujourd'hui la même que celle présentée lors du dernier contrôle. La relation contractuelle est la même.

Il n'y a pas eu de modification fonctionnelle de la solution anti-DDOS mais le seuil d'alerte a été modifié pour tenir compte de l'augmentation du nombre de téléchargements [redacted]

[redacted] nous informe que le Ministère s'interroge sur les attentes de la CNIL au regard de l'obligation de mettre les solutions anti-DDOS dans les analyses d'impact de

protection des données dans la mesure où cela fait partie des dispositifs de sécurité indispensables et communs pour protéger les serveurs.

En ce qui concerne les nouvelles fonctionnalités de l'application TousAntiCovid

La délégation est informée des éléments suivants :

Une mise à jour de l'application StopCovid a été faite et l'application a été renommée TousAntiCovid à partir de la version v2.0.

iOS ne permettant pas à l'application StopCovid/TousAntiCovid de garantir une connexion à un serveur au second plan dans certains cas, un système de « push server » a été mis en place au mois d'août afin que le téléphone fasse au moins un « status » chaque jour. Ce « push serveur » consiste en un appel à l'« Apple Push Notification Server (APNS) » lui transmettant l'identifiant « Pushtoken » pour permettre à l'APNS de notifier le terminal correspondant, une fois par jour.

Demandons copie du code Swift de l'application iOS permettant de constater le nombre d'occurrence d'appels à cet identifiant (voir pièces) ainsi que de la documentation d'Apple relative à l'utilisation de cet identifiant « Pushtoken » ainsi que le contenu de la notification en clair.

Une fonctionnalité d'information a été ajoutée permettant la consultation des chiffres clés et des dernières actualités concernant la situation sanitaire au niveau national.

En ce qui concerne la liste noire limitant l'utilisation de l'application

La délégation est informée des éléments suivants :

Une liste des terminaux ne pouvant pas installer l'application est mise en place. Cette liste est dressée à partir des informations transmises par le Play Store sur une partie du parc Android indiquant les téléphones qui ne sont pas supportés (marque, modèle, chipset). La liste des terminaux physiques ne pouvant pas installer l'application, indépendamment des versions du système d'exploitation, a été établie suite aux tests [redacted] Cette liste comporte cinq téléphones Samsung et un téléphone Sony.

Demandons copie de la liste des terminaux exclus.

Par ailleurs, un deuxième filtre permettant de vérifier au sein de l'application si BLE est mis en place. Si le scan et la diffusion (broadcast) renvoient une erreur, l'application ne fonctionne pas. L'information de non-fonctionnement du BLE ne remonte pas sur les différents serveurs. Dans ce cas, l'utilisateur est informé que la fonctionnalité de contact tracing ne fonctionne pas.

Demandons copie d'une capture d'écran présentant l'information transmise à l'utilisateur.

Au niveau logiciel, les versions minimums sur lesquelles les applications TousAntiCovid peuvent être exécutées sont Android 5.0 (et supérieures) et la dernière version d'iOS 11 (et supérieures).

Compte tenu des nouvelles fonctionnalités de l'application (chiffres et actualités sanitaires, attestation de déplacement dérogatoire), l'application Android est ouverte progressivement aux utilisateurs n'ayant pas un smartphone supportant le BLE afin que les utilisateurs puissent bénéficier des nouvelles fonctionnalités autres que le contact tracing.

En ce qui concerne la possibilité de générer une attestation dérogatoire de déplacement directement dans l'application

La délégation est informée des éléments suivants :

Sur la version de TousAntiCovid sortie le 22 octobre (2.0) la fonctionnalité de génération d'attestation consiste en un lien hypertexte intégré sur la page d'accueil, lequel redirige vers le site du Ministère de l'Intérieur permettant de visualiser son attestation et de la télécharger au format pdf.

Suite aux retours des utilisateurs n'arrivant pas à retrouver l'attestation, il a été décidé de remplacer la solution du lien vers le site du Ministère de l'Intérieur par une attestation entièrement intégrée à TousAntiCovid.

Sur la version de TousAntiCovid sortie le 3 novembre (2.1), la fonctionnalité de génération d'attestation consiste en la possibilité pour l'utilisateur de remplir son formulaire d'attestation directement dans TousAntiCovid. Ces données sont prénom, nom, date de naissance, lieu de naissance, adresse, date et heure de sortie, motif de sortie. Ces attestations sont stockées localement dans le téléphone et présentées au format texte, encodées dans un QR code.

Sommes informés qu'il n'existe pas de lien entre le QR code et un identifiant unique spécifique au protocole ROBERT.

Les attestations sont conservées localement, sur le terminal de l'utilisateur, pour une durée définie à 24h, sauf à ce que l'utilisateur supprime manuellement son attestation. A chaque lancement de l'application par l'utilisateur, l'application vérifie que les attestations existantes ne sont pas générées depuis plus de 24h. Elle supprime automatiquement toutes les attestations de plus de 24h (en se basant sur la date et l'heure de génération de l'attestation (timestamp)).

Demandons l'extrait de code de génération d'attestation ainsi que le code responsable des suppressions (automatiques) des données à ouverture de l'application, ainsi que de la suppression manuelle.

Demandons les captures d'écran ou la vidéo du parcours utilisateur lors de la création puis suppression manuelle d'une attestation.

[redacted]nous informe qu'il a été décidé de faire apparaître en clair, sous le QR code, une partie du texte encodé dans le QR code ; que cette modification a de fait corrigé la problématique évoquée dans la presse de scans impossibles des QR codes par l'application QRDNUM, développée par la division numérique du Ministère de l'Intérieur et utilisée par les forces de l'ordre.

[redacted]nous informe que ces deux faits sont décorrélés, que ce bug était dû à l'ajout involontaire d'un « s » dans le texte de l'attestation.

Concernant les données stockées pour la génération ultérieure d'attestations :

La délégation est informée des éléments suivants :

Les prénom, nom, date de naissance, lieu de naissance, adresse peuvent être conservés localement pour la génération d'attestations ultérieures. Ces données sont stockées dans les espaces de stockages chiffrés proposés par les systèmes d'exploitation iOS et Android.

[redacted] nous informe que le moyen le plus simple de démontrer que ces dernières informations ne sont pas remontées au serveur consiste en la vérification de la génération des requêtes dans le code des applications, avant qu'ils ne soient transmis aux serveurs ROBERT.

Cela concerne 5 services : « register », « unregister », « report », « deleteExposureHistory », « status ».

Constatons la construction des requêtes pour les services « register », « report », « deleteExposureHistory », et « status » de l'application iOS (voir pièces).

En ce qui concerne la fonctionnalité en projet de filtrer les chiffres relatifs à la situation sanitaire en fonction d'un code postal :

La délégation est informée des éléments suivants :

Cette fonctionnalité, aujourd'hui réservée à la version bêta de l'application (non disponible sur les stores), consiste en la possibilité de filtrer les chiffres clés en fonction d'un département au choix de l'utilisateur (lieu d'intérêt).

Dans tous les cas, le contenu des chiffres clés de chaque département sera téléchargé, en plus des chiffres clés nationaux. Il s'agit d'un filtre de visualisation et non d'un filtre de téléchargement, ce qui permet de ne pas transmettre le code postal à un serveur.

Sommes informés que le renseignement de ce code postal sera facultatif pour l'utilisateur et qu'en l'absence de code postal renseigné, l'utilisateur verra les chiffres nationaux.

Demandons transmission de l'extrait de code relatif à cette fonctionnalité, une fois qu'elle sera déployée.

Avons demandé communication des documents nécessaires à l'accomplissement de notre mission et en avons pris des copies figurant dans l'inventaire joint en annexe du présent procès-verbal ;

Par ailleurs, demandons communication, de manière sécurisée, dans un délai de **8 jours ouvrés**, de la copie des pièces suivantes nécessaires à l'accomplissement de notre mission :

- l'extrait de code responsable de l'exécution du CAPTCHA (frontend et backend) ainsi que l'URL correspondante sur le Gitlab d'INRIA.

- une capture d'écran actualisée, telle que celle transmise précédemment et démontrant l'arrêt du webservice lié au [redacted]

À l'issue du contrôle, [redacted] responsable des lieux, a fait les observations suivantes :

Pas d'observation.

La mission de contrôle s'est terminée, ce jour, à 22h15;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé par nous et [redacted] responsable des lieux.

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

Paraphes [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

ANNEXE 1 :

INVENTAIRE DES PIÈCES RECUEILLIES

Les copies, notamment informatiques, effectuées par la délégation de la CNIL font l'objet de mesures de protection particulières destinées à assurer leur confidentialité.

Les copies informatiques font l'objet d'un calcul d'empreinte numérique garantissant leur intégrité et leur authenticité.

Ces empreintes numériques sont calculées par l'intermédiaire de l'algorithme SHA256.

Le responsable des lieux a été mis en mesure de consulter les pièces copiées.

[redacted]

 [redacted]

[redacted]

Paraphes [redacted]

[redacted]

Paraphes [redacted]

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

Paraphes [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

PROCÈS-VERBAL DE CONTRÔLE SUR PLACE

En application des dispositions prévues par les articles 55 à 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les articles 10, 19 et 25 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, L. 251-1 et suivants du code de la sécurité intérieure, et des articles 16 à 37 du décret n°2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 précitée ;

Conformément à la décision de la présidente de la CNIL n°2020-270C en date du 22 octobre 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité de tout traitement accessible à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, ou portant sur des données à caractère personnel collectées à partir de cette application aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n°78-17 du 6 janvier 1978 modifiée ;

Nous soussignés [redacted] agents de la CNIL, dûment habilités à procéder à des missions de vérification sur place ;

Le présent procès-verbal ainsi que les pièces annexées et celles pouvant être transmises ultérieurement sont susceptibles d'être communiquées à d'autres autorités de contrôle en application du chapitre VII section 2 du règlement (UE) 2016/679 susvisé ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 13 novembre 2020, à 9h, dans les locaux de INRIA, situés 2 rue Simone Iff à PARIS (75012) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité [redacted], a reçu et pris connaissance, au début du contrôle, de l'objet des vérifications, de l'identité et de la qualité des personnes chargées du contrôle, ainsi que des dispositions prévues à l'article 19 de la loi précitée ; le responsable des lieux a été informé au début du contrôle de son droit d'opposition et ne l'a pas exercé ;

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne le décret du 29 mai 2020 relatif au traitement de données dénommé « StopCovid » :

La délégation est informée des éléments suivants :

Une évolution du décret n°2020-650 du 29 mai 2020 est prévue afin que les nouvelles fonctionnalités de l'application y soient mentionnées :

- le fait que les utilisateurs puissent indiquer qu'ils sont « cas contact » (au sens de l'application), pour bénéficier d'une priorisation dans l'exécution d'un test, comme c'est actuellement le cas pour les personnes identifiées par la CPAM comme « cas contact » ;
- la génération des attestations de déplacement dérogatoires directement au sein de l'application TousAntiCovid, comprenant la collecte des informations nécessaires à la génération des attestations, y compris les dates et heures de sortie, dont les données pouvant être mémorisées localement dans le téléphone (nom, prénom, adresse, date de naissance, lieu de naissance) ;
- l'affichage des informations sanitaires ;
- la collecte d'un code postal (en local) en tant que lieu d'intérêt ;
- la date des derniers contacts avec les dernières personnes identifiées comme positives à la COVID-19, afin d'affiner l'échéance à laquelle l'utilisateur doit faire un test ;
- la prolongation jusqu'au 1er avril 2021 du traitement des données en lien avec l'application.

L'évolution du décret s'accompagne d'une évolution des mentions portées dans l'AIPD (voir pièces annexées au présent procès-verbal).

Le Ministère prévoit de saisir la CNIL de cette évolution du décret et de l'AIPD dans les prochains jours. [redacted] nous informe que cette saisine n'est pas encore intervenue, en raison de la volonté du Ministère de regrouper les modifications intervenues ou à venir des traitements mis en œuvre dans le cadre de l'application TousAntiCovid au sein d'une même notification et ainsi éviter de nombreux aller-retours entre le Ministère, la CNIL et le Conseil d'Etat.

En ce qui concerne l'analyse de l'efficacité de l'application TousAntiCovid dans la lutte contre l'épidémie de COVID-19 :

La délégation est informée des éléments suivants :

Plusieurs études ont été engagées, certaines déjà rendues, portant sur l'efficacité de l'application dans le cadre de la lutte contre l'épidémie de COVID-19.

Une de ces études a été établie par l'INSERM, de sa propre initiative, en lien avec l'Institut Pasteur.

Demandons copie du lien permettant d'accéder publiquement aux conclusions de cette étude de l'INSERM.

D'autres études ont été commandées par le Ministère, notamment une étude qualitative réalisée par KANTAR.

Une actualisation des études est prévue, compte tenu du nombre croissant d'utilisateurs de l'application.

Une étude de terrain est prévue, relative au fonctionnement de l'application.

Un autre moyen de mesurer l'efficacité de l'application dans la lutte contre le virus serait opéré à travers une évolution (un « champ joker ») des informations du traitement SI-DEP, qui permettrait de savoir comment la personne a eu connaissance de son statut à risque.

En ce qui concerne la définition de « cas contact » dans l'application :

La délégation est informée des éléments suivants :

L'arrêté du 30 mai 2020, définissant les critères de distance et de durée de contact au regard du risque de contamination par le virus COVID-19 pour le fonctionnement du traitement de données en lien avec l'application va être modifié. Ces modifications sont en cours d'adoption au sein du Ministère ; le projet d'arrêté modificatif a été transmis au Ministre hier, le 12 novembre 2020.

Ces modifications visent à porter les critères de distance et de durée du contact mentionnés dans l'article 2 du décret du 29 mai 2020 à :

- 1 mètre pendant au moins 5 minutes
  - **ou**
- **2 mètres pendant au moins 15 minutes**

Ces nouveaux critères de distance et de durée ont été définis sur la base d'une recommandation de Santé Public France démontrant la proximité suffisante pour une contamination dans deux situations à risques :

- les lieux clos où le port du masque n'est pas constant (bars et restaurants), où 5 minutes à 1 mètre de distance suffisent à une contamination ;
- les lieux clos (transports en commun ou lieux dont l'aération est insuffisante), où 2 mètres pendant au moins 15 minutes suffisent à une contamination malgré le port du masque.

En ce qui concerne l'interconnexion de l'application avec les autres applications européennes de contact tracing :

La délégation est informée des éléments suivants :

Aucune évolution n'est prévue sur le protocole ROBERT.

Il n'est pas prévu, aujourd'hui, de mettre en œuvre le protocole DESIRE, dont l'intérêt principal est de permettre une interaction entre plusieurs applications de *contact tracing* au sein des pays européens, dans la mesure où la plupart des pays européens disposent déjà de leurs applications de *contact tracing*, dans lesquelles ils ont déjà investi des ressources de développement importantes. Il n'apparait donc pas pertinent de mettre en œuvre ce protocole, en l'absence de manifestation d'intérêt de la part des autres Etats européens.

Par ailleurs, il n'est pas prévu d'utiliser l'API « Google Apple Exposure Notification » (GAEN) au sein de l'application TousAntiCovid.

En ce qui concerne la problématique dite du « Petit Poucet » (décrite par des chercheurs de l'Ecole Polytechnique Fédérale de Lausanne) :

Mentionnons que cette problématique consiste en la désynchronisation des renouvellements des adresses MAC diffusées par bluetooth et des EBID, pouvant permettre d'identifier que plusieurs paquets avec des EBID différents proviennent d'un même appareil.

La délégation est informée des éléments suivants :

Le changement des adresses mac est imposée par iOS et Android. Ce risque est connu mais n'a pas été mise en évidence par INRIA et la communauté ayant examiné TousAntiCovid.

[redacted] nous informe que les chercheurs de l'EPFL visaient dans leur papier l'API « Google Apple Exposure Notification ».

En ce qui concerne la transmission des requêtes « status » :

La délégation est informée des éléments suivants :

[redacted] nous informe qu'il est nécessaire pour assurer l'effectivité de l'application que celle-ci effectue une requête « status » idéalement une fois par jour au serveur ROBERT.

Pour ce faire, l'application doit techniquement être en mesure d'exécuter cette requête. Sur iOS comme sur Android, lorsque l'application est en tâche de fond, il n'est pas certain qu'elle ait les ressources matérielles (CPU) pour exécuter cette requête.

Puisqu'il est nécessaire que cette requête puisse être exécutée une fois toutes les 24h, les modalités suivantes sont mises en œuvre :

- Sur iOS comme sur Android, pour augmenter les chances qu'au moins une requête « status » puisse être exécutée sur 24h, l'application tente d'exécuter cette requête au plus toutes les 6h.
- Sur iOS, il est fréquent que malgré le paramétrage précité, l'application ne soit pas en mesure d'exécuter cette requête. Pour cette raison, une fois par jour, une notification push est envoyée au téléphone iOS. La réception de cette notification permet à l'application TousAntiCovid de bénéficier de ressources matérielles (CPU) à sa

disposition quelques secondes ; temps suffisant pour permettre l'exécution d'une requête « status ».

Constatons que pour l'envoi de la notification push, le fuseau horaire (*timezone*) ainsi que la langue d'affichage du téléphone (*locale)* sont transférés au serveurs backend (SI TousAntiCovid), lequel interagit ensuite avec les serveurs d'Apple (serveur APNS) pour l'envoi de la notification, sans transmission du fuseau horaire (*timezone*) ni de la langue d'affichage du téléphone (*locale)*.

En ce qui concerne le « réveil » des applications TousAntiCovid sur iOS par les applications TousAntiCovid sur Android :

Mentionnons, pour rappel, que cette fonctionnalité est décrite dans la précédente procédure de contrôle du traitement mis en œuvre dans le cadre de l'application (n°2020-097C).

La délégation est informée des éléments suivants :

[redacted]nous informe que cette fonctionnalité est toujours d'actualité et qu'elle n'est pas en lien avec la fonctionnalité « push APNS » sur les applications iOS mentionnée hier dans le procès-verbal n°2020-170-2, qui consiste à la transmission d'une notification push, de manière à autoriser une exécution applicative, utilisée pour la transmission d'une requête « status ».

En ce qui concerne la problématique d'impossibilité d'exécuter un scan BLE sur certains terminaux, pour lesquels le GPS n'est pas actif :

La délégation est informée des éléments suivants :

INRIA et ORANGE ont connaissance de cette défaillance d'Android et sont en train d'examiner quels terminaux sont concernés et les moyens qui pourraient permettre de le résoudre.

A ce jour, l'utilisateur d'un terminal concerné par cette problématique n'est pas informé de ce que la fonctionnalité de *contact tracing* est inopérante.

[redacted]nous informe que cette problématique d'impossibilité d'exécuter un scan BLE sur certains terminaux, pour lesquels le GPS n'est pas actif (nonobstant l'autorisation donnée par l'utilisateur que l'application puisse accéder aux services de position (*location services*)) doit être distinguée de la problématique de l'impossibilité matérielle pour un terminal donné d'utiliser le protocole BLE (mentionnée hier dans le procès-verbal n°2020-170-2).

Mentionnons que l'une et l'autre de ces problématiques sont elles-mêmes distinctes de la question vue dans le contrôle des traitements de l'application StopCovid (procédure n°2020-097C) relative à la nécessité sur Android d'accorder la permission d'accès aux services de position pour pouvoir fonctionner.

INRIA rappelle qu'en aucun cas TousAntiCovid n'utilise les données de géolocalisation (GPS).

En ce qui concerne la liste des terminaux exclus :

La délégation est informée des éléments suivants :

La liste d'exclusion a été téléversée sur le compte développeur du PlayStore de l'application TousAntiCovid.

Cette liste, n'aura plus d'intérêt quand la possibilité de télécharger l'application sera offerte aux téléphones de cette liste, pour bénéficier des fonctionnalités autres que le *contact tracing*.

Si le téléphone n'est pas exclu à partir de la liste mais que le BLE ne fonctionne pas, constatons que l'utilisateur est informé que « le téléphone est incompatible » (voir pièces).

[redacted] nous informe que le nombre de terminaux ne pouvant bénéficier de l'application n'est pas connu, que les téléphones affichant le message d'erreur précité ne figurent pas dans la liste d'exclusion. A l'inverse, il est possible qu'un utilisateur qui aurait installé l'application Android, depuis l'APK et pas depuis le Play Store, voit ce message d'erreur, alors qu'il utilise l'un des terminaux figurant sur la liste d'exclusion.

[redacted] nous indique qu'à sa connaissance il y aurait 20% du parc Android concerné.

Par ailleurs, demandons communication, de manière sécurisée, dans un délai de **8 jours ouvrés**, de la copie des pièces suivantes nécessaires à l'accomplissement de notre mission :

- la liste exhaustive des exclusions, comprenant les critères d'exclusion

À l'issue du contrôle, [redacted] responsable des lieux, a fait les observations suivantes :

Pas d'observation

La mission de contrôle s'est terminée, ce jour, à 19h30 ;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé par nous et [redacted] responsable des lieux.

 Paraphes [redacted]

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

ANNEXE 1 :

INVENTAIRE DES PIÈCES RECUEILLIES

Les copies, notamment informatiques, effectuées par la délégation de la CNIL font l'objet de mesures de protection particulières destinées à assurer leur confidentialité.

Les copies informatiques font l'objet d'un calcul d'empreinte numérique garantissant leur intégrité et leur authenticité.

Ces empreintes numériques sont calculées par l'intermédiaire de l'algorithme SHA256.

Le responsable des lieux a été mis en mesure de consulter les pièces copiées.

[redacted]

Paraphes [redacted]

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

PROCÈS-VERBAL DE CONTRÔLE SUR PLACE

En application des dispositions prévues par les articles 55 à 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les articles 10, 19 et 25 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, L. 251-1 et suivants du code de la sécurité intérieure, et des articles 16 à 37 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 précitée ;

Conformément aux décisions de la présidente de la **CNIL n° 2020-270C en date du 22 octobre 2020** et **n° 2021-141C en date du 29 juin 2021**, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité de tout traitement accessible à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, ou portant sur des données à caractère personnel collectées à partir de cette application ainsi qu'à la vérification de la conformité de l'ensemble des traitements de données à caractère personnel mis en œuvre dans le cadre du Passe Sanitaire prévu par le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire ainsi que dans le cadre des protocoles sanitaires pour les bars, les restaurants et restaurants d'hôtel et de reprise des activités physiques et sportives (dont, notamment, les traitements en lien avec les cahiers de rappel numérique et papier) aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n° 78-17 du 6 janvier 1978 modifiée ;

Nous soussignés, [redacted] agents de la CNIL, dûment habilités à procéder à des missions de vérification sur place ;

Le présent procès-verbal ainsi que les pièces annexées et celles pouvant être transmises ultérieurement sont susceptibles d'être communiquées à d'autres autorités de contrôle en application du chapitre VII section 2 du règlement (UE) 2016/679 susvisé ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 6 juillet 2021, à 9 heures, dans les locaux d'INRIA, situés 2 rue Simone Iff à PARIS (75012) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité [redacted] a reçu et pris connaissance, au début du contrôle, de l'objet des vérifications, de l'identité et de la qualité des personnes chargées du contrôle, ainsi que des dispositions prévues à l'article 19 de la loi précitée ; le responsable des lieux a été informé au début du contrôle de son droit d'opposition et ne l'a pas exercé ;

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne les évolutions apportées à l'application « TousAntiCovid » (ci-après « TousAntiCovid » ou « TAC »)

Mentionnons que [redacted] effectue une présentation des faits marquants et évolutions de l'application TousAntiCovid intervenus depuis les contrôles de la CNIL du mois de novembre 2020.

Prenons copie de la présentation des faits marquants et évolutions de l'application TousAntiCovid intervenus depuis les contrôles de la CNIL du mois de novembre 2020.

[redacted] *nous informe des éléments suivants :*

Depuis les contrôles de la CNIL du mois de novembre 2020 :

- l'infogérance et la tierce maintenance applicative du *backend* ont été repris par les équipes [redacted] (en remplacement des équipes [redacted] depuis le mois de mars 2021) ;
- une ressource [redacted] dédiée au pilotage du projet et à l'appui de la maîtrise d'ouvrage est arrivée en mars 2021 ;
- les fonctionnalités de TAC CARNET (2D-DOC) ont été déployées le 19 avril 2021 ;
- la fonctionnalité TAC SIGNAL a été déployée le 25 mai 2021 ;
- un service qui permet de remonter des statistiques anonymes sur le serveur central a été déployé dans le courant du mois de mai 2021 ;
- les certificats européens (DCC) ont été déployés le 23 juin 2021 dans TAC CARNET et le module de conversion le 1er juillet 2021.

Suite au déploiement des nouvelles fonctionnalités dans l'application TousAntiCovid, l'analyse d'impact sur la protection des données (AIPD) relative à l'application a été mise à jour. Une nouvelle AIPD dédiée à la fonctionnalité SIGNAL a été mise en œuvre. Une nouvelle AIPD dédiée aux traitements mis en œuvre dans le cadre du Passe Sanitaire (prévu par le décret

n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire) a également été mise en œuvre.

Prenons copie de l'AIPD TousAntiCovid mise à jour.

Prenons copie de l'AIPD TousAntiCovid SIGNAL.

Prenons copie de l'AIPD PASSE SANITAIRE.

Aucune des évolutions mises en œuvre depuis le mois d'avril 2021 (TAC SIGNAL et TAC CARNET notamment) ne nécessite la mise à jour du décret n° 2020-650 du 29 mai 2020.

En ce qui concerne les destinataires des données issues de l'application TousAntiCovid et la sous-traitance

[redacted] *nous informe des éléments suivants :*

Au jour du contrôle, les principaux sous-traitants du ministère des solidarités et de la santé sont :

- [redacted]INRIA (coordination et pilotage du projet notamment) ;
- [redacted] (appui pilotage) ;
- [redacted] (développement et exploitation de l'application mobile) ;
- [redacted] (prestation anti-DDOS) ;
- [redacted] (exploitation du *backend*) ;
- [redacted] (hébergement notamment) ;
- [redacted] (mise à disposition d'un *bucket* pour les QR codes de lieux) ;
- [redacted] (développement et infogérance du *backend* de conversion des certificats au format 2D DOC) ;
- [redacted] (gestion de la hotline et des courriers électroniques envoyés par les utilisateurs de l'application TAC) ;
- [redacted] (prestation anti-DDOS).

Depuis les contrôles effectués en novembre 2020, les sous-traitants [redacted] participent désormais à la mise en œuvre du traitement TousAntiCovid.

Au jour du contrôle, la société [redacted] traite des données pour le compte du ministère des solidarités et de la santé dans le cadre de sa prestation anti-DDOS et pare-feu. L'étude de faisabilité technique du remplacement de cette solution par [redacted] est en cours d'analyse.

Prenons copie de l'ensemble des contrats passés avec les nouveaux sous-traitants.

[redacted] nous informe qu'il ignore si ces sous-traitants ont recours à de la sous-traitance ultérieure. L'ensemble des contrats passés prévoient une mention précisant que les éventuels sous-traitants ultérieurs sous soumis aux mêmes obligations en matière de protection de données que celles fixées dans le contrat initial.

L'ensemble des nouveaux sous-traitants ont été mentionnés dans les AIPD mises à jour au titre des destinataires de données. Les utilisateurs de l'application TousAntiCovid ne sont pas informés de l'ensemble de ces sous-traitants au titre des destinataires des données.

En ce qui concerne l'analyse de l'efficacité de l'application TousAntiCovid dans la lutte contre l'épidémie de Covid-19

[redacted] *nous informent des éléments suivants :*

Le ministère des solidarités et de la santé n'a pas produit de rapport d'analyse de l'efficacité de l'application TousAntiCovid dans la lutte contre l'épidémie de Covid-19.

Le comité de contrôle et de liaison Covid-19, chargé notamment « *d'évaluer l'apport réel des outils numériques à leur action, et de déterminer s'ils sont, ou pas, de nature à faire une différence significative dans le traitement de l'épidémie* », a publié plusieurs avis sur les outils utilisés dans le cadre de la lutte contre l'épidémie de Covid-19, et notamment l'outil de traçage numérique TousAntiCovid.

Prenons copie du dernier avis rendu le 3 mai 2021 par le comité de contrôle et de liaison Covid-19 en lien avec l'évaluation de l'efficacité de l'application TousAntiCovid dans la lutte contre l'épidémie de Covid-19.

En ce qui concerne les statistiques d'utilisation de l'application TousAntiCovid

[redacted] *nous informent des éléments suivants :*

Au jour du contrôle, 21 696 000 personnes ont téléchargé et activé l'application TousAntiCovid, 206 000 ont été notifiées d'un risque d'exposition au Covid-19 et 324 000 se sont déclarées positives. La notion d'« activation de l'application » recouvre le fait de réaliser une action émettrice d'une requête vers le *backend* de l'application. Cela n'inclut donc pas par exemple la seule utilisation du générateur d'attestation ou la consultation des statistiques. Au contraire, l'activation de la fonction de traçage ou encore le scan d'un QR code « SI-DEP » constituent des exemples d'actions émettrices d'une requête vers le *backend*.

Des données d'analyse sont générées pour évaluer l'utilisation qui est faite de l'application. Une partie des actions sur l'application entraîne l'émission d'une donnée d'analyse. Cela comprend notamment la consultation de pages sur l'application, le flash de QR codes ou la réception d'alertes.

Ces données comprennent également des informations sur la version de l'application utilisée, le nombre de QR codes de lieu scannés, les événements réalisés et les codes d'erreur remontés en cas d'échec d'un web service.

Ces données d'analyse font également remonter des événements de type « sanitaire », et notamment :

- lorsqu'un utilisateur se déclare positif au Covid-19 ;
- lorsqu'un utilisateur reçoit une alerte par son application relative à un risque d'exposition au Covid-19 (au sens « ROBERT » ou « SIGNAL » du terme).

Prenons copie une documentation des données d'analyse et un extrait des journaux associés.

À terme, ces outils d'analyse seront améliorés et utilisés pour mieux évaluer l'efficacité de l'application. Au jour du contrôle, l'analyse des données d'usage révèle que les deux fonctionnalités les plus utilisées sont la consultation des statistiques liées à l'évolution de la situation sanitaire et la génération d'attestations dérogatoires de sortie.

En ce qui concerne la nouvelle fonctionnalité dénommée « TousAntiCovid SIGNAL »

Mentionnons que la Commission a rendu un avis dans une première délibération n° 2020-135 du 17 décembre 2020 concernant le dispositif numérique d'enregistrement de visites de certains lieux recevant du public, faisant intervenir des codes QR générés par les établissements concernés et reposant sur le protocole initial TAC-WARNING. Ce dispositif a pour objectif de prévenir les utilisateurs de TAC, qui auront scanné le code QR d'un établissement, qu'ils ont été présents dans un même lieu et sur une même plage horaire qu'une ou plusieurs personnes ultérieurement diagnostiquées ou dépistées positives au Covid-19. Une demande de conseil a également été reçue par les services de la CNIL en avril 2021 concernant le nouveau protocole CLEA, visant à remplacer le protocole « TAC-WARNING » pour la fonctionnalité « TousAntiCovid-Signal ». Le protocole « TAC-WARNING » n'est plus utilisé à ce jour.

La délégation est informée des éléments suivants :

Les gérants de lieux mettent à disposition des visiteurs de leur établissement un QR code statique ou dynamique. Les personnes peuvent ainsi le scanner, et quand une personne se déclare positive au Covid-19 sur l'application, la liste des identifiants des établissements qu'elle a visitée est remontée à un serveur central dédié au service « CLEA ». La liste des identifiants des lieux ainsi considérés à risque est ensuite publiée et récupérée par les applications. Les personnes ayant fréquenté des lieux identifiés à risque sont ensuite notifiées par leur application.

La corrélation entre les lieux visités par la personne et les lieux à risque est effectuée localement, sur son téléphone.

Le seuil de risque dépend de la nature du lieu et le contenu des notifications envoyées aux personnes est fixé en conséquence.

Demandons copie des différents messages de notification envoyés aux personnes potentiellement contaminées.

Demandons la liste exhaustive des critères permettant la définition des différents seuils de risque.

Les identifiants des lieux à risque remontés dans le serveur « CLEA » suite à une déclaration de contamination au Covid-19 par une personne sont conservés pendant 14 jours à compter de la déclaration. Les identifiants des lieux visités enregistrés en local dans le téléphone sont conservés pendant 14 jours à compter du scan du QR code du lieu.

À notre demande, [redacted] affiche les fichiers contenant les informations relatives aux lieux à risque. Ces fichiers sont librement accessibles sur le web, à partir d'une URL. Un fichier sert d'index pour les identifiants de lieu, ces derniers étant ensuite déclinés dans des fichiers individuels.

Prenons copie d'un exemple de fichier de remontée de lieux à risque.

Prenons copie de la fréquence de génération des fichiers d'index relatifs aux lieux à risque.

Pour chaque lieu à risque apparaissant dans ces fichiers, leur identifiant est affiché avec l'information relative au début de la plage horaire ainsi que la durée pendant laquelle les visiteurs de l'établissement ont été exposés à un risque de contamination. La durée de cette plage horaire est directement liée à la nature de l'établissement.

À notre demande, [redacted] accède à l'URL « https://qrcode.tousanticovid.gouv.fr » et génère un QR code de lieu.

Un QR code de lieu contient un identifiant unique propre au lieu non chiffré et des informations chiffrées indiquant la nature du lieu, la durée de la plage horaire associée et la période de validité du QR code. La clef privée de déchiffrement est connue uniquement du serveur central. Les secrets sont stockés grâce à deux bibliothèques logicielles « Consul » et « Vault » qui permettent de stocker des secrets chiffrés.

Prenons copie de la version du composant logiciel « Vault ».

Demandons copie de la version du composant logiciel « Consul ».

Demandons copie de la documentation associée aux composants logiciels « Vault » et « Consul ».

Les QR codes sont générés en local dans le navigateur, avec une bibliothèque Javascript. Il n'est ainsi pas possible d'avoir des indicateurs sur le nombre de QR codes générés.

Constatons que l'outil de génération des QR codes est librement accessible sur le web et qu'à ce titre n'importe qui est en mesure de générer un QR code, par exemple pour un événement privé.

Prenons copie du fichier au format PDF généré contenant les QR codes à afficher.

Demandons copie de la spécification relative au protocole CLEA.

Il est possible d'utiliser des QR codes dynamiques, qui changent régulièrement. Ces QR codes dynamiques ne sont cependant pas encore effectivement opérationnels et nécessiteront le déploiement d'appareils spéciaux ou d'une application pour leur affichage et leur renouvellement régulier.

La particularité de ces QR codes est que leur validité est temporaire, contrairement aux QR codes statiques qui restent indéfiniment valables. Ainsi, si une personne scanne un QR code dynamique après sa période de validité, il sera refusé par l'application et ne sera pas ajouté dans le journal de rappel.

Les seules versions de TLS autorisées pour chiffrer les communications entre l'application et le serveur central « CLEA » sont celles supérieures ou égales à 1.2.

Des unités de stockage hébergées par [redacted] sont en place pour répartir les requêtes entre les différents services applicatifs. Les deux services CLEA et ROBERT sont situés sur des sous-réseaux différents.

L'infrastructure hébergeant le service CLEA est issue de l'offre de cloud privé virtuel [redacted] dénommée « CloudGouv ». Cette offre, également utilisée pour le serveur du service ROBERT, est labélisée « SecNumCloud ».

Il n'y a pas aujourd'hui de lien réalisé entre les cahiers de rappel sur papier et la fonctionnalité « Signal » de l'application TousAntiCovid. Lorsqu'une personne se déclare positive auprès de l'Assurance maladie, les enquêteurs sanitaires peuvent être informés que la personne a visité un certain lieu. L'Assurance maladie peut alors se rapprocher du gérant du lieu pour qu'il fournisse le cahier de rappel sur la plage de temps pertinente.

Prenons copie des communications émises par le MSS à propos des cahiers de rappel sur papier.

Lorsqu'une personne scanne son certificat de test positif « SI-DEP », la remontée des contacts se fait dans le protocole ROBERT. En réponse, un jeton est envoyé sur le téléphone pour permettre la remontée des lieux avec le protocole CLEA. Il n'y a pas d'autre lien entre les protocoles ROBERT et CLEA.

Prenons copie d'un diagramme de flux du protocole ROBERT mis à jour sur ce sujet.

Prenons copie des extraits du code du service ROBERT relatifs aux communications entre ses services et ceux de CLEA.

Il n'y a pas eu d'audit de sécurité réalisé depuis la mise en œuvre des nouvelles fonctionnalités.

En ce qui concerne les constats dans la base de données

Mentionnons utiliser un téléphone « Pixel 3XL » de la marque Google.

Mentionnons que le téléphone utilisé pour le présent contrôle est réinitialisé dans ses paramètres d'usine.

Mentionnons créer un compte Google pour les besoins du contrôle.

Mentionnons mettre à jour le système d'exploitation Android.

Installons l'application « TousAntiCovid » à partir du magasin d'applications « Google Play ».

Scannons avec la fonctionnalité « Signal » de l'application « TousAntiCovid » le QR code de lieu généré plus tôt par INRIA.

À notre demande, [redacted] se connecte à la base de données du service CLEA en tant que l'utilisateur « Clea ». [redacted] Neuf personnes, travaillant dans l'équipe en charge de l'infogérance, ont les droits d'utilisation de ce compte. Il n'existe pas de compte nominatif.

La connexion au bastion permettant l'accès à la base de données se fait également au moyen d'un compte partagé.

[redacted] réalise un export de la base de données du service CLEA. Les tables présentes dans la base de données sont :

- *exposed_visits* : liste des identifiants des lieux et des plages horaires remontés par les personnes déclarées positives au Covid-19 ;
- *cluster_periods* : données agrégées sur les lieux considérés comme à risque ;
- *stat_location* : nombre de visites « à risque » par période et par type de lieu ;
- *stat_reports* : nombre d'identifiants de lieux et de plages horaires remontées par déclaration de contamination au Covid-19.

Constatons qu'initialement, l'identifiant de lieu correspondant à notre QR code scanné n'apparaît pas dans la table « exposed_visits ».

Scannons le QR code correspondant à un certificat de test positif mis à disposition par INRIA.

Constatons l'apparition dans la table « exposed_visits » de notre identifiant de lieu scanné.

À notre demande, [redacted] affiche les lignes les plus anciennes présentes dans la table « exposed_visits ». Constatons que ces lignes datent du 22 avril 2021.

Sommes informés que ces lignes correspondent à des tests réalisés à cette date. Constatons que la deuxième date la plus ancienne est celle du 21 juin 2021.

Prenons copie des captures d'écran.

Demandons copie des extractions réalisées.

Demandons des données statistiques relatives au nombre de remontées d'historiques de lieux visités et au nombre d'établissements identifiés comme étant à risque.

Par ailleurs, demandons communication, de manière sécurisée, dans un délai de **8 jours ouvrés**, de la copie des pièces suivantes nécessaires à l'accomplissement de notre mission :

- les différents messages de notification envoyés aux personnes potentiellement contaminées ;
- la liste exhaustive des critères permettant la définition des différents seuils de risque ;
- la version du composant logiciel « Consul » ;
- la documentation associée aux composants logiciels « Vault » et « Consul » ;
- la spécification relative au protocole CLEA ;
- les extractions réalisées dans la base de données du service CLEA ;
- les données statistiques relatives au nombre de remontées d'historiques de lieux visités et au nombre d'établissements identifiés comme étant à risque.

À l'issue du contrôle, [redacted] responsable des lieux, a fait les observations suivantes :

Pas d'observation

La mission de contrôle s'est terminée, ce jour, à 19h30 ;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé par nous et [redacted] responsable des lieux.

 Paraphes [redacted]

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

Paraphes [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

ANNEXE 1 :

INVENTAIRE DES PIÈCES RECUEILLIES

Les copies, notamment informatiques, effectuées par la délégation de la CNIL font l'objet de mesures de protection particulières destinées à assurer leur confidentialité.

Les copies informatiques font l'objet d'un calcul d'empreinte numérique garantissant leur intégrité et leur authenticité.

Ces empreintes numériques sont calculées par l'intermédiaire de l'algorithme SHA256.

Le responsable des lieux a été mis en mesure de consulter les pièces copiées.

[redacted]

 Paraphes [redacted]

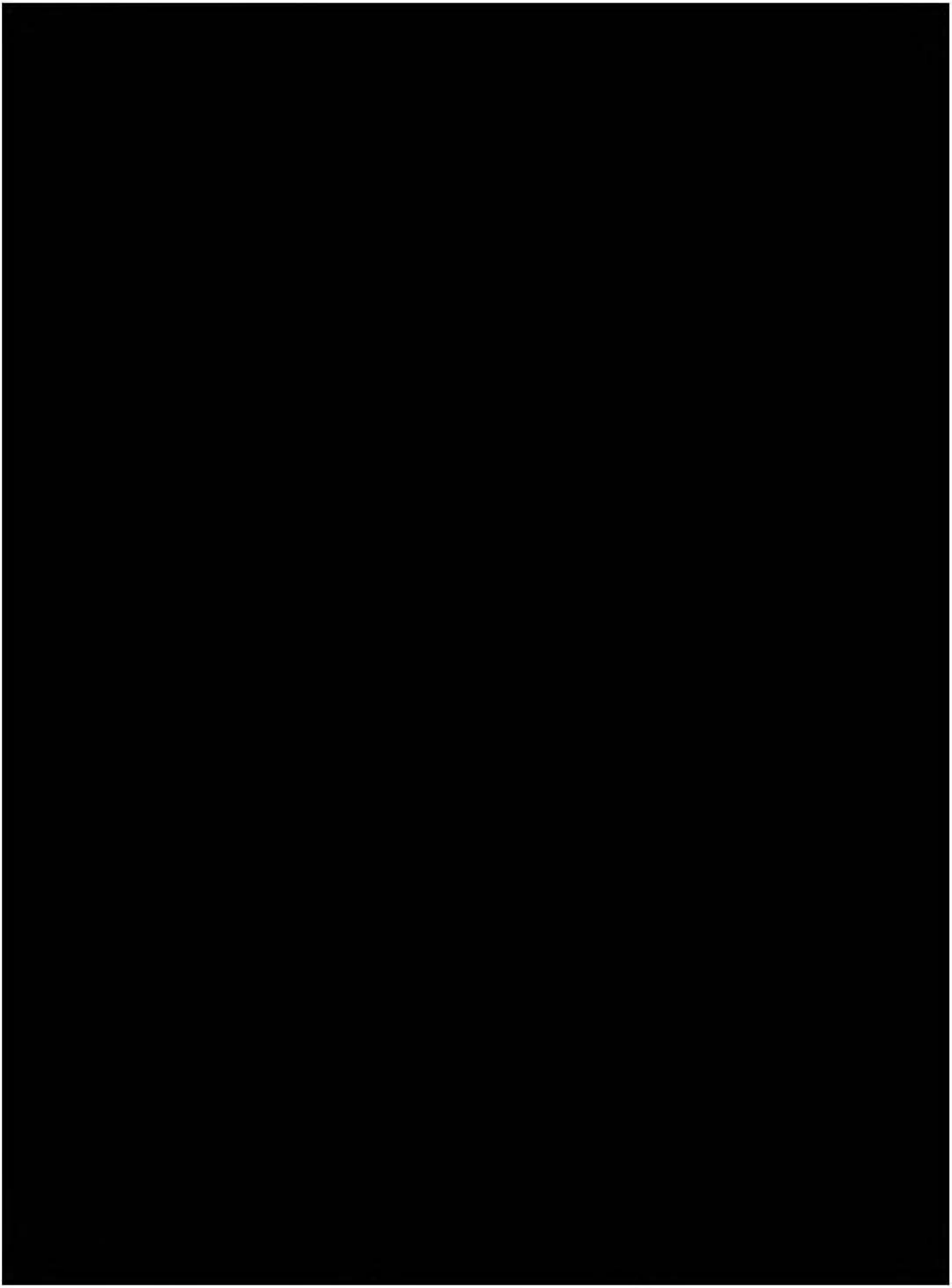
[redacted]

Paraphes

[redacted]

[redacted]

Paraphes [redacted]



Paraphes

Paraphes

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

Paraphes [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

PROCÈS-VERBAL DE CONTRÔLE SUR PLACE

En application des dispositions prévues par les articles 55 à 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les articles 10, 19 et 25 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, L. 251-1 et suivants du code de la sécurité intérieure, et des articles 16 à 37 du décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi du 6 janvier 1978 précitée ;

Conformément aux décisions de la présidente de la **CNIL n° 2020-270C en date du 22 octobre 2020** et **n° 2021-141C en date du 29 juin 2021**, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité de tout traitement accessible à partir de l'application « TousAntiCovid », mise en œuvre par la Direction Générale de la Santé du Ministère des Solidarités et de la Santé, ou portant sur des données à caractère personnel collectées à partir de cette application ainsi qu'à la vérification de la conformité de l'ensemble des traitements de données à caractère personnel mis en œuvre dans le cadre du Passe Sanitaire prévu par le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire ainsi que dans le cadre des protocoles sanitaires pour les bars, les restaurants et restaurants d'hôtel et de reprise des activités physiques et sportives (dont, notamment, les traitements en lien avec les cahiers de rappel numérique et papier) aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n° 78-17 du 6 janvier 1978 modifiée ;

Nous soussignés, [redacted] agents de la CNIL, dûment habilités à procéder à des missions de vérification sur place ;

Le présent procès-verbal ainsi que les pièces annexées et celles pouvant être transmises ultérieurement sont susceptibles d'être communiquées à d'autres autorités de contrôle en application du chapitre VII section 2 du règlement (UE) 2016/679 susvisé ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 7 juillet 2021, à 9 heures, dans les locaux d'INRIA, situés 2 rue Simone Iff à PARIS (75012) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité, [redacted] a reçu et pris connaissance, au début du contrôle, de l'objet des vérifications, de l'identité et de la qualité des personnes chargées du contrôle, ainsi que des dispositions prévues à l'article 19 de la loi précitée ; le responsable des lieux a été informé au début du contrôle de son droit d'opposition et ne l'a pas exercé ;

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne le répartiteur de charge en place auprès du serveur CLEA
La délégation est informée des éléments suivants :

Lorsqu'une personne se déclare positive au Covid-19, l'historique de ses lieux visités est transmis à un répartiteur de charge, lequel exclut l'adresse IP utilisée pour la remplacer par sa propre adresse IP avant de l'adresser à une passerelle [redacted] puis au serveur central du service CLEA. Ainsi ni ce dernier, ni [redacted] n'ont connaissance des adresses IP des téléphones.

Prenons copie d'une capture de flux du répartiteur de charge opéré par [redacted] à destination de la passerelle [redacted]

Sommes informés que les adresses IP reçues par la passerelle sont celles du répartiteur de charge et que les adresses IP reçues par le serveur central CLEA sont celles de la passerelle.

En ce qui concerne la purge des identifiants de lieux dans le serveur CLEA
La délégation est informée des éléments suivants :

[redacted] nous informe avoir opéré une vérification sur les constats opérés la veille (cf. PV n° 2020-270/5) s'agissant des données constatées en date du 22 avril 2021. [redacted] nous informe que ces données étaient bien des données de test, néanmoins elles auraient dû être purgées. Le fait qu'elles ne l'aient pas été est dû au maintien d'un paramètre relatif à la suspension de la purge.

Ces données ont vocation à être purgées au lendemain du contrôle de ce jour.

Prenons copie du fichier de configuration contenant l'information relative à la non-exécution quotidienne du processus de purge sus-décrit.

En ce qui concerne la fonctionnalité dénommée « TousAntiCovid CARNET »

[redacted] effectue une présentation du dispositif de passe sanitaire à partir d'un fichier PowerPoint.

Prenons copie du fichier de présentation des traitements en lien avec le passe sanitaire.

[redacted] *nous informe des éléments suivants :*

Le passe sanitaire, prévu par le décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire, est mis en œuvre afin de limiter le risque de contamination en conditionnant certains déplacements ainsi que l'accès à certains lieux, établissements et évènements à la présentation d'un des trois justificatifs suivants :

- un test de dépistage à la Covid-19 négatif,
- une attestation de vaccination,
- un certificat de rétablissement à la suite d'une contamination antérieure au Covid-19.

Il existe deux types de contrôles du passes sanitaires :

- le passe sanitaire « activités », d'une part, s'agissant de l'accès à des événements de plus de mille personnes ;
- le passe sanitaire « frontière », d'autre part, s'agissant de la circulation au sein des pays membres de l'Union européenne (et, à terme, à l'international).

Le passe sanitaire peut être présenté sous un format numérique ou papier, dans lequel figure un 2D-DOC (désormais DCC depuis le 24 juin 2021 afin de se conformer au format standard européen).

Les contrôles de la validité des passes présentés sont réalisés localement sur le téléphone du contrôleur au moyen de l'application TousAntiCovid-Vérif, développée par [redacted] et disponible dans deux modes :

- TAC VERIF « LITE », dans le cadre du passe sanitaire « activités » et affichant le minimum d'information aux personnes chargées des contrôles (passage autorisé/interdit) ;
- TAC VERIF « OT », dans le cadre du passe sanitaire « frontière », et permettant l'affichage de plus d'informations nécessaires afin de procéder à la validation du passe en fonctions des règles qui peuvent être fluctuantes dans les différents pays d'accueil ;

Par ailleurs, une API est mise à disposition des polices aux frontières exclusivement via le réseau privé interministériel de l'État (RIE) pour permettre à ces dernières d'intégrer la fonctionnalité TAC VERIF à leurs outils.

Les preuves constituant le passe sanitaire (test de dépistage du Covid-19 ou attestation de vaccination) peuvent être stockées au format numérique dans le module « Carnet » de l'application TousAntiCovid.

Le module « Carnet » dans l'application TousAntiCovid permet d'enregistrer les 2D-DOC (maintenant DCC à compter du 24 juin 2021) des justificatifs. Les personnes ayant enregistré

leur justificatif avant le 24 juin (version 2D-DOC) peuvent désormais les convertir au format européen DCC à partir d'une fonctionnalité de convertisseur de certificat, disponible dans l'application TousAntiCovid depuis le 1er juillet.

Un décret relatif au convertisseur de certificat a été publié (décret n° 2021-901 du 6 juillet 2021 relatif au traitement automatisé de données à caractère personnel dénommé « Convertisseur de certificats »).

En ce qui concerne le processus de génération et d'intégration des preuves de test de dépistage dans TousAntiCovid CARNET
La délégation est informée des éléments suivants :

Les preuves de test de dépistage au Covid-19 sont générées par le système d'information SI-DEP. Le 2D-DOC (et désormais le DCC) présent dans le certificat de test est généré par le sous-traitant de l'AP-HP dénommé [redacted]

Lorsqu'une personne se fait dépister au Covid-19 dans une pharmacie ou n'importe quel centre de test, le résultat du dépistage est centralisé dans la base SI-DEP.

SI-DEP transmet alors un SMS (acheminé par [redacted] ou un courrier électronique (en fonction des informations qui ont été transmises par la personne au moment de son test) à la personne dépistée l'informant que le résultat de son test est disponible à partir du portail accessible depuis l'URL « sidep.gouv.fr ».

La personne peut se connecter au portail accessible à partir de l'URL « sidep.gouv.fr » par deux moyens :

- soit la personne peut saisir sa date de naissance (fournie par la personne lors de la réalisation de son test ou, à défaut, collectée à partir des informations contenues dans la carte vitale de la personne qu'elle a présentée lors de son test) ; elle reçoit alors un OTP par SMS, composé de six caractères (chiffres / lettres majuscules) ; l'OTP est généré aléatoirement par SI-DEP depuis [redacted] et est distribué par SMS par le prestataire [redacted]
- soit la personne peut se connecter directement à partir de ses identifiants « FranceConnect ». Pour l'accès à son/ses test(s), l'utilisateur reçoit également un OTP de la même façon que dans l'hypothèse précédente.

Un fois connectée, la personne peut avoir accès au résultat de son test de dépistage. Si la personne est connectée à l'aide de ses identifiants « FranceConnect », elle pourra avoir accès à l'ensemble de ses certificats de tests réalisés au cours des 90 derniers jours.

En cas de test positif, un second SMS est également envoyé à la personne l'informant de la possibilité de déclencher la remontée de ses contacts et identifiants de lieux à partir de l'application TousAntiCovid le cas échéant. Cette remontée automatique s'effectue au moyen d'un lien profond (*deeplink*) contenu dans le SMS. Ce *deeplink* contient un code à usage unique fourni par INRIA à SI-DEP et qui entraine la remontée des contacts et des identifiants de lieux dans l'application TousAntiCovid. Ce processus n'entraine pas l'enregistrement dans TousAntiCovid CARNET du certificat de test positif.

Le certificat de test reçu contient un QR code (contenant un *deeplink*) ainsi qu'un 2D-DOC (ou DCC depuis le 24 juin 2021). Il est alors possible pour un utilisateur de l'application TousAntiCovid de scanner le 2D-DOC (ou DCC) à partir de la fonctionnalité TAC CARNET. Le certificat de test est alors enregistré dans l'application TousAntiCovid. Lorsque l'utilisateur

scanne le QR code à partir d'un outil de lecture de QR codes, il obtient un lien permettant d'ouvrir l'application TousAntiCovid, ce qui lui permet d'enregistrer le certificat dans TAC CARNET. Si l'utilisateur ne possède pas l'application, il est redirigé vers le portail web « bonjour.tousanticovid.gouv.fr », l'invitant à télécharger l'application TousAntiCovid.

Prenons copie des maquettes de communications par courrier électronique et par SMS envoyées aux personnes dans le cadre de la récupération des preuves.

L'enregistrement du certificat de test dans l'application TousAntiCovid n'entraine aucun flux de donnée vers le serveur ROBERT. L'intégralité des données contenues dans le certificat est conservée en local.

À notre demande, un faux certificat de test positif au Covid-19 a été créé pour les besoins du contrôle et généré à partir du serveur de production de SI-DEP (voir pièces). Sommes informés que la date de naissance correspondante est le 1er mai 1968.

Mentionnons utiliser un téléphone de type iPhone 10, propriété du service des contrôles de la CNIL. Constatons la réception de deux SMS :

Cliquons sur le premier lien. Constatons une redirection vers le portail accessible à partir de l'URL « sidep.gouv.fr » :

[redacted]

Saisissons la date de naissance « 01/05/1968 » et constatons la réception d'un code composé de six chiffres et lettres majuscules. Saisissons le code et constatons notre authentification au portail SI-DEP. Constatons l'accès au certificat de test positif.

Mentionnons installer l'application TousAntiCovid et cliquer sur « Activer TousAntiCovid ». Cliquons sur le lien profond présent dans le second SMS reçu. Constatons l'affichage suivant :

 Paraphes [redacted]

Cliquons sur « Valider » et constatons que l'historique de contact a été transmis avec succès (voir pièces).

À notre demande, un faux certificat de test négatif est mis à la disposition de la délégation.

Mentionnons utiliser un téléphone de type PIXEL 3XL, propriété du service des contrôles de la CNIL. Mentionnons ouvrir l'application TousAntiCovid téléchargée lors du contrôle en date du 6 juillet 2021.

À notre demande [redacted] affiche le faux certificat de test négatif. Constatons la présence d'un QR code ainsi que d'un 2D-DOC. Sommes informés que le QR code, lequel contient un *deeplink*, peut être lu par n'importe quel appareil et entraine l'ouverture de l'application TousAntiCovid. Le 2D-DOC peut être de son côté directement lu par l'application TousAntiCovid.

À notre demande, [redacted] affiche l'URL vers laquelle pointe le QR code et constatons l'affichage du *deeplink* (voir pièces).

Mentionnons scanner le 2D-DOC à l'aide de la fonctionnalité « Carnet » de l'application TousAntiCovid.

Constatons que le certificat de test a été ajouté avec succès au carnet de l'application TousAntiCovid.

En ce qui concerne le processus de génération et d'intégration des preuves de vaccination dans TousAntiCovid CARNET
La délégation est informée des éléments suivants :

Après la réception d'une dose de vaccin, le candidat à la vaccination reçoit un certificat de vaccination au format papier édité par la Caisse Nationale d'Assurance Maladie (CNAM), lequel contient un QR code ainsi qu'un 2D-DOC (DCC depuis le 24 juin 2021). Le 2D-DOC (et désormais DCC) est généré en interne par un outil de la CNAM.

Si une personne n'a pas reçu de certificat de vaccination au format papier à l'issue de sa vaccination, celle-ci peut également l'obtenir à partir du portail accessible à partir du site « attestation-vaccin.ameli.fr ». La connexion est alors effectuée à partir de ses identifiants « FranceConnect ».

Dans le cas où une personne n'aurait pas de compte « FranceConnect » ou ne bénéficierait pas d'un accès à internet, celle-ci aurait alors toujours la possibilité de se rapprocher de son centre de vaccination, d'un médecin, d'un pharmacien ou d'une CPAM afin d'obtenir un certificat de vaccination au format papier.

Lorsqu'une personne reçoit son certificat de vaccination, il lui est alors possible de le scanner afin de l'ajouter à la fonctionnalité « Carnet » de son application TousAntiCovid. Sommes informés que le QR code, lequel contient un *deeplink*, peut être lu par n'importe quel appareil et entraine l'ouverture de l'application TousAntiCovid. Le 2D-DOC peut être de son côté directement lu par l'application TousAntiCovid et ajoute automatiquement le certificat dans la fonctionnalité « Carnet ».

À notre demande, un faux certificat de vaccination est mis à la disposition de la délégation.

Mentionnons utiliser un téléphone de type iPhone X, propriété du service des contrôles de la CNIL, pour les besoins du contrôle.

Mentionnons désinstaller l'application TousAntiCovid installée précédemment et la réinstaller.

À notre demande, [redacted] affiche le 2D-DOC du faux certificat de vaccination qui est mis à la disposition de la délégation.

Mentionnons scanner le 2D-DOC affiché à l'aide de la fonctionnalité « Carnet » de l'application TousAntiCovid.

Constatons que le certificat de vaccination a été ajouté avec succès à la fonctionnalité « Carnet » de l'application TousAntiCovid.

En ce qui concerne l'authenticité des preuves
La délégation est informée des éléments suivants :

Des demandes de signature de certificat sont générées par la CNAM, [redacted] et par [redacted] pour le compte de l'AP-HP s'agissant de ce dernier. Ces demandes de signature de certificat ont été signées par l'Agence nationale des titres sécurisés (ANTS), seule autorité possédant la clef de signature CSCA pour la France.

Deux conventions ont été signées, d'une part entre [redacted] et INRIA (sous-traitant de la DGS), et d'autre part entre la DGS, l'ANTS et la Direction des libertés publiques et des affaires juridiques, dépendant du ministère de l'Intérieur, pour permettre la signature des preuves de dépistage négatif ou des attestations de vaccination au format DCC. Les preuves sont aujourd'hui directement générées au format DCC et signées par la CNAM ou l'AP-HP. Les preuves initialement générées au format 2D-DOC peuvent également être converties au format DCC et signées par [redacted]

[redacted] génère et signe les preuves au format DCC dans certains cas, notamment pour le compte du Ministère des Armées et pour les personnes résidant dans les collectivités d'outre-mer.

Demandons la liste des situations dans lesquelles [redacted] génère et signe les preuves au format DCC.

Demandons copie de la convention signée entre la DGS, l'ANTS et la Direction des libertés publiques et des affaires juridiques.

Prenons copie de deux documents formalisant le mécanisme de génération et de partage des clefs de signature.

Demandons la liste des certificats versées dans le dépôt public européen pour la France.

En ce qui concerne le convertisseur de certificats
La délégation est informée des éléments suivants :

Pour permettre l'intercompréhension des preuves dans différents pays, un convertisseur de preuves sanitaires a été mis en œuvre. Initialement, le format de preuve utilisé en France était le format 2D-DOC, spécifié par l'ANTS. Ce format a été utilisé jusqu'au 24 juin 2021, date à

laquelle il a été remplacé par le format DCC. [redacted] nous informe qu'une AIPD relative au convertisseur de certificat a été mise en œuvre.

Prenons copie de cette AIPD relative au convertisseur de certificat.

Si une preuve a été importée dans l'application avant le 24 juin 2021, il est possible depuis le 1er juillet 2021 de réaliser la conversion depuis le format 2D-DOC vers le format DCC. Lors de l'opération de conversion, le contenu du code à barres au format 2D-DOC est envoyé vers un serveur géré par [redacted] qui va s'assurer de l'intégrité de la preuve, puis va réaliser la conversion de format et signer le nouveau certificat avec une clef gérée par [redacted] Ce nouveau certificat est ensuite disponible dans l'application TousAntiCovid. La clef publique pour la vérification de la signature a été disposée dans un dépôt public européen.

[redacted]

Demandons toute documentation utile relative au projet en cours.

Un dispositif anti-DDOS et un pare-feu sont mis en œuvre par la société [redacted] afin de filtrer l'ensemble des requêtes adressées aux serveurs d'[redacted] lesquelles contiennent l'intégralité des 2D-DOC à convertir et certains nouveaux DCC à signer. Un changement de prestataire est à l'étude afin de remplacer la solution de la société [redacted] par une solution d'un autre prestataire européen. Le chiffrement de bout en bout précité resterait applicable même dans l'hypothèse d'une reprise de ces activités par un nouveau prestataire.

Prenons copie d'un extrait des journaux du serveur anti-DDOS et pare-feu mis en œuvre par la société [redacted]

Les requêtes de demande de conversion sont adressées à des infrastructures hébergées à la fois par [redacted] et par [redacted] à des fins de redondance, grâce à un répartiteur de charge. Le service de conversion est cependant uniquement hébergé chez [redacted]

À l'avenir, il est prévu que le service de conversion des certificats puisse permettre la conversion vers d'autres formats que le format DCC, notamment internationaux.

Le serveur central ne stocke aucune donnée de façon persistante. Les journaux des requêtes ne font apparaître aucune donnée personnelle relative aux certificats convertis.

Prenons copie d'un extrait des journaux du serveur de conversion.

Certains codes 2D-DOC ne contiennent pas suffisamment d'informations pour permettre leur bonne conversion au format DCC. Pour chacun des tests réalisés ces trois derniers mois, un nouveau certificat au format DCC a été généré par SI-DEP.

Nous munissons à nouveau du téléphone iPhone X de la marque Apple.

Ouvrons l'application TousAntiCovid et accédons à la fonctionnalité « Carnet » de cette dernière.

Affichons le certificat de vaccination précédemment importé.

Demandons la réalisation de l'opération de conversion du certificat depuis le format 2D-DOC vers le format DCC.

Affichons les conditions générales d'utilisation de l'application TousAntiCovid et en prenons des copies écran.

Réalisons la conversion à proprement parler au format DCC du certificat de vaccination.

Constatons l'affichage du certificat de vaccination au format DCC.

Prenons avec le téléphone Pixel 3XL une photographie de l'écran de l'iPhone affichant le certificat précité au format DCC.

Opérons une transcription du certificat DCC, au moyen de la fonction « Lens » de la galerie de photos Android.

Par ailleurs, demandons communication, de manière sécurisée, dans un délai de **8 jours ouvrés**, de la copie des pièces suivantes nécessaires à l'accomplissement de notre mission :

- la convention signée entre la DGS, l'ANTS et la Direction des libertés publiques et des affaires juridiques ;
- toute documentation utile relative au projet de chiffrement de bout en bout du certificat à convertir lors de sa transmission ;
- la liste des situations dans lesquelles [redacted] génère et signe les preuves au format DCC ;
- le nombre total de preuves au format 2D-DOC générés depuis le début des traitements décrits dans le présent procès-verbal ;
- le nombre total de preuves au format DCC générés depuis le début des traitements décrits dans le présent procès-verbal ;
- le nombre d'opérations de conversion depuis le format 2D-DOC vers le format DCC réalisées depuis le début des traitements décrits dans le présent procès-verbal ;
- tout schéma illustratif pertinent relatif à la mise en œuvre des traitements décrits dans le présent procès-verbal.

À l'issue du contrôle, [redacted] responsable des lieux, a fait les observations suivantes :

 Paraphes [redacted]

La mission de contrôle s'est terminée, ce jour, à 21 heures 35 ;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé par nous et [redacted] responsable des lieux.

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
3, place de Fontenoy – TSA 80715
75334 PARIS Cedex 07
www.cnil.fr

ANNEXE 1 :

INVENTAIRE DES PIÈCES RECUEILLIES

Les copies, notamment informatiques, effectuées par la délégation de la CNIL font l'objet de mesures de protection particulières destinées à assurer leur confidentialité.

Les copies informatiques font l'objet d'un calcul d'empreinte numérique garantissant leur intégrité et leur authenticité.

Ces empreintes numériques sont calculées par l'intermédiaire de l'algorithme SHA256.

Le responsable des lieux a été mis en mesure de consulter les pièces copiées.

[redacted]

Paraphes

[redacted]

[redacted]

Paraphes

[redacted]

[redacted]

Paraphes

[redacted]

[redacted]

Paraphes

[redacted]

Paraphes

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[redacted]

[redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

MINISTÈRE DES SOLIDARITÉS
ET DE LA SANTÉ
MONSIEUR LE MINISTRE
14 AVENUE DUQUESNE
75350 PARIS SP 07

Paris, le 23 JUIL. 2021

N/Réf. : [redacted]CS211057
LRAR n° 2C 156 060 2190 8
À rappeler dans toute correspondance

Monsieur le Ministre,

Conformément aux décisions **n° 2020-270C en date du 22 octobre 2020** et **n° 2021-124C en date du 29 juin 2021**, la Commission nationale de l'informatique et des libertés (CNIL) a effectué des contrôles des traitements accessibles à partir de l'application « TousAntiCovid » afin de vérifier leur conformité aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 et de la loi du 6 janvier 1978 modifiée.

Ces vérifications font suite à l'ajout des nouvelles fonctionnalités TAC CARNET et TAC SIGNAL dans l'application TousAntiCovid, ainsi qu'au déploiement de l'ensemble des traitements en lien avec la mise en œuvre du passe sanitaire en France. Une série de contrôles a ainsi été effectuée en juin et juillet 2021 auprès du ministère des Solidarités et de la Santé ainsi que de son sous-traitant l'INRIA, ayant en particulier pour objet de vérifier les conditions de traitements des tests de dépistage positifs ou négatifs et des attestations de vaccination au sein de l'application TousAntiCovid.

Sans préjuger des suites qui seront apportées à cette procédure de contrôle et des vérifications complémentaires que la CNIL pourrait être amenée à réaliser à l'avenir, les constatations effectuées me conduisent à vous faire part des observations suivantes.

La délégation a constaté que la nouvelle version de l'application TousAntiCovid, déployée le 1er juillet 2021, permet aux utilisateurs de convertir au format européen DCC, directement dans l'application, leurs justificatifs importés avant le 24 juin 2021 au format 2D- DOC jusqu'à présent utilisé en France. Lors de cette opération de conversion, le contenu du code à barres au format 2D-DOC est envoyé vers un serveur géré par [redacted] qui va s'assurer de l'intégrité du justificatif, puis va réaliser la conversion de format et signer le nouveau certificat avec une clef gérée par [redacted]

La délégation a également constaté qu'un dispositif anti-DDoS et un pare-feu sont mis en œuvre par la société [redacted] prestataire [redacted] afin de filtrer l'ensemble des requêtes qui sont adressées aux serveurs de ce dernier. Ces requêtes contiennent l'intégralité des 2D-DOC à convertir et certains nouveaux DCC à signer qui comporte dès lors des données de santé. Les investigations menées ont également permis d'établir que les serveurs de la société [redacted] sur lesquels transitent les données précitées sont en partie situés aux États-Unis et que ces transferts sont uniquement encadrés par des clauses contractuelles types, sans mesures additionnelles particulières.

Or, je vous rappelle qu'en application des dispositions de l'article 46 du Règlement précité, « *en l'absence de décision en vertu de l'article 45, paragraphe 3 [décision d'adéquation], le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effective* ». A cela s'ajoute le fait que la Cour de justice de l'Union européenne (CJUE) a précisé dans son arrêt C-311/18 (Schrems II) que la législation américaine, à savoir la Section 702 de la FISA et l'Exécutive Order 12 333 (permettant aux autorités américaines l'accès à des données d'utilisateur en dehors des EU), ne respectait pas les garanties minimums qu'imposent les principes du RGPD, ce qui implique notamment, préalablement à de tels transferts, de prendre des mesures techniques supplémentaires afin des rendre l'accès à ces données par les autorités américaines impossible ou ineffectif.

Pour rappel, l'EDPB indique, dans ses recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, que lorsque les données peuvent faire l'objet d'un accès par les autorités du pays de destination même lors du transit vers celui-ci et que ce dernier n'offre pas un niveau de protection essentiellement équivalent, des mesures doivent être prises afin de rendre l'accès aux données impossibles ou ineffectives. Les mesures identifiées par le CEPD à ce jour sont les suivantes :

- un chiffrement du transport est utilisé, pour lequel il est garanti que les protocoles de chiffrement employés sont à la pointe de la technologie et offrent une protection efficace contre les attaques actives et passives menées au moyen de ressources dont disposent les autorités publiques du pays tiers ;
- au cas où le chiffrement du transport n'offre pas, en soi, une sécurité suffisante en raison de la vulnérabilité de l'infrastructure ou du logiciel utilisé, les données à caractère personnel sont également chiffrées de bout en bout sur la couche application grâce à des méthodes de chiffrement de pointe ;
- l'algorithme de chiffrement et son paramétrage (par exemple, la longueur de clé, le mode opératoire, le cas échéant) sont conformes à l'état de la technique et peuvent être considérés comme résistants à une cryptanalyse réalisée par les autorités publiques du pays destinataire, compte tenu des ressources et des capacités techniques (par exemple, la puissance de calcul pour les attaques par force brute) dont elles disposent.

Je relève à cet égard que si les données sont transmises aux serveurs de la société [redacted] *via* un tunnel TLS, celles-ci ne sont en elles-mêmes pas chiffrées. Ainsi, la société [redacted] dispose de la possibilité d'accéder à l'intégralité des 2D-DOC et DCC (une fois convertis) qui transitent par ses serveurs et peut donc accéder aux données stockées sur ces supports.

J'ai bien pris note qu'un changement de prestataire est à l'étude afin de remplacer la solution de la société [redacted] par une solution d'un autre prestataire soumis à des juridictions relevant exclusivement de l'Union européenne, pour autant, **dans l'attente de ce changement, il vous appartient de prendre les mesures nécessaires afin de garantir la conformité des traitements mis en œuvre dans les plus brefs délais.** La mise en place d'un chiffrement de bout en bout des certificats à convertir durant leur transmission, en plus du tunnel TLS déjà en place, sur laquelle il a été indiqué à la délégation de la CNIL que vos services travaillaient déjà, apparaît constituer une solution satisfaisante.

Sur ce point, j'attire votre attention sur le fait que l'algorithme de chiffrement à déployer devra être conforme à l'annexe B2 du référentiel général de sécurité (RGS). Ces exigences sont également valables pour le tunnel TLS mis en place entre l'application TousAntiCovid et les serveurs [redacted]

Dans ces conditions, **je vous remercie de bien vouloir indiquer à la Commission dans les meilleurs délais, et au plus tard le 2 août 2021, les mesures prises afin de permettre une mise en œuvre effective de ce protocole de chiffrement. À défaut, je me réserve la possibilité de prononcer une mise en demeure à l'égard du ministère des solidarités et de la santé sur ce point.**

Mes services [redacted] se tiennent à la disposition des vôtres pour toute information complémentaire.

Je vous prie d'agréer, Monsieur le Ministre, l'expression de ma plus haute considération.

Marie-Laure DENIS

Copie à [redacted] (Déléguée à la protection des données)