CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Missions de vérification de la CNIL portant sur la conformité à la règlementation du traitement de données à caractère personnel dénommé « SI-DEP » (système d'information de dépistage) (mai 2020-décembre 2021)

La Présidente

Le 22 mai 2020

Décision n° 2020-092C 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 de tous traitements

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, du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le ministre chargé de la santé (direction générale de la santé) et de tout traitement lié ;

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 25/05/2020

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-2020-001 du 14 mai 2020 habilitant des agents de la CNIL à procéder à des missions de vérification ;

Charge [redacted]

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°2020-092C du 22 mai 2020.

Le secrétaire général,

Louis DUTHEILLET de LAMOTHE

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Le 20/09/2021

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 31 mai 2021 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 ;

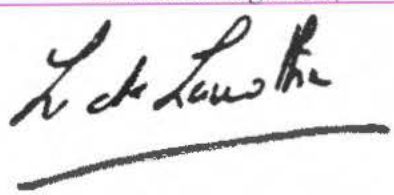
Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

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-2021-002 du 6 mai 2021 habilitant des agents de la CNIL à procéder à des missions de vérification ;

Charge, [redacted] de procéder, dans les conditions prévues aux articles 19 de la loi du 6 janvier 1978 modifiée et L. 253-3 du code de la sécurité intérieure, aux vérifications décidées par la Présidente dans sa décision n° 2020-092C du 22 mai 2020.

Le secrétaire général,



Louis DUTHEILLET de LAMOTHE

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°2020-092C en date du 22 mai 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de 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, du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le ministre chargé de la santé (direction générale de la santé) et de tout traitement lié ;

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

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 1er juillet 2020, à 9h00, dans les locaux de l'Assistance Publique - Hôpitaux de Paris (AP-HP), situés 33 Boulevard de Picpus 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 l'information des personnes

[redacted] nous informe que l'information des personnes concernant le traitement de leurs données à caractère personnel au sein du traitement SI-DEP ne figure pas sur le site Internet de l'AP-HP.

À notre demande, [redacted] se connecte sur le site internet du Ministère des solidarités et de la santé.

Constatons, au bas de la page d'accueil de ce site, la présence d'un lien intitulé « Données personnelles et cookies » ; cliquons sur ce lien et constatons l'affichage d'une page ayant pour URL https://solidarites-sante.gouv.fr/ministere/article/donnees-personnelles-et-cookies.

Constatons que cette page comporte notamment un onglet dénommé « Direction générale de la santé (DGS) » ; cliquons sur l'icône « + » afin d'ouvrir l'onglet et constatons que la présence de mentions d'informations relatives au traitement SI-DEP.

[redacted] *nous informent des éléments suivants :*

L'objectif de la page « données personnelles et cookies » est de regrouper toute l'information des personnes concernant les traitements mis en œuvre par l'ensemble des directions du Ministère des solidarités et de la santé.

Début mai 2020, le Ministère a publié sur son site internet une page dénommée « Contact-COVID et SI-DEP, les outils numériques du dépistage COVID-19 » (voir pièce).

[redacted] *nous informe des éléments suivants :*

Un modèle de mentions relatives à la protection des données personnelles intitulé « SI-DEP : NOTICE D'INFORMATIONS POUR LES LABORATOIRES » contenant un modèle à afficher ainsi qu'à insérer dans le compte-rendu d'analyse a été adressé par la Direction générale de la santé à l'ensemble des laboratoires concernés par le dispositif SI-DEP préalablement au déploiement de ce dernier. Un guide a également été adressé à l'ensemble des laboratoires dont l'objet est de présenter le dispositif SI-DEP (voir pièce).

[redacted] *nous informe des éléments suivants :*

La Direction générale de la santé ne dispose pas d'un modèle de compte-rendu d'analyse envoyé par des laboratoires hors MGI dans la mesure où ce compte-rendu est produit dans le système d'informations propre à chaque laboratoire.

Les champs relatifs à l'adresse email et au numéro de téléphone sont renseignés au moyen des coordonnées fournies par le patient, qui peuvent être les siennes ou celles d'une personne désignée par le patient. Seuls les champs d'adresse email et de numéro de téléphone peuvent contenir des données concernant une personne tierce. Dans le cas où le patient choisit de donner les coordonnées d'une personne tierce et non les siennes, cette personne réceptionne le compte-rendu d'analyse de la personne dépistée. Ce compte-rendu d'analyse contient les mentions relatives à la protection des données personnelles. C'est lors de la réception de ce compte-rendu qu'elle est informée des mentions relatives à la protection des données personnelles.

Les cas dans lesquels une personne dépistée désigne une personne de confiance sont très rares en pratique. Ils correspondent aux cas dans lesquels la personne dépistée ne dispose ni d'un numéro de téléphone mobile ni d'une adresse mail.

En ce qui concerne l'exercice des droits

[redacted] *nous informent des éléments suivants :*

Une adresse mail permettant d'exercer ces droits concernant SI-DEP a été créée (sidep-rgpd@sante.gouv.fr) et figure dans les mentions présentes sur le site Internet ainsi que celles remises par les laboratoires. Une adresse postale est également indiquée. Seules 5 demandes ont été reçues par courrier.

À ce jour, la DGS a reçu 52 demandes portant sur des sujets divers tels que le souhait de connaître davantage sur le dispositif SI-DEP, de s'opposer au traitement SI-DEP dans son intégralité. Les réponses aux demandes d'exercice des droits ont lieu par le même canal que la demande initiale (email ou courrier).

L'équipe, composée de 6 personnes au sein de la DGS, examine la recevabilité de la demande. En cas de demande de suppression des données, la DGS précise aux personnes concernées qu'elle ne peut pas faire droit à leur demande. Elle leur précise également qu'elles peuvent s'opposer à la transmission de leurs données à des fins de recherche à Health Data Hub et à la CNAM, conformément aux dispositions réglementaires. Suite à cette précision, 25 personnes ont transmis les informations permettant l'exercice de ce droit d'opposition.

[redacted] *nous informe des éléments suivants :*

A ce jour, aucune transmission de données en direction de Health Data Hub et la CNAM n'ont été réalisées dans la mesure où l'architecture technique de celles-ci n'est pas finalisée. La finalisation est prévue à la mi-juillet 2020.

[redacted] *nous informent des éléments suivants :*

L'analyse d'impact relative à la protection des données sera mise à jour dès que les transmissions à Health Data Hub et à la CNAM seront effectives.

A ce jour, la gestion des demandes d'opposition n'est pas implémentée dans l'application SI-DEP, elle le sera lors de l'ouverture des flux vers le Health Data Hub et la CNAM. Cette fonctionnalité est en cours de déploiement. La liste des personnes s'étant opposées à ce jour est consignée dans un fichier Excel qui est alimenté et mis à jour par l'AP-HP en la personne de [redacted]

Dès que la fonctionnalité relative au droit d'opposition sera effective dans l'application SI-DEP, les données contenues dans le fichier Excel précité seront intégrées dans le dispositif SI-DEP.

[redacted] *nous informent des éléments suivants :*

4 demandes de droits d'accès ont été reçues et traitées à ce jour. Il incombe à l'AP-HP de procéder aux extractions de données puis de les transmettre à la personne concernée. A ce jour, les réponses à ces demandes de droit d'accès ont été adressées par email, sans mesure de chiffrement.

[redacted] *nous informent des éléments suivants :*

Les durées de conservation relatives aux demandes et aux réponses sur l'exercice des droits sont à l'étude par l'archiviste de la Direction générale de la santé.

Une fiche CYCLAD est en cours d'élaboration.

En ce qui concerne les durées de conservation

[redacted] *nous informe des éléments suivants :*

Le projet de loi organisant la sortie de l'état d'urgence sanitaire devrait être adopté d'ici quelques jours. L'article 2 de ce projet de loi prévoit d'allonger la durée de conservation des données issues du traitement SI-DEP pour les finalités de recherche et d'analyse épidémiologique. Ces données devront être pseudonymisées et leur durée de conservation devra être prévue par décret pris en Conseil d'état après avis de la CNIL mais ne pourra, en tout état de cause, dépasser les six mois.

Ce projet de loi n'aura pas d'impact sur la durée de conservation des données dans le traitement SI-DEP car celui-ci n'a pas pour finalité le suivi épidémiologique et la recherche.

En ce qui concerne les flux de données entrants et sortants de SI-DEP

[redacted] *nous informent des éléments suivants :*

Tous les résultats des tests réalisés par des établissements de santé ou des laboratoires privés sont transportés par l'application d'intégration (EAI) [redacted], dont l'hébergement est certifié HDS. Les résultats sont rapatriés selon des formats standards pour les données de santé (HL7, H'santé et H' médecin) puis sont déposés sur un NAS avant d'être intégrés à la base de données de SI-DEP. Le portail applicatif permettant de consulter les données intégrées à la base de données de SI-DEP est appelé Cybercovid.

L'EAI est également utilisé pour des flux de sortie : la transmission des résultats d'analyse à destination de la DREES (messages cumulés de la journée dans un NAS au format CSV puis transmis une fois par jour) et Santé publique France (transmission des messages au fil de l'eau via un flux HL7).

L'architecture d'un nouveau flux vers le Health Data Hub géré par la CNAM est en cours de validation. Ce nouveau flux fera l'objet d'une mise à jour de l'AIPD et d'une information à la CNIL.

Dans le cadre du dispositif SI-DEP, des laboratoires dits « MGI » ont été équipés de machines de test à haut débit de la société MGI dans le but d'augmenter la capacité de test (2 000 tests par jour pour chaque laboratoire) afin de réaliser 40 000 à 50 000 tests par jour au total. 18 de ces sites sont des laboratoires publics et 2 privés.

Les sites MGI sont généralement dédiés à des dépistages populationnels, plutôt qu'individuels. Une ARS peut décider d'aller tester des lieux publics, par exemple tous les résidents d'un EPHAD, ce qui déclenche une intervention de la part d'un laboratoire MGI.

Les préleveurs du laboratoire peuvent générer sur place les fiches relatives aux patients prélevés ou bien celles-ci peuvent être créées en masse, par import de fichier CSV dans SI-DEP, avant l'intervention si l'identité des personnes à tester est connue à l'avance. Lors du prélèvement, un lien est créé dans SI-DEP entre la fiche du patient et l'écouvillon qui contient le prélèvement. Cybercovid envoie alors une demande d'analyse vers le labo MGI pour tous les patients pour lesquels une fiche a été créée. Le laboratoire MGI qui reçoit cette demande doit réaliser l'analyse suite au rapatriement des écouvillons et transmettre en réponse le résultat du test à travers un flux HL7 contenant les données du test, le résultat ainsi que le PDF certifié COFRAC du compte-rendu de résultat d'analyse. Cela permet au patient de consulter son compte-rendu de résultat d'analyse sur l'interface de SI-DEP.

Les médecins prescripteurs reçoivent le compte-rendu de résultat d'analyse sur leur messagerie sécurisée de santé si cette information a été renseignée dans la fiche du test. Si leur adresse de messagerie sécurisée n'a pas pu être retrouvée, un envoi par courrier est déclenché (via la chaîne éditique).

Dans le cas des laboratoires non MGI, le compte-rendu de résultat d'analyse est transmis directement au patient concerné par les laboratoires. Le résultat d'analyse est transmis sous forme de données structurées à SI-DEP.

Si un patient est dépisté positif et que sa fiche dans SI-DEP comporte une adresse email et un numéro de téléphone portable, il sera informé par email qu'une fiche de résultat le concernant est accessible sur l'interface de SI-DEP au moyen d'un lien fourni dans l'email. L'activation du lien permet d'accéder au portail. Le patient y renseigne sa date de naissance ce qui entraîne

l'envoi d'un mot de passe à usage unique au patient par SMS qu'il devra renseigner pour pouvoir consulter sa fiche de résultat. La fiche de résultat est générée à chaque connexion à l'interface de SI-DEP à partir des informations contenues dans le système d'information. La fiche n'est pas stockée par ailleurs dans le système d'information.

Si le patient n'a pas fourni d'adresse email ou de numéro de téléphone portable, la fiche de résultat est éditée via un système d'éditique afin de l'adresser au patient par courrier. Le fichier contenant les informations nécessaire à la génération du courrier est transmis au système d'éditique (CORUS) par l'intermédiaire d'un espace tampon sur lequel le fichier n'est conservé que quelques minutes puis arrive sur le serveur CORUS où il est détruit après édition ou bien stocké 5 jours au maximum en cas d'erreur à l'impression.

En ce qui concerne les liens avec l'application STOP COVID

[redacted] *nous informent des éléments suivants*

Afin de permettre aux patients de renseigner leur statut de dépistage positif au sein de l'application mobile STOP COVID, un QR code leur est fourni par SI DEP en cas de dépistage positif lorsqu'ils accèdent à leur fiche de résultat. Ces QR codes ont une durée de validité de 7 jours à partir de leur attribution à une fiche de résultat.

Une application JAVA a été développée pour générer des QR codes au format UUID v4 pseudo-aléatoire sur un serveur géré par STOP COVID. Ces codes sont ensuite déposés sur un serveur SFTP sous la forme d'une archive dont l'intégrité est vérifiée [redacted] Un applicatif d'intégration (EAI) à la main du projet SI-DEP vérifie toutes les 5 minutes la mise à disposition de ce fichier contenant les QR codes puis, après vérification de l'empreinte du fichier, transfère le fichier vers l'applicatif Cybercovid.

Lors de la génération des QR Code, le logiciel JAVA effectue une vérification des collisions pour ne pas générer un QR code correspondant à un UUID déjà existant dans la base de QR codes valables de STOP COVID.

5000 QR codes ont été générés pour chaque jour compris entre le début du traitement et le mois de février 2021. Chaque QR code est lié à une date d'attribution spécifique permettant de s'assurer de sa validité pour une durée de 7 jours après attribution. Ainsi, chaque jour, il est possible d'attribuer jusqu'à 5000 QR codes à des fiches de résultat. Si nécessaire, en cas de pic de fiches de résultats positifs à générer dans une journée, il est possible de demander à STOP COVID de générer des QR codes supplémentaires.

Lorsqu'une fiche de résultat est générée, parmi la liste des QR codes valides pour une durée de 7 jours à compter de la date du jour, un QR code est sélectionné par SI-DEP puis assigné à ce résultat. En cas de nouvelle génération de la fiche de résultat (consultation ultérieure par le patient sur le portail SI-DEP), un lien entre le résultat et le QR code en base permettra d'assigner toujours le même code à la fiche.

Chaque jour, les QR codes périmés sont détruits ainsi que les QR codes non assignés de la veille.

En ce qui concerne les données collectées

[redacted] *nous informe des éléments suivants :*

Les données concernant un patient et un résultat d'analyse sont renseignées dans Cybercovid par les laboratoires réalisant les analyses soit au moyen de la connexion des systèmes MGI avec SI-DEP, soit au moyen d'une connexion du système de gestion du laboratoire (SGL) avec SI-DEP (à travers l'EAI), soit manuellement par le personnel du laboratoire via l'interface web Cybercovid.

Les données enregistrées dans SI-DEP sont volontairement réduites au minimum nécessaire au suivi épidémiologique, à l'information du patient et à l'enquête sanitaire. Les informations supplémentaires dont les laboratoires peuvent disposer concernant un patient ou une analyse n'ont pas vocation à quitter leur SGL. En particulier, SI-DEP n'accepte pas de champ de type commentaire libre ou notes diverses en provenance des systèmes d'information des laboratoires.

Les flux émis par les laboratoires respectent la norme Interop'Santé. Un contrôle qualité des données transmises par les laboratoires a lieu au sein de l'EAI puis dans SI-DEP afin de déterminer si les données peuvent intégrées telles quelles, qu'elles nécessitent une amélioration ou qu'elles ne peuvent être enregistrées (car elles ne permettent pas d'identifier le patient par exemple). Un retour automatisé est effectué auprès des laboratoires afin de permettre d'obtenir, le cas échéant, les données corrigées.

En ce qui concerne les mesures de sécurité

À notre demande, [redacted] se connecte à l'interface Cybercovid permettant d'accéder aux données figurant dans une base de qualification de l'application SI-DEP et documente sa navigation à l'aide de copies d'écran (voir pièces).

[redacted] *nous informent des éléments suivants :*

La base de données de qualification a été créée à partir d'une copie pseudonymisée de la base de production au sein de laquelle ont été opérées une suppression de certaines données et une distribution aléatoire des données situées dans les champs nom, prénom, adresse et date de naissance vers d'autres lignes.

L'accès à l'interface Cybercovid [redacted] est soumise à authentification de l'utilisateur. Depuis le réseau de l'AP-HP, ou depuis un VPN, il est possible de s'authentifier à l'aide d'un couple nom d'utilisateur/mot de passe. [redacted]

L'ensemble des comptes utilisateurs permettant d'accéder à Cybercovid sont individuels.

Les mots de passe des comptes utilisateurs de l'outil Cybercovid sont créés par les utilisateurs lors de leur première connexion. [redacted]

À notre demande, [redacted] e connecte à la base de données de qualification au moyen d'un compte utilisateur disposant d'un profil Administrateur Gestionnaire [redacted]

Ce profil est attribué aux agents de l'AP-HP en charge de l'administration de la solution Cybercovid. Il permet notamment la création de comptes utilisateur et l'affectation de tous les types de profils. Il s'agit du profil disposant des privilèges les plus élevés au sein de l'application Cybercovid.

L'application distingue les droits liés au profil (opérations autorisées) et au profil d'accès (données autorisées). Cette distinction a lieu au moyen de groupes qui permettent de cloisonner les patients auxquels les membres du groupe ont accès.

[redacted] modifie temporairement le paramétrage de l'environnement de qualification afin que celui-ci exige une authentification forte, y compris pour une connexion depuis le réseau de l'AP-HP afin de présenter le processus de connexion dans ce cas à la délégation, puis se déconnecte de l'interface. Constatons qu'après avoir renseigné son nom d'utilisateur et son mot de passe, il reçoit un SMS sur son téléphone concernant un code qu'il renseigne dans un champ dédié afin de s'authentifier.

[redacted]

[redacted] désactive l'exigence d'utilisation d'une authentification forte depuis le réseau de l'AP-HP sur l'environnement de qualification.

En ce qui concerne les habilitations

[redacted] *nous informent des éléments suivants :*

À notre demande [redacted] e déconnecte puis se reconnecte à l'interface Cybercovid de l'environnement de qualification au moyen d'un compte utilisateur disposant de chacun des profils utilisateur suivants, nous présente les différents écrans et données accessibles et documente sa navigation à l'aide de captures d'écran :

- [redacted]

Ce profil utilisé par les personnes de l'AP-HP effectuant du support utilisateur pour des questions de création de compte ou de vérification de flux.

Constatons que le menu « Labo » n'est plus affiché pour ce profil. Ce menu correspond à du paramétrage concernant l'intégration des résultats de tests réalisés par les laboratoires.

- Profil Régulateur sanitaire national : [redacted]

Ce type de profil est utilisé par la CNAM afin de réaliser du support de niveau 1 (création de compte déléguée par l'AP-HP pour les laboratoires).

Ce profil n'a pas accès au menu « système » et ne peut créer que des comptes de régulateur sanitaire local, d'enquêteur sanitaire ou de laboratoire non-connecté.

Ce compte dispose de la possibilité de faire des exports de données au format CSV.

- Profil Régulateur sanitaire local (ARS-CPAM) [redacted]

Ce profil est attribué aux régulateurs sanitaires des ARS et des CPAM. Ils disposent des mêmes droits que le Régulateur sanitaire national excepté la capacité de créer des comptes utilisateur disposant du profil de Régulateur sanitaire local.

- Profil Enquêteur sanitaire (ARS-CPAM) : [redacted]

Ce profil est attribué aux enquêteurs sanitaires habilités au sein des ARS et des CPAM. Il ne permet pas de réaliser d'export de données, permet d'accéder à toutes les fiches des patients, mais pas de lister tous les utilisateurs de Cybercovid.

- Profil Laboratoire non connecté : [redacted]

Ce profil est attribué au personnel de laboratoires non connectés et permet la saisie d'un nouveau « dossier », à savoir un patient et un résultat d'analyse. Il ne permet pas de rechercher ou de consulter de fiche patient ou de résultat d'analyse.

- Profil Administrateur local MGI : [redacted]

Ce profil est attribué à l'administrateur d'un site MGI. Il permet un accès en lecture uniquement aux patients dépistés au sein de son laboratoire. L'administrateur local peut voir tous les profils utilisateur du site de rattachement et peut créer ou modifier des groupes. Il peut réaliser des exports de données.

[redacted]réalise un export au moyen du compte utilisé pour la démonstration. Constatons que les patients listés dans le fichier sont rattachés à deux numéros de laboratoires.

[redacted] nous informe que l'un de ces numéros correspond au site Broussais (qui est le site attaché au compte utilisateur utilisé pour le test) et que le second correspond au site de Bichat ; qu'il ne sait pas pourquoi des patients de ces deux sites sont accessible à partir de ce compte utilisateur ; qu'il s'agit peut-être d'un écart de fonctionnement de l'environnement de qualification par rapport à l'environnement de production ; que des compléments seront fournis à la délégation sur les restrictions d'accès aux patients par site MGI.

- Profil Référent informatique : [redacted]

Ce profil est similaire au profil d'administrateur local mais ne permet pas d'export de données.

Mettons fins à nos constatations pour la journée et informons le responsable des lieux que celles-ci se poursuivront le lendemain.

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 :

- le document listant l'ensemble des données conservées dans SI-DEP, les exigences de conservation et les lieux de stockage des données ;
- la description des mécanismes restreignant l'accès des utilisateurs situés sur les sites MGI aux fiches des patients ;
- préciser si la procédure relative à l'exercice des droits a été formalisée par écrit et si oui, en communiquer une copie ;
- communiquer, de manière sécurisée, au médecin expert désigné dans le cadre de la présente procédure de contrôle, les 4 demandes de droit d'accès ayant été émises ainsi que les réponses apportées ;
- préciser les modalités d'information des personnes concernées dans les cas où le prélèvement n'a pas lieu dans un laboratoire ;
- indiquer les modalités selon lesquelles les médecins responsable de la prise en charge sont informés du traitement de leurs données et communiquer le support d'information fournie aux personnes concernés ;
- [redacted]
- l'exemple d'export au format CSV depuis le profil Régulateur Sanitaire National ;

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

[redacted]

La mission de contrôle s'est terminée, ce jour, à 21h00 ;

 Paraphes [redacted]

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.

PIECE N°1 : [redacted]

- [redacted]

PIECE N°2 : [redacted]

- [redacted]

PIECE N°3 : [redacted]

 Paraphes [redacted]

- [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°2020-092C en date du 22 mai 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de 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, du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le ministre chargé de la santé (direction générale de la santé) et de tout traitement lié ;

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

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 2 juillet 2020, à 9h00, dans les locaux de l'Assistance Publique - Hôpitaux de Paris (AP-HP), situés 33 Boulevard de Picpus à PARIS (75012) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité [redacted]
[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.

 Paraphes [redacted]

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne la visibilité des données de patients rattachés à un laboratoire

[redacted] nous informe, suite aux interrogations de la délégation lors de la mission du 1er juillet 2020, que la visibilité des fiches patient ou prélèvements est calculée selon l'organisation de rattachement du compte utilisateur et des patients ou prélèvements ; qu'un laboratoire pouvant analyser des prélèvements pour le compte d'autres laboratoires ou sur différents centres de prélèvement (intervention dans des établissements par exemple), il est possible qu'un utilisateur accède à des données de patients rattachés à différents groupes (correspondant à des centre de prélèvement différents).

En ce qui concerne les habilitations

Mentionnons que la base de données de qualification a été créée à partir d'une copie pseudonymisée de la base de production au sein de laquelle ont été opérées une suppression de certaines données et une distribution aléatoire des données situées dans les champs nom, prénom, adresse et date de naissance vers d'autres lignes.

À notre demande [redacted] se connecte à l'interface Cybercovid de l'environnement de qualification au moyen d'un compte utilisateur disposant de chacun des profils utilisateur suivants, nous présente les différents écrans et données accessibles et documente sa navigation à l'aide de captures d'écran :

- [redacted]

Ce profil est affecté aux biologistes situés dans les centres MGI. Le biologiste est responsable du résultat du test effectué, il a besoin d'un accès en lecture à tous les tests effectués par son organisation (laboratoire) afin de valider que l'information transmise est correcte.

Constatons que ce profil permet d'accéder en modification à une fiche de patient.

Constatons la présence dans le menu d'une rubrique « Audit ».

[redacted] nous informe que ce menu permet d'afficher l'historique des modifications ayant eu lieu sur la fiche (voir pièces).

 Paraphes [redacted]

- [redacted]

Ce profil est affecté aux personnes en charge de réaliser les prescriptions connectées. Il permet de rechercher un patient rattaché à un de ses centres de prélèvement, de créer un nouveau patient et de créer un nouveau dossier. Un dossier correspond à une demande de prélèvement (prescription connectée) qui sera réalisé par la suite avant analyse de l'échantillon.

- [redacted]

Ce profil est affecté aux préleveurs qui peuvent travailler sur différents centres de prélèvement et ainsi disposer d'une visibilité sur un nombre de groupes plus importants. Il dispose des mêmes droits que le préleveur mais peut accéder à un plus grand nombre de groupes de patients en raison de sa mobilité géographique. [redacted]ous informe qu'il n'y a pas de compte avec un tel profil sur l'environnement de qualification.

- [redacted]

Ce profil permet uniquement de constater l'état d'un dossier affecté à l'organisation de l'utilisateur. Il est utilisé dans les laboratoires MGI par des personnes en charge du support afin de permettre le suivi des dossiers en cours, entre la création de la demande de prélèvement et la transmission du résultat. Constatons qu'il n'est pas possible d'accéder au détail d'un dossier mais uniquement à son état.

- [redacted]

Ce profil est affecté aux médecins prescripteurs qui disposent d'un accès à SI-DEP. Cela est le cas typiquement pour des médecins en charge d'un établissement au sein duquel aura lieu une campagne de dépistage populationnel. Il peut accéder aux résultats de dépistage de l'ensemble des personnes dont il a la charge au sein de son établissement (Résidents pour un médecin d'EPHAD ou salariés pour un médecin du travail par exemple).

- [redacted]

Ce profil est affecté à un directeur d'établissement dans lequel a lieu une campagne de prélèvement (centre de prélèvement). Ce profil permet d'avoir accès en lecture à la liste des prescriptions en cours (dossiers) afin de suivre l'état d'avancement d'une campagne de prélèvement au sein de son établissement (groupe) sans connaître les résultats de dépistage.

[redacted]ous informe que les trois niveaux permettant de gérer la visibilité des dossiers dans Cybercovid sont l'organisation (laboratoire de rattachement), le groupe (établissement concerné, centre de prélèvement) et l'équipe (1 voire 2 par centre de prélèvement).

[redacted]nous informe que la procédure de création et de désactivation des comptes utilisateur SI-DEP est à la main de chaque organisation, l'administrateur local ayant pour mission de créer les comptes des personnes dont il a la charge et d'en gérer la désactivation lorsque nécessaire.

 Paraphes [redacted]

En ce qui concerne la traçabilité

[redacted] se connecte à l'interface de Cybercovid de l'environnement de qualification au moyen d'un compte ayant un profil de gestionnaire.

Constatons que, en consultant un résultat d'analyse, il est possible d'accéder à un journal des opérations ayant eu lieu sur ce résultat d'analyse.

Constatons que, sur l'écran de consultation d'un compte utilisateur, il est possible d'afficher un historique des modifications ayant affecté ce compte utilisateur.

[redacted]

[redacted] nous informe qu'il n'est pas possible d'accéder à l'audit concernant une fiche utilisateur, patient ou dossier si le profil du compte ne permet pas l'accès à ladite fiche mais que l'accès à une fiche ne donne pas nécessairement accès à l'historique des modifications. Constatons qu'un compte disposant d'un profil préleveur peut accéder au résultat d'analyse mais ne peut pas accéder au journal de modification.

[redacted] nous présente le journal des sessions, accessible à partir du profil gestionnaire. À notre demande, [redacted] effectue un export de toutes les traces enregistrées pour les journées du 1er et 2 juillet 2020 sur l'environnement de qualification.

À notre demande, [redacted] envoie un email informant qu'un résultat d'analyse est disponible à un patient de test. Constatons la réception dans sa boîte de messagerie d'un email informant de la disponibilité d'un résultat et contenant un lien permettant d'accéder au dit résultat. [redacted] clique sur le lien et constatons l'ouverture d'une page web correspondant à l'interface de Cybercovid et demandant la saisie de la date de naissance du patient. [redacted] saisit la date de naissance correspondant à l'utilisateur de test et valide ceci. Un décompte de 5 minutes s'affiche et [redacted] reçoit un SMS lui indiquant un code à renseigner dans le champ prévu à cet effet. [redacted] renseigne ce code, valide et constatons l'affichage d'une nouvelle page présentant les informations personnelles du patient ainsi que la liste de ses dossiers [redacted] télécharge le compte rendu d'analyse au format PDF (voir pièces).

Constatons que la page de résultat propose un second onglet concernant un autre patient de test. [redacted] nous informe que ce second patient est accessible car la même adresse email et le même numéro de téléphone sont utilisés comme moyens d'authentification.

Constatons que ce second patient de test est dépisté positif et que deux documents supplémentaires lui sont accessibles (voir pièces).

Constatons que la mention d'information au bas de la page fait référence à l'adresse email de l'AP-HP en ce qui concerne l'exercice des droits et non l'adresse email dédiée à SI-DEP de la DGS. [redacted] nous indique qu'il s'agit de la mention figurant sur l'environnement

de qualification, qu'une vérification doit être effectuée concernant la mention figurant sur l'environnement de production.

[redacted] affiche de nouveau les journaux de session sur l'environnement de qualification et constatons la présence de deux nouvelles lignes faisant référence à la connexion patient simulée par [redacted]

Constatons la présence d'autres types de journaux (actions dossier, actions patient, règles). Demandons copie de la documentation de l'éditeur MIPS concernant les différentes traces et journaux applicatifs dans Cybercovid.

[redacted] ous informe qu'une traçabilité du paramétrage est accessible au moyen du bouton « audit » situé sur chaque page de paramétrage et traçant les modifications de paramètres accessibles à partir de cette page.

En ce qui concerne la base de données

À notre demande [redacted] contacte [redacted] afin de nous présenter la base de données de production de l'application SI-DEP via visioconférence. [redacted] documente la navigation à l'aide de copies d'écran.

Précisons indiquer à [redacted] que la délégation n'a pas vocation à constater des données individuelles de santé sur cette base de production et que les vérifications porteront sur la sécurité et l'hébergement des données.

[redacted] *ous informent des éléments suivants :*

La base de données est accessible à partir d'un réseau d'administration dont un point accès est disponible dans les locaux de la DSI de l'AP-HP sur le site du 33 boulevard Picpus. La base de données en elle-même est hébergée dans un *data center* agréé HDS [redacted]

La connexion au serveur de base de données [redacted] se fait par un couple nom utilisateur et mot de passe via un compte d'administration générique. [redacted] Une fois connectés au serveur, les administrateurs utilisent les droits d'administration du compte utilisateur pour se connecter à la base de données.

La base de données Oracle est chiffrée [redacted]

[redacted]

En ce qui concerne les durées de conservation

[redacted] *nous informe des éléments suivants :*

La durée de conservation des données est calculée à partir de la date du prélèvement (saisie manuellement) ou de la date d'intégration dans SI-DEP selon la plus ancienne des deux.

 Paraphes [redacted]

Le mécanisme de purge a pour vocation de supprimer toutes les données dont le délai de conservation est échu. Celui-ci a été finalisé par l'AP-HP et testé en qualification. Les données ne font pas l'objet d'une procédure d'archivage. Ce système de purge a vocation à être exécuté de manière automatique et régulière.

Demandons copie de la spécification du mécanisme de purge, ainsi qu'un exemple de contenu de fichier journal de l'exécution du script de purge et la durée et les conditions de conservation de ces journaux.

[redacted] *nous informe des éléments suivants :*

La durée de conservation des fiches de résultats d'analyse des patients testés positifs sera mise à jour dans une prochaine version de l'AIPD concernant le traitement SI-DEP.

[redacted] *nous informe des éléments suivants :*

L'ensemble des flux sortants faisant l'objet d'une pseudonymisation (à destination de la DREES, de Santé Publique France et, à l'avenir, du Health Data Hub et de la CNAM) subissent la même procédure de pseudonymisation [redacted] L'ensemble des fichiers impliqués dans ces flux ne sont hébergés que pour le temps du transfert vers les tiers et ne sont pas conservés sur des serveurs intermédiaires (à l'exception du fichier transmis à la DREES qui constitue un cumul des données pour une durée d'une journée).

Un outil de supervision fonctionnelle [redacted] est en cours de déploiement afin de surveiller l'activité (charge et comportements anormaux) en se basant sur les différents fichiers journaux. La supervision applicative des outils de l'AP-HP – y compris SI-DEP – est réalisée par une équipe dédiée.

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 :

- [redacted] ;
- la documentation MIPS concernant les différentes traces applicatives ;
- les scripts de pseudonymisation de la base de qualification ;
- le registre des violations de données de la Direction générale de la santé ;
- les spécifications à date de l'outil de supervision fonctionnelle en cours de déploiement ;
- la spécification du mécanisme de purge, ainsi qu'un exemple de contenu de fichier journal de l'exécution du script de purge et la durée et les conditions de conservation de ces journaux ;
- la copie écran du portail patient testé dans l'environnement de production ainsi que la copie écran de la page éventuelle renvoyant vers les mentions relatives à la protection des données (en masquant les données individuelles) ;
- le nombre de tests réalisés enregistrés dans le dispositif SI-DEP ;
- l'AIPD concernant le traitement SI-DEP mise à jour lorsque celle-ci sera disponible ;
- le nombre de personnes ayant accès au compte utilisateur permettant l'administration de la base de données ;

 Paraphes [redacted]

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

[redacted]

La mission de contrôle s'est terminée, ce jour, à 18h30 ;

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.

PIECE N°1 : [redacted]

PIECE N°2 : [redacted]

PIECE N°3 : [redacted]

PIECE N°4 : [redacted]

PIECE N°5 : [redacted]

PIECE N°6 : [redacted]

PIECE N°7 : [redacted]

PIECE N°8 : [redacted]

PIECE N°9 : [redacted]

 Paraphes [redacted]

PIECE N°10 : [redacted]

PIECE N°11 : [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 à la décision de la présidente de la CNIL n°2020-092C en date du 22 mai 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de 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, du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le ministre chargé de la santé (direction générale de la santé) et de tout traitement lié ;

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

En présence du [redacted] médecin expert judiciaire près la cour d'appel de Paris, en qualité de médecin expert ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 3 juillet 2020, à 9h00, dans les locaux du site Broussais de l'Assistance Publique - Hôpitaux de Paris (AP-HP), situés 8 rue Maria Héléna Vieira Da Silva à Paris (75014) 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 site de BROUSSAIS

Sommes informés par [redacted] *les éléments suivants :*

Le site Broussais de l'AP-HP intègre un laboratoire d'analyse dit « MGI ». Il existe 20 plateformes MGI en France dont 2 laboratoires privés. Le laboratoire a une capacité de 4000 prélèvements par jour (2 MGI). Il effectue des tests dits « RT-PCR ». Il n'effectue pas de test sérologique. Ce site n'effectue pas de prélèvement et n'accueille pas de patients.

Les prélèvements transmis et analysés au site Broussais sont effectués par des équipes de l'AP-HP sur des sites ciblés selon la politique de dépistage définie par l'ARS Ile-de-France, tels que des EPHAD ou des barnums installés temporairement, dans le but de détecter et prévenir les éventuels clusters. Ces équipes de préleveurs sont accompagnés de médecins de l'ARS Ile-de-France et/ou de l'AP-HP. Ces équipes sont rattachées à une antenne au site Picpus de l'AP-HP, où elles récupèrent notamment des kits de prélèvement comprenant notamment des éléments d'information des personnes.

Les équipes du laboratoire du site Broussais ne se déplacent pas sur les sites de prélèvement.

En ce qui concerne le parcours des données utilisateurs

À notre demande [redacted] se connecte à la plate-forme de production.

[redacted] nous informe que, dans un premier temps, une prescription connectée de test sera créée par [redacted] afin de présenter la séquence de traitement des données personnelles lors d'un dépistage, sans qu'il ne soit nécessaire à la délégation d'accéder à des données individuelles de santé (voir pièces) ; que cette prescription sera créée dans une organisation permettant de s'assurer que les données ne seront pas prises en compte dans les statistiques de SI-DEP ou bien lors des exports vers les systèmes tiers.

Constatons un champ permettant de renseigner un numéro d'échantillon.

[redacted] nous informe que le prescripteur qui prépare la prescription connectée renseigne le numéro de code barre associé au tube destiné à recueillir le prélèvement du patient via écouvillon ; que tous les tubes de prélèvement sont pré-étiquetés sur le site de Broussais avec des numéros uniques permettant de les référencer dans le système d'information de laboratoire du site de Broussais ; que chaque laboratoire dispose de son propre système de numérotation indépendant.

Constatons qu'il est possible de sélectionner si oui ou non le résultat du dépistage peut être consulté sous-forme numérique sur le portail ; que par défaut, l'option « oui » est cochée.

[redacted] nous informe que cette option est définie par défaut conformément aux dispositions de l'article D6211-3 du Code de la santé publique.

[redacted] nous informent que cela permet d'assurer au maximum une communication du résultat rapide au patient, contrairement à l'envoi par courrier.

Constatons qu'après création de la prescription connectée, plusieurs fonctions sont disponibles sur l'écran de visualisation de la prescription finalisée.

[redacted] nous informe qu'il s'agit d'options disponibles par défaut dans le logiciel Cyberlab ; que seule l'option « discontinuer » est a priori utilisée dans le cadre du traitement SI-DEP, afin d'interrompre le traitement d'un dossier qui présenterait des anomalies.

Mentionnons nous déplacer dans les locaux du laboratoire MGI du site Broussais afin de constater les étapes de la réception des prélèvements à la validation du résultat par le biologiste.

[redacted] *nous informe des éléments suivants :*

À leur arrivée au sein du laboratoire chaque tube de prélèvement contenant un écouvillon est emballé dans un sachet individuel marqué du nom, du prénom de la date de naissance et du sexe du patient prélevé. Cette information permet, lors de l'ouverture du sachet, de vérifier que le numéro de code barre présent sur le tube référence bien la personne dont l'identité figure sur le sachet. Les laboratoires d'analyse font preuve d'une vigilance particulière sur l'identité des patients (identitovigilance).

Toute la phase d'analyse du prélèvement fait l'objet d'un suivi détaillé à l'aide du logiciel [redacted] système d'information de laboratoire (SIL) utilisé par les sites de l'AP-HP. Le traitement des données dans [redacted] est distinct du traitement SI-DEP.

Les échantillons subissent plusieurs opérations avant le test RT-PCR, notamment des phases d'inactivation, de centrifugation, d'extraction d'ARN.

Le test RT-PCR a pour objectif de déterminer la présence d'ARN du virus SARS-COV2 dans l'échantillon. Le résultat du test est transmis sous forme de courbe de détection de marqueurs au SIL afin que le biologiste valide le résultat de positivité ou non du prélèvement. Une fois validé dans le SIL, le statut de positivité, négativité, d'indétermination ou de non-conformité est transmis à SI-DEP.

[redacted] indique dans le SIL un résultat fictif pour le numéro d'échantillon précédemment créé par [redacted] afin que cette information soit transférée dans SI-DEP pour les besoins de la démonstration.

[redacted] nous présente l'affichage des résultats du test fictif dans SI-DEP du point de vue d'un patient (voir pièces). Constatons la présence de mentions d'information et de liens vers une politique de protection des données sur le portail de consultation des résultats (voir pièces).

Mentionnons que la délégation quitte la pièce et demande à [redacted] prenne connaissance de données réelles de patients accessibles par les utilisateurs SI-DEP du site de Broussais sans que la délégation n'en prenne connaissance dans un premier temps. [redacted] nous informe de la possibilité de prendre connaissance des données médicales individuelles figurant dans le traitement dans le cadre de la mission de contrôle. Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle de [redacted] médecin expert.

[redacted] nous présente les données auxquelles il peut accéder à partir de son compte disposant d'un profil de biologiste dans l'environnement de production SI-DEP et documente sa navigation à l'aide de copies d'écran (voir pièces).

[redacted] nous présente les données accessibles et opérations autorisées aux utilisateurs disposants des profils d'administrateur local et documente sa navigation à l'aide de copies d'écran (voir pièces). Constatons qu'il est possible à [redacted] de consulter la liste des centres de prélèvement rattachés à l'organisation d'Aix-en-Provence ; qu'il ne lui est pas possible de modifier l'organisation de rattachement d'un centre de prélèvement rattaché à l'organisation d'Aix-en-Provence.

Constatons que les comptes utilisateurs comportent un champ « Remarques » de texte libre. [redacted] nous informe qu'il est utilisé pour renseigner des coordonnées d'un préleveur référent dans le cas où un unique compte de préleveur est créé pour une opération de dépistage sur un centre de prélèvement et utilisé par plusieurs préleveurs.

Constatons qu'il est possible d'exporter au format CSV la liste des données administratives et de résultats concernant les patients rattachés à l'organisation de Broussais.

[redacted] nous informe que seul le profil d'administrateur local peut réaliser cette opération ; qu'elle n'est réalisée qu'en cas d'investigation pour faciliter la recherche d'anomalie et leur résolution ; les personnes disposant d'un compte utilisateur ayant un profil d'administrateur local signent un engagement de confidentialité (voir pièces).

[redacted] créé un compte fictif avec le profil préleveur rattaché au centre de prélèvement de Sevran afin de nous présenter les restrictions d'accès de ce type de compte aux données rattachées à son centre de prélèvement et documente sa navigation à l'aide de copies d'écran (voir pièces).

[redacted] modifie les droits du compte fictif afin de lui affecter un profil de prescripteur afin de nous présenter les restrictions d'accès de ce type de compte aux données rattachées à son centre de prélèvement et documente sa navigation à l'aide de copies d'écran (voir pièces).

En ce qui concerne la *hotline* Broussais

[redacted] *ous informe des éléments suivants :*

Les informations communiquées aux patients incluent le numéro de téléphone de l'équipe de prélèvement afin de les contacter, notamment lorsqu'ils n'ont pas reçu les résultats de leur test.

En cas d'anomalie au niveau des coordonnées de contact du patient (email, numéro de téléphone), l'équipe de prélèvement redirige le patient vers une hotline mise en place sur le site Broussais.

Les appels reçus par la hotline sont traités par des techniciens de laboratoire et par l'équipe projet local Broussais qui disposent d'un compte d'accès à SI-DEP ayant un profil d'administrateur local afin de pouvoir identifier la source du problème et effectuer des modifications sur les coordonnées des fiches patient si nécessaire.

Ce compte est commun à tous les techniciens (identifiant et mot de passe unique).

Les techniciens ne communiquent pas les résultats du test par téléphone. Ils déclenchent un nouvel envoi du courriel d'accès au portail sécurisé de consultation de résultat via SI-DEP.

Les techniciens émargent à chaque prise de poste et ont signé une charte des systèmes d'information hospitalier et un engagement de confidentialité.

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 ;

Mentionnons que [redacted] médecin expert, a demandé au responsable des lieux copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui seront communiqué de façon sécurisée sans que les membres de la délégation n'en prennent copie

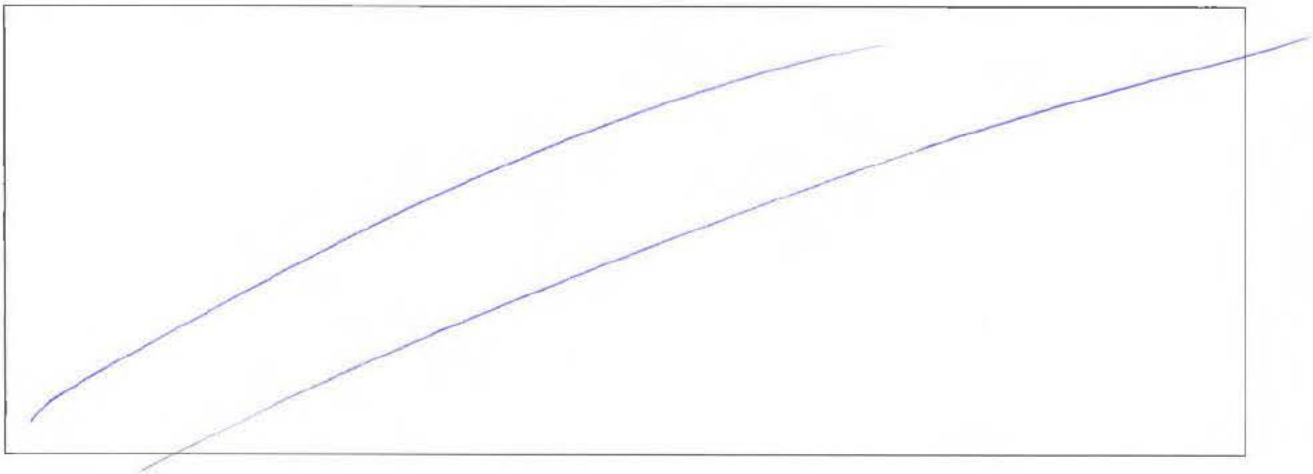
Par ailleurs, demandons communication, de manière sécurisée, dans un délai de **8 jours ouvrés**, de la copie des pièces suivantes nécessaires à l'accomplissement de notre mission :

- Une extraction de tous les champs « remarque » des comptes d'utilisateur ;
- Un exemple de kit d'information remis aux patients prélevés ;
- Un exemple de kit de formation remis aux préleveurs ;
- Statistiques sur le taux de résultats de tests « Non Conforme ».

Demandons également que soient communiquées au [redacted] de manière sécurisée, dans un délai de **8 jours ouvrés**, la copie des pièces suivantes nécessaires à l'accomplissement de notre mission :

- Les 4 demandes de droit d'accès reçues par l'AP-HP ;
- Captures d'écran des fiches patient accédées depuis un compte ayant un profil d'administrateur local ;
- Captures d'écran des fiches patient accédées depuis un compte ayant un profil de biologiste ;
- Export CSV effectué depuis un compte ayant un profil d'administrateur local ;
- Liste PDF des échantillons pouvant être consultés depuis le profil de préleveur créé ;

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



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.

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.

PIECE N°1 : [redacted]

- [redacted]
- [redacted]

PIECE N°2 : [redacted]

PIECE N°3 : [redacted]

PIECE N°4 : [redacted]

PIECE N°5 : [redacted]

PIECE N°6 : [redacted]

PIECE N°7 : [redacted]

 Paraphes [redacted]

PIECE N°8 : [redacted]

PIECE N°9 : [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 à la décision de la présidente de la CNIL n° 2020-092C en date du 22 mai 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le Ministre chargé de la santé (Direction générale de la santé) et de tout traitement lié auprès de tout organisme concerné par sa mise en œuvre, aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n° 78-17 du 6 janvier 1978 modifiée et, le cas échéant aux dispositions des articles L. 251-1 et suivants du code de la sécurité intérieure ;

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

En présence du [redacted], médecin expert judiciaire près de la Cour d'appel de Paris, en qualité de médecin expert ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 23 octobre 2020, à 9 heures 30, dans les locaux de l'Assistance publique – Hôpitaux de Paris situés 33 boulevard Picpus 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 ;

[redacted]

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne les flux de données à destination des partenaires de SI-DEP

À notre demande, [redacted] nous présente l'architecture générale du traitement SI-DEP ainsi que les interactions avec les systèmes d'information partenaires (voir pièces).

[redacted] *nous informent des éléments suivants :*

La plupart des utilisateurs disposant d'un accès à SI-DEP à des fins de *contact tracing* (enquêteurs sanitaires CNAM, ARS ???) accèdent aux données à travers l'interface de l'application. Les administrateurs locaux des ARS disposent de la possibilité d'exporter des données.

Des flux de données dédiés au *contact tracing* ont été mis en œuvre au début du mois d'octobre 2020 à destination des services chargés du suivi des cas contacts.

Ces flux ont été mis en œuvre à destination des administrateurs nationaux pour combler des défauts d'ergonomie et de disponibilité de l'interface de l'outil Cybercovid. Le système d'information a en effet connu des indisponibilités durant l'été, notamment dues à des attaques par déni de service.

Dans ce cadre, les données nominatives de SI-DEP sont mises à disposition des administrateurs nationaux de la DRSM (CNAM) ainsi qu'à la DNUM au moyen de fichiers CSV. Cette mise à disposition s'effectue au moyen de flux sécurisés par l'ETL médiation.

Des données pseudonymisées sont transmises à Santé publique France (SPF) et à la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES). Les pseudonymes utilisés au sein de ces flux permettent de comptabiliser une seule fois chaque patient.

Les données sont transmises à SPF [redacted] en temps réel, et à la DREES via un export quotidien au format CSV.

L'intégration dans SI-DEP des résultats de tests antigéniques est en cours d'examen.

En ce qui concerne le flux à destination du Health Data Hub

[redacted] *nous informe des éléments suivants :*

L'objectif de ce flux de données est d'alimenter le *Health Data Hub* afin de fournir aux chercheurs un accès aux données à des fins de recherche. Ces données sont pseudonymisées par la CNAM afin de permettre un chaînage avec d'autres données de la CNAM, dont celles du système national des données de santé (SNDS).

La transmission des données à la CNAM s'effectue via deux flux distincts :

- d'une part les données métier (résultats de test, date, données contextuelles…) qui contiennent un identifiant de corrélation créé par SI-DEP, sont transmises au format CSV, via un flux sécurisé à destination du portail PETRA de la CNAM ;
- d'autre part, un fichier TXT contient l'INS, l'identifiant de corrélation et la date de naissance du patient. Ce fichier est transmis via un flux sécurisé à destination du portail SAFE de la CNAM.

Ces deux flux permettent à la CNAM de reconstituer le jeu de données complet, en ne disposant pour identifier le patient que d'un pseudonyme qu'elle seule est capable de générer [redacted] Ce pseudonyme permettra de relier les résultats de tests pseudonymisés versés dans le *Health Data Hub (HDH)* aux données de recherche présentes dans d'autres systèmes d'information de la CNAM.

À ce jour, un premier envoi de fichiers TXT et CSV à destination respectivement des portails SAFE et PETRA a eu lieu. [redacted]

Il n'a ainsi été possible à la CNAM d'intégrer aucun jeu de données complet en provenance de SI-DEP dans le *HDH* à ce jour. Des correctifs sont en cours de mise en œuvre afin que le flux vers le *HDH* soit fonctionnel.

Les données CSV transmises à PETRA lors de ce premier test ne pourront pas être chaînées avec d'autres données de la CNAM dans la mesure où le fichier TXT contenant le lien entre les INS et identifiants de corrélation a été rejeté et n'existe plus à ce jour.

Les données de résultats de test situées dans SI-DEP étant supprimées au-delà de 92 jours, il n'est plus possible de regénérer le couple fichier TXT et CSV pour les données antérieures à ce délai.

Initialement, les données devaient être transmises une fois par mois au *HDH*. Au vu des contraintes techniques, cette fréquence sera augmentée afin de diminuer le volume de données transféré tout en laissant aux personnes le temps de s'opposer préalablement à la transmission de leurs données au *HDH*.

En ce qui concerne le droit d'opposition

[redacted] *nous informent des éléments suivants :*

Les personnes peuvent s'opposer à ce que leurs données collectées dans SI-DEP soient réutilisées pour les finalités de recherche.

Lorsqu'une personne s'oppose, deux cas de figure se présentent :

- si la personne s'oppose préalablement à la transmission de ses données à la CNAM, ses données ne seront pas extraites ni renseignées dans les fichiers TXT et CSV transmis ;
- si la personne s'oppose postérieurement à la transmission de ses données à la CNAM, l'AP-HP ajoute l'INS de la personne dans un autre fichier TXT à destination de la CNAM afin que celle-ci retrouve et supprime les données de la personne concernée issues de SI-DEP.

Dans les deux cas, l'INS de la personne alimente une liste d'opposition maintenue à jour par l'AP-HP pour éviter toute transmission accidentelle ou ultérieure au *HDH*.

86 personnes ont exercé leur droit d'opposition à ce jour auprès de la DGS.

178 personnes ont exercé leur droit d'accès auprès de la DGS.

En ce qui concerne les durées de conservation

À notre demande, [redacted] effectue des requêtes visant à afficher les données présentes dans SI-DEP selon des filtres basés sur les dates de prélèvement et/ou de dernier compte-rendu.

Mentionnons que la délégation quitte la pièce et demande à [redacted] prenne connaissance de données réelles de patients affichées sans que la délégation n'en prenne connaissance dans un premier temps. [redacted] nous informe de la possibilité de prendre connaissance des données médicales individuelles figurant dans le traitement dans le cadre de la mission de contrôle. Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle [redacted] médecin expert.

[redacted] effectue une requête visant à afficher les lignes pour lesquelles la date de prélèvement se situe entre le 1er février et le 15 juillet 2020.

Constatons la présence de 812 résultats dont le plus ancien affiche une date de prélèvement au 20 février 2020.

[redacted] effectue une requête visant à afficher les lignes pour lesquelles la date de dernier compte-rendu se situe entre le 1er février 2020 et le 21 juillet 2020. Constatons la présence de 469 résultats. Constatons que tous ces résultats présentent une date de prélèvement postérieure au 21 juillet 2020, à l'exception de 3 d'entre eux, datés respectivement des 8, 16 et 17 juillet 2020.

[redacted] *nous informent des éléments suivants :*

La date de dernier compte-rendu est une date saisie par le médecin du laboratoire. Si cette date n'est pas renseignée, le système d'information SI-DEP renseignera une date technique égale à la date de l'intégration de la donnée dans SI-DEP.

[redacted]

[redacted] nous informent ultérieurement aux constatations que les trois résultats des 8, 16 et 17 juillet 2020 observés précédemment sont désormais supprimés : [redacted]

À notre demande, [redacted] effectue une requête visant à afficher les lignes pour lesquelles la date de dernier compte-rendu se situe entre le 1er février 2020 et le 21 juillet 2020, de manière identique à précédemment. Constatons que les trois résultats visés ci-dessus ne sont plus affichés ; que le résultat ayant une date de prélèvement la plus ancienne est daté du 23 juillet 2020.

En ce qui concerne les fichiers traités par l'ETL [redacted]

[redacted] *nous informent des éléments suivants :*

L'interface d'administration de l'outil ETL [redacted] est une interface web [redacted]

[redacted] utilise pour se connecter un compte dénommé [redacted]

À notre demande, [redacted] affiche les fichiers correspondant aux flux à destination de SPF et la DREES, conservés par l'ETL pour des raisons techniques de manière temporaire et documente sa navigation à l'aide de copies d'écran (voir pièces).

Constatons la présence de 7 fichiers à destination de la DREES dont le plus ancien date du 16 octobre 2020.

Constatons la présence de plus de 1,7 millions d'envois à destination de SPF dont le plus ancien date du 16 octobre 2020.

En ce qui concerne les mails transmis au patient suite à la réalisation de tests virologiques

[redacted] nous informent que les courriels invitant les patients à se connecter au portail SI-DEP sont transmis dans deux cas :

- soit le patient a été dépisté positif au COVID-19 suite à son test. Dans ce cas, l'espace de résultat sur l'interface SI-DEP mentionne le résultat positif au test et contient une notice de rappel des consignes sanitaires à destination des personnes positives ;
- soit le prélèvement du patient a été analysé par un laboratoire « site MGI », indépendamment du résultat positif ou non. Dans ce cas, l'espace de résultat sur l'interface SI-DEP contient le compte-rendu d'analyse médicale ainsi que, le cas échéant, la notice de rappel des consignes sanitaires.

[redacted] nous informe qu'environ 25% des résultats intégrés dans SI-DEP proviennent d'analyses réalisées par des « sites MGI ».

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 :

- la procédure de création des trois fichiers transmis à la CNAM pour alimentation du *Health Data Hub* (TXT, CSV et liste d'opposition) (données extraites, structure des fichiers, algorithmes appliqués pour la création d'identifiants de corrélation et de pseudonymes...) accompagnée de fichiers exemples permettant de visualiser la structure ;
- [redacted]
- les annexes des contrats de sous-traitance préalablement transmis à la CNIL relatives à l'encadrement du traitement de données à caractère personnel contenues dans le traitement SI-DEP lorsqu'elles n'ont pas été transmises ;
- le nombre global de résultats intégrés dans SI-DEP depuis le début de sa mise en œuvre ;
- un descriptif des actions en cours ou déjà mises en œuvre suite à la lettre de la Présidente de la CNIL en date du 11 septembre 2020.

Demandons également communication, de manière sécurisée, à destination de [redacted] dans un délai de **8 jours ouvrés**, de la copie des éléments suivants, nécessaire à la rédaction de son rapport :

- un exemple d'export au format CSV de données à destination des administrateurs nationaux de la DRSM.

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

[redacted]

La mission de contrôle s'est terminée, ce jour, à 17 heures 40 ;

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.

PIECE N°1 : [redacted]

PIECE N°2 : [redacted]

PIECE N°3 : [redacted]

PIECE N°4 : [redacted]

PIECE N°5 : [redacted]

Paraphes [redacted]

PIECE N°6 : [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 à la décision de la présidente de la CNIL n° 2020-092C en date du 22 mai 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le Ministre chargé de la santé (Direction générale de la santé) et de tout traitement lié auprès de tout organisme concerné par sa mise en œuvre, aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n° 78-17 du 6 janvier 1978 modifiée et, le cas échéant aux dispositions des articles L. 251-1 et suivants du code de la sécurité intérieure ;

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

En présence du [redacted], médecin expert judiciaire près de la Cour d'appel de Paris, en qualité de médecin expert ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 12 mars 2021, à 9 heures 30, dans les locaux de l'Assistance Publique – Hôpitaux de Paris, situés 33 boulevard Picpus à PARIS (75012) et avons été reçus immédiatement ;

La 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 :

Présentation [redacted] de l'historique de SI-DEP et des flux SI-DEP (voir pièce)

[redacted] nous présente l'architecture générale du traitement SI-DEP ainsi que les interactions avec les systèmes d'information partenaires (voir pièce) et nous informe des éléments suivants :

Depuis novembre 2020, les tests antigéniques réalisés dans les pharmacies sont intégrés dans le dispositif SI-DEP.

La liste des professionnels de santé pouvant alimenter le dispositif SI-DEP a évolué depuis le précédent contrôle de la CNIL effectué dans les locaux de l'AP-HP le 23 octobre 2020. Depuis l'ouverture du portail de saisie des tests antigéniques, 40 000 connexions de professionnels de santé différents ont été constatés, auxquels s'ajoutent 4 500 laboratoires qui alimentent directement SI-DEP (non via le portail CYBERCOVID).

La liste des praticiens habilités à réaliser des examens de dépistage est désormais la suivante : les médecins, les biologistes médicaux, les pharmaciens, les infirmiers, les chirurgiens-dentistes, les sages-femmes et les masseurs-kinésithérapeutes, compte tenu du décret n° 2020-1387 du 14 novembre 2020 et du décret n° 2020-1514 du 3 décembre 2020.

Depuis le 27 janvier 2021, les tests salivaires ainsi que des informations relatives aux variants sont remontés dans le dispositif le SI-DEP.

Depuis le contrôle du 23 octobre 2020 de la CNIL, le décret n° 2020-1387 du 14 novembre 2020 prévoit un nouveau destinataire des données issues de SI-DEP : le Service Public d'Information en santé (« SPIS »), entité rattachée au Ministère de la Santé. Le SPIS reçoit des données relatives aux professionnels de santé enregistrées dans SI-DEP. L'objet de ce transfert est de permettre une cartographie de l'offre de soins à destination de la population. Cette cartographie est disponible sur le site Internet « santé.fr ».

[redacted] nous liste les principales modifications apportées par le décret du 14 novembre 2020 au décret n° 2020-551 du 12 mai 2020. Celles-ci portent notamment sur l'ajout du code postal du lieu dans lequel la personne envisage de séjourner dans les 7 jours suivants la réalisation du dépistage, sur l'ajout aux examens de dépistage des mentions « virologique ou sérologique », sur une reformulation de la mention concernant le QR Code à l'article 9, par l'ajout du SPIS à l'article 10.4 du décret n° 2020-551 du 12 mai 2020 et sur

l'ajout de la mention « dans les conditions prévues aux articles 28 à 31 du règlement (UE) du 27 avril 2016 susvisé » concernant la sous-traitance.

En ce qui concerne le flux de données à destination de la CNAM dans le cadre des transferts vers le Health Data Hub

[redacted] nous informent que les objectifs et les modalités de transferts actés au PV n° 2020-092/6 du 23 octobre 2020 restent inchangés.

L'objectif de ce flux de données est d'alimenter le Health Data Hub afin de fournir aux chercheurs un accès aux données à des fins de recherche. Ces données sont pseudonymisées par la CNAM afin de permettre un chaînage avec d'autres données de la CNAM, dont celles du système national des données de santé (SNDS).

La transmission des données à la CNAM s'effectue via deux flux distincts :

- d'une part les données métier (résultats de test, date, données contextuelles…) qui contiennent un identifiant de corrélation créé par SI-DEP, sont transmises au format CSV, via un flux sécurisé à destination du portail PETRA de la CNAM ;
- d'autre part, un fichier texte contient l'INS, l'identifiant de corrélation et la date de naissance du patient. Ce fichier est transmis via un flux sécurisé à destination du portail SAFE de la CNAM.

Ces deux flux permettent à la CNAM de reconstituer le jeu de données complet, en ne disposant pour identifier le patient que d'un pseudonyme qu'elle seule est capable de générer [redacted]

Initialement, en raison de dysfonctionnements techniques, les transferts vers la CNAM à destination du Health Data Hub ont été réalisés de façon sporadique avec occasionnellement des ratés.

Depuis le 21 décembre 2020, les transferts vers la CNAM à destination du Health Data Hub sont pleinement opérationnels. Des données sont envoyées tous les quinze jours [redacted]. Ces données sont générées automatiquement toutes les deux semaines et mis à disposition via une plateforme sécurisée d'échange de fichiers [redacted] gérée par l'AP-HP. Les fichiers restent disponibles pendant une semaine sur la plateforme [redacted] au cas où il serait nécessaire de reproduire l'envoi d'un des fichiers vers la CNAM en raison d'un dysfonctionnement.

À notre demande, [redacted] nous présente les interfaces des outils SAFE, PETRA et [redacted] SE [redacted] documente sa navigation au moyen de captures d'écran. Il nous informe que seul lui-même et son collègue ont accès aux interfaces des outils SAFE et PETRA afin d'y déposer les fichiers extraits de SI-DEP.

[redacted] *nous informe que :*

[redacted]

[redacted]

[redacted]

Immédiatement après avoir procédé aux envois [redacted] nous informe qu'il supprime les fichiers de son ordinateur et vide sa corbeille.

Les transferts depuis la CNAM vers le Health Data Hub ne sont pas encore opérationnels, selon les informations communiquées par la CNAM.

En ce qui concerne les flux de données à destination des partenaires de SI-DEP

[redacted] nous informent que les objectifs et les modalités de transferts à destination de la CNAM, de Santé Publique France et de la DREES actés au PV n° 2020-092/6 du 23 octobre 2020 restent inchangés.

Des données pseudonymisées sont transmises à Santé publique France (SPF) et à la Direction de la recherche, des études, de l'évaluation et des statistiques (DREES). Les pseudonymes utilisés au sein de ces flux permettent de comptabiliser une seule fois chaque patient.

Depuis le contrôle du 23 octobre 2020 de la CNIL, le décret n° 2020-1387 du 14 novembre 2020 prévoit un nouveau destinataire des données issues de SI-DEP : le Service Public d'Information en santé (« SPIS »), entité rattachée au Ministère de la Santé.

Des transferts quotidiens sont réalisés vers le SPIS, [redacted] Ce fichier contient, pour chaque test réalisé, le numéro d'identifiant RPPS ou FINESS du professionnel ou du laboratoire, le code LOINC correspondant au geste médical réalisé (test RT-PCR, test antigénique, test sérologique…) et la date de la réalisation du geste médical.

Ces transferts vers le SPIS ne concernent pas les données des patients et n'incluent pas les résultats des tests.

En ce qui concerne les nouveaux professionnels de santé autorisés à réaliser des examens de dépistage et en particulier les tests antigéniques effectuées en pharmacies

[redacted] nous informe que les modalités techniques d'intégration et d'accès aux données SI-SEP sont réalisées par les professionnels de santé au travers du portail applicatif CYBERCOVID. Seul l'interfaçage avec la carte professionnelle de santé (CPS) ou sa version dématérialisée (e-CPS) ont nécessité un développement spécifique pour permettre l'authentification des professionnels.

Des tests antigéniques sont remontés par les laboratoires au moyen des interfaces déjà existantes, opérées pa[redacted]

[redacted] *nous informe des éléments suivants :*

Les professionnels de santé se connectent au portail SI-DEP de l'AP-HP soit au moyen de leur carte professionnelle de santé (carte CPS via un lecteur de carte physique) soit via leur e-CPS. Dans ce dernier cas, il s'agit d'une carte CPS dématérialisée enregistrée dans une application mobile permettant ainsi de n'avoir à faire usage du lecteur de carte physique. [redacted]

Les modalités d'authentification sont décrites dans un tutoriel vidéo adressé à l'ensemble des professionnels de santé qui alimentent SI-SEP depuis novembre 2020 (voir pièce). Ce tutoriel décrit également la saisie des données patients dans CYBERCOVID.

Ce tutoriel fait partie d'un « Kit » d'information « Guide SI-DEP » adressé à l'ensemble des professionnels des santé comprenant également un rappel sur la règlementation RGPD. Ce guide contient des modèles de mentions d'information à destination des professionnels de santé ayant pour objet d'informer les personnes testées. Il comporte également des mentions d'information « RGPD » à destination des professionnels de santé concernant le traitement de de leurs propres données.

Les informations relatives à la protection des données sont également portées à la connaissance des personnes testées dans le compte-rendu détaillant le résultat du test.

Une campagne d'information a été menée par la DGS auprès des nouveaux professionnels de santé autorisés à tester et à renseigner SI-DEP. Cette campagne a été réalisée par courriel et visioconférence à destination des ordres et des syndicats représentatifs des professions concernées. Des messages d'information sont régulièrement envoyés depuis novembre 2020 en cas de mise à jour.

L'ensemble de ces informations sont également disponibles sur le portail CYBERCOVID. À chaque connexion du professionnel à l'application à CYBERCOVID, une page d'accueil « Bienvenue dans SI-DEP » s'affiche. Constatons que cette page comporte un lien vers le tutoriel SI-DEP et une mention qui rappelle « *n'hésitez pas à afficher et/ou remettre au patient le contenu de la section « Système d'information relatif au dépistage de la population » en annexe du tutoriel* ».

[redacted] présente à la délégation, au moyen du tutoriel vidéo, les champs pouvant être renseignés par le professionnel de santé dans le portail CYBERCOVID (voir pièce).

L'INS n'est pas un champ présent dans le portail CYBERCOVID. Le professionnel de santé ne le renseigne pas dans le portail CYBERCOVID. L'INS de la personne testée est intégré dans SI-SEP au moyen du téléservice INSi de la CNAM qui permet de le récupérer.

En ce qui concerne les habilitations pour l'accès à la base SI-DEP

À notre demande, [redacted] se connecte à l'interface de l'outil CYBERCOVID de l'environnement de qualification contenant des données fictives au moyen d'un compte utilisateur disposant du profil d'utilisateur [redacted] et nous présente les différents écrans et données accessibles et documente sa navigation à l'aide de captures d'écran.

Ce profil s'adresse aux médecins, pharmaciens et personnes sous l'autorité de ces derniers, chirurgiens-dentistes, masseurs kinésithérapeutes, sages-femmes et infirmiers libéraux. Ce

profil permet de saisir un nouveau dossier, de rechercher et de finaliser un dossier existant. Un professionnel ne peut consulter et modifier que les dossiers et les profils de patients qu'il aura lui-même créés dans le système.

Un professionnel de santé peut laisser un dossier incomplet pour revenir le finaliser plus tard, par exemple pour renseigner le résultat d'un test. Une fois le résultat du test renseigné, la fiche est complète et ne peut plus être modifiée.

Lorsqu'il crée une fiche pour un patient sur l'interface de CYBERCOVID, seuls les nom, prénom, sexe et date de naissance sont enregistrés. Seul le professionnel de santé qui a créé la fiche peut la consulter par la suite.

Ce profil ne propose pas de fonction d'export de données.

En ce qui concerne les durées de conservation des données

[redacted] accède à l'interface de production de CYBERCOVID.

La délégation est informée que la durée de conservation de 92 jours pour les données présentes dans SI-DEP se compte à partir de la date de prélèvement lors du test.

À notre demande, [redacted] effectue une requête visant à afficher les lignes pour lesquelles la date de prélèvement se situe entre le 1er février 2020 et le 9 décembre 2020.

Mentionnons que la délégation quitte la pièce et demande à ce que [redacted] prenne connaissance de données réelles de patients affichées sans que la délégation n'en prenne connaissance dans un premier temps. [redacted] nous informe de la possibilité de prendre connaissance des données médicales individuelles figurant dans le traitement dans le cadre de la mission de contrôle. Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle [redacted], médecin expert.

Mentionnons que [redacted] a veillé au masquage des données nominatives apparaissant dans les résultats.

Constatons la présence de 25 résultats. Les dates d'intégration dans SI-DEP de ces résultats datent du 12 mars 2021, et [redacted] nous informe qu'ils seront supprimés lors de la prochaine purge quotidienne. [redacted] nous informe que ces résultats correspondraient à des erreurs de saisie ou des intégrations tardives de la part des professionnels.

En ce qui concerne les tests salivaires

[redacted] *nous informe des éléments suivants :*

Les prélèvements de tests salivaires peuvent être effectués, par exemple, dans des établissements scolaires, dans le cadre de campagne de dépistage massif. Ces tests salivaires sont analysés par des laboratoires d'analyse. Les résultats du test et les données de la personne testée sont intégrés dans le dispositif SI-DEP par les laboratoires selon les mêmes modalités usuelles déjà décrites lors des précédents contrôles de la CNIL. La seule différence porte sur la description de l'acte, c'est-à-dire, que l'acte est codifié selon la norme LOINC, qui va indiquer qu'il s'agit d'un test salivaire.

Le personnel qui effectue les prélèvements en établissement scolaires n'ont pas accès à CYBERCOVID.

En ce qui concerne les observations formulées dans les courriers de suivi du 11 septembre 2020 et du 18 janvier 2021

[redacted] *nous informe des éléments suivants :*

Les données à destination de la CNAM pour la finalité de suivi des contacts sont transmises via l'outil « ETL [redacted] ». Des évolutions ont été réalisées avec [redacted] r le sujet des comptes partagés utilisés pour accéder à cet outil. Il existait ainsi deux comptes partagés génériques (« supervision » et « exploit »). Le compte « supervision » est maintenu en l'état dans la mesure où seul un automate [redacted] destiné à la supervision du bon fonctionnement de SI-DEP l'utilise.

Le compte générique « exploit » utilisé pour accéder à l'interface « ETL [redacted] et constaté lors du contrôle du 23 octobre 2020 a été désactivé par l'AP-HP et n'est plus utilisé. Des comptes nominatifs ont été créés dans l'outil « ETL [redacted] ».

Par ailleurs des travaux sont en cours avec [redacted] pour déléguer la gestion des comptes dans l'Active Directory. [redacted] a prévu de livrer ces travaux fin mars, et dès la qualification, l'AP-HP procèdera à l'implémentation.

La journalisation des accès à la base SI-DEP par les administrateurs a été configurée dans le système. Son déploiement nécessite le redémarrage de la base de données SI-DEP. Ce redémarrage interviendra le dimanche 14 mars 2021 dans le cadre de la mise en œuvre du plan de reprise d'activité.

Les habilitations des personnes en charge du support téléphonique ont été réévaluées de telle sorte qu'elles ne disposent plus de droits excessifs au regard de leur mission.

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 :

- le nombre total de tests réalisés enregistrés dans le dispositif SI-DEP depuis sa mise en œuvre, en distinguant les tests PCR et les tests antigéniques ;
- le nombre total de résultats de tests intégrés dans le dispositif SI-DEP depuis sa mise en œuvre ;
- indiquer le nombre de personnes ayant exercé leur droit d'accès ;
- indiquer le nombre de personnes ayant exercé leur droit d'opposition ;
- l'analyse d'impact sur la protection des données mise à jour ;
- des fichiers de test complets utilisés dans le cadre de la préparation des transferts vers la CNAM au travers des interfaces de SAFE et de PETRA ;
- un extrait de dix lignes du fichier de données transmis au SPIS ;
- une copie du premier email et de la dernière communication adressés chacun des ordres et des syndicats représentatifs ainsi que le nombre de campagne d'information réalisée depuis novembre 2020 ;
- les modalités d'information des représentants légaux et des élèves sur le dispositif « SI-DEP » lors des campagnes de dépistage par tests salivaires ;

- des informations complémentaires sur les éventuels échanges que la DGS a pu avoir avec les acteurs intervenant dans la mise en œuvre de ces campagnes salivaires (notamment, les ARS, l'Éducation nationale…) ;
- un récapitulatif des actions entreprises s'agissant des observations formulées dans les courriers de suivi du 11 septembre 2020 et du 18 janvier 2021 ;

Demandons également communication, de manière sécurisée, à destination de [redacted] dans un délai de **8 jours ouvrés**, de la copie des éléments suivants, nécessaire à la rédaction de son rapport :

- des extraits d'une centaine de lignes de fichiers transmis à la CNAM dans le cadre des envois vers le Health Data Hub au travers des interfaces de SAFE et de PETRA ;

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

[redacted]

La mission de contrôle s'est terminée, ce jour, à 20 heures 15 ;

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.

PIÈCE N°1 : [redacted]

- [redacted]

PIÈCE N°2 : [redacted]

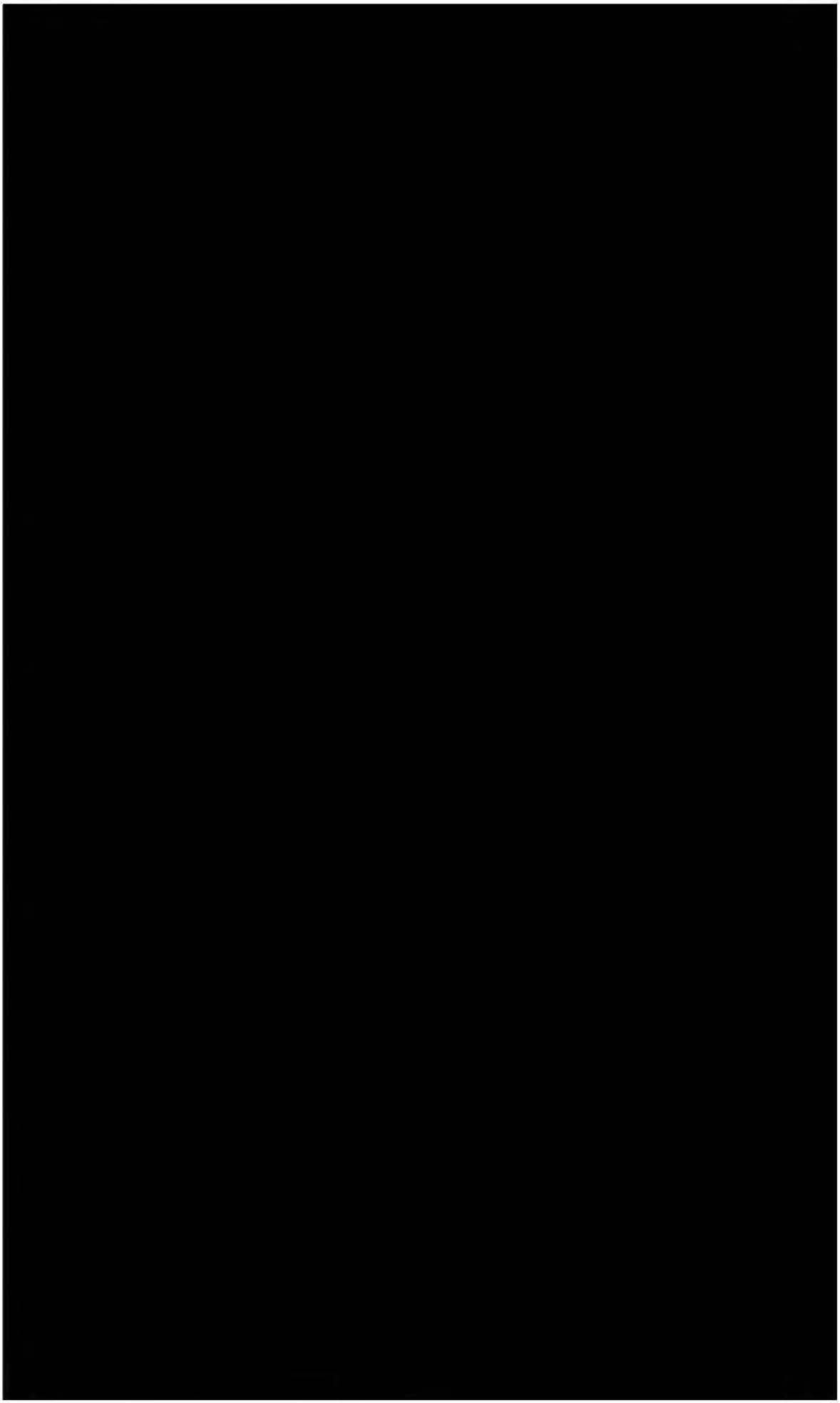
- [redacted]

 Paraphes [redacted]

- [redacted]

PIÈCE N°3 : [redacted]

- [redacted]



- [redacted]

PIÈCE N°4 : [redacted]

PIÈCE N°5 : [redacted]

PIÈCE N°6 : [redacted]

PIÈCE N°7 : [redacted]

PIÈCE N°8 : [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 le sarticles 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° 2020-092C en date du 22 mai 2020, la mission de vérification a eu pour objet de procéder à la vérification sur place de la conformité du traitement de données à caractère personnel dénommé « SI-DEP » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le Ministre chargé de la santé (Direction générale de la santé) et de tout traitement lié auprès de tout organisme concerné par sa mise en œuvre, aux dispositions du règlement (UE) 2016/679 susvisé et de la loi n° 78-17 du 6 janvier 1978 modifiée et, le cas échéant aux dispositions des articles L. 251-1 et suivants du code de la sécurité intérieure ;

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

Le procureur de la République territorialement compétent préalablement informé ;

La déléguée à la protection des données [redacted] a été préalablement informé du contrôle par appel téléphonique et courriel le 22 septembre 2021.

Nous sommes présentés le 28 septembre 2021, à 9 heures 30, dans les locaux de AP-HP, situés 33 boulevard Picpus 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 et des modalités 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 :

Mentionnons que le ministère des Solidarités et de la Santé a notifié une violation de données personnelles le 15 septembre 2021 à la CNIL, ayant pour référence FR2109151400003. Cette violation de données concerne des données issues du dispositif « SI-DEP », pour lequel l'AP-HP agit en qualité de sous-traitant pour le compte du ministère des Solidarités et de la Santé.

En ce qui concerne les envois de données vers la CNAM et la plateforme d'échange de fichiers de l'AP-HP dénommée « [redacted] *nous informe des éléments suivants :*

Une présentation de la violation de données est faite à la délégation (cf. pièces).

Dans le cadre du *contact tracing*, les résultats des tests de dépistage, positifs et négatifs, sont transmis à la CNAM de façon régulière.

Depuis la mise en place du dispositif « SI-DEP » (mai 2020), jusqu'à la fin du mois de septembre 2020, la CNAM disposait d'un accès sécurisé à SI-DEP pour récupérer chaque jour la liste des tests réalisés, dans le cadre du *contact tracing*.

En septembre 2020, l'augmentation du nombre de tests réalisés quotidiennement (près d'un million de test par jour, contre les 750 000 tests par semaine initialement prévus en mai 2020) oblige l'AP-HP à mettre en place un canal chiffré et sécurisé de transmission des données vers la CNAM.

Cela se matérialise à partir du 12 octobre 2020, avec la mise en route des envois automatiques à destination de la CNAM, via l'ETL « [redacted]

Jusqu'au 10 juillet 2021, en cas de dysfonctionnement des envois des données issus de SI-DEP vers la CNAM à des fins de *contact tracing*, la plateforme [redacted] était utilisée comme solution de secours pour la transmission rapide des données à la CNAM.

La solution [redacted] était également utilisée comme solution de partage au sein de l'équipe « SI-DEP » afin d'analyser précisément les incidents remontés par la CNAM et la DNUM. Cette solution a été accepté par l'ensemble des partenaires du projet, dont la CNAM, la DGS et la DNUM (DSI du ministère des Solidarités et de la Santé).

Depuis cette date, le processus d'envoi automatisé des données vers la CNAM est suffisamment rodé pour ne plus nécessiter l'utilisation de la plateforme [redacted] comme solution de secours.

Une présentation de la plateforme [redacted] est faite à la délégation (voir pièces).

La plateforme [redacted] est un espace sécurisé d'envoi et de partage de documents. Cette plateforme est éditée par la société [redacted] Elle est utilisée au sein de l'AP-HP depuis 2015. Les données de la plateforme [redacted] sont hébergées sur les serveurs de l'AP-HP. Il y a environ 10 000 personnes ayant un compte utilisateur sur la plateforme [redacted]

L'éditeur du logiciel intervient de manière ponctuelle sur la plateforme [redacted] et uniquement à la demande de l'AP-HP pour les besoins de support.

La plateforme [redacted] n'a pas fait l'objet d'un audit de sécurité dédié depuis son déploiement en 2015. Des tests d'exposition sur internet sont effectués régulièrement par l'ANSSI, depuis septembre 2020, et par l'AP-HP, visant à mettre en évidence des vulnérabilités sur un certain nombre d'URL et d'adresses IP gérées par l'AP-HP, dont celles de [redacted]

Huit analyses ont été réalisées par l'ANSSI depuis le début de l'année 2021, sur une base mensuelle. Depuis le 26 août 2021, l'AP-HP procède elle-même à des analyses sur une base hebdomadaire. Dans ce cadre, elle utilise l'outil [redacted]

Aucune alerte critique n'a jamais été signalée sur la plateforme [redacted] dans le cadre de ces tests d'exposition, à l'exception de deux alertes mineures signalées par l'outil [redacted] signalées le 26 août 2021. Ces vulnérabilités ont été remontées à l'éditeur pour correction.

Les mises à jour de la plateforme [redacted] sont généralement implémentées par l'AP-HP dans les trente jours suivant leur mise à disposition, sauf correctif de sécurité critique qui sont installés immédiatement.

Avant le 10 juillet 2021, lorsque l'utilisation de [redacted] était nécessaire dans les conditions décrites précédemment, un agent des équipes « SI-DEP » de l'AP-HP procédait à une extraction des données issues de SI-DEP. Il déposait le fichier ainsi extrait sur son espace personnel sur la plateforme [redacted] Il générait un lien de partage public, par ailleurs protégé par un code d'accès, qu'il communiquait à la CNAM.

Ce lien avait une durée de validité de sept jours, et les agents avaient pour consigne de supprimer les extraits de données dès leur bonne réception par la CNAM.

[redacted]

La plateforme [redacted] a également été utilisé dans le cadre de l'envoi des données vers la CNAM, pour la transmission au « Health Data Hub » du 21 décembre 2020 à 10 mai 2021.

Aujourd'hui, [redacted] n'est plus utilisée dans le cadre d'envoi de données vers des destinataires de SI-DEP. Il n'est toutefois pas exclus d'utiliser la solution en cas d'incident majeure, en faisant appel à un surchiffrement au moyen d'un conteneur Zed.

En ce qui concerne l'origine de la faille de sécurité

[redacted] *nous informe des éléments suivants :*

Le 22 juin 2021 à 16 heures 59, le logiciel [redacted] a été mis à jour.

Le 22 juin 2021, à 20 heures 36, un lien de consultation publique vers une communication « DGS URGENT », ayant une durée de validité de trente jours, a été partagé auprès des professionnels de santé par un agent de l'équipe « SI-DEP ».

Le 25 juin 2021, la communication « DGS URGENT » a été supprimée de l'espace de partage par la même personne de l'équipe « SI-DEP », avant l'expiration du lien.

La montée de version du 22 juin 2021 a introduit une faille de sécurité dans le logiciel [redacted] Ainsi, l'accès à un lien « orphelin » (c'est-à-dire vers un document supprimé) donnait accès à l'ensemble du répertoire de la personne ayant partagé le document en premier lieu.

La personne ayant partagé le document « DGS URGENT » avait procédé à des extractions de données de SI-DEP et à leur partage vers la CNAM, dans le cadre du fonctionnement décrit précédemment des envois dans le cadre du *contact tracing* et du diagnostic de dysfonctionnement, et n'avait pas procédé à leur suppression à la suite de ces opérations.

Cette vulnérabilité décrite ci-dessus n'avait pas été détectée par l'éditeur de la plateforme [redacted] depuis la sortie de la version l'ayant introduite en avril 2021.

Du 29 juin au 20 juillet 2021, des accès aux fichiers contenus dans le répertoire [redacted] de l'agent ayant partagé le document « DGS URGENT » sont constatés. Cette analyse a été réalisée à la suite de la violation de données, sur la base des journaux d'utilisation de la plateforme [redacted]

378 fichiers ont ainsi été rendus disponibles par cette faille de sécurité. La majorité sont des documents de travail liés au projet SI-DEP, et quatorze fichiers contiennent des données à caractère personnel issues de SI-DEP.

Les données compromises en ce qui concerne les personnes testées sont notamment le nom, le prénom, la date de naissance, le numéro de sécurité sociale, le sexe, le numéro de téléphone, l'adresse de courrier électronique, le résultat du test et le lieu du test. Pour les professionnels de santé ayant réalisé des tests, seul le numéro RPPS a été diffusé. Les fichiers étaient au format CSV, XLSX (Excel) et HPR.

Tous ces fichiers ne contiennent pas l'ensemble de ces données. Sur l'ensemble des fichiers compromis, il s'y trouvait 352 198 numéros de sécurité sociale différents.

Les fichiers compromis par la violation de données ont été générés par l'AP-HP et ont été déposés sur la plateforme [redacted] aux mois d'août et septembre 2020, et correspondent à des tests réalisés pendant cette même période.

Les quatorze fichiers contenant des données issues de SI-DEP représentent en tout 8 404 988 lignes, correspondant à 1 571 391 personnes uniques.

[redacted]

Le dédoublonnage s'est fait sur la base de la combinaison du nom, du prénom, du sexe et de la date de naissance des personnes.

Il n'y a pas eu de comptage du nombre de professionnels de santé concernés par la violation de données, le ministère des Solidarités et de la Santé ayant donné la priorité au comptage des données des patients.

En ce qui concerne les mesures prises à la suite de la violation
[redacted] *ous informe des éléments suivants :*

Le 9 septembre 2021 à 17 heures 56, l'ANSSI, via CERT-FR, informe l'AP-HP, ainsi que le FSSI du ministère des Solidarités et de la Santé et le CERT-SANTÉ de l'ANS d'une fuite de données de plusieurs gigaoctets sur le site web [redacted]

L'AP-HP a eu confirmation de la fuite de données le 12 septembre 2021 au soir, et en a informé la DGS le 13 septembre 2021.

À partir du 13 septembre 2021, les accès à [redacted] depuis internet ont été coupés et les mots de passe des agents « SI-DEP » ont été modifiés.

Le 14 septembre 2021, les données ont été supprimées du site web [redacted] à la demande de l'ANSSI.

Le 15 septembre 2021, l'AP-HP et la DGS ont déposé chacun une plainte en justice, et le ministère des Solidarités et de la Santé a notifié la CNIL de la violation de données.

Le 18 septembre 2021, après trois jours d'expertise, l'éditeur [redacted] a informé l'AP-HP de l'existence de la vulnérabilité à la suite de l'analyse des journaux de la plateforme [redacted] de l'AP-HP. Ces journaux ont une durée de rétention de 90 jours.

Le 19 septembre 2021, un script a été exécuté pour supprimer les liens orphelins.

Le 21 septembre 2021, un patch de correction de la vulnérabilité a été appliqué sur la plateforme [redacted] de l'AP-HP. Ce patch a été diffusé auprès de l'ensemble des clients de la société [redacted]

L'accès à [redacted] depuis internet a été rétabli le même jour, à la suite de l'application du patch correctif et vérification de son effectivité.

Une revue des répertoires personnels sur [redacted] des agents travaillant sur SI-DEP a été réalisée de manière à mettre en évidence la présence de fichiers issus de SI-DEP. Quelques fichiers ont été identifiés dans ce contexte et immédiatement supprimés.

Des mesures organisationnelles ont été prises par l'AP-HP, visant notamment à alerter les équipes travaillant sur SI-DEP de la nécessité de supprimer les fichiers en temps utile de la plateforme [redacted]

Un courrier électronique a été adressé par le DSI de l'AP-HP à l'ensemble des utilisateurs AP-HP de la plateforme [redacted] afin de les sensibiliser sur les bonnes pratiques de sécurité dans le cadre de l'utilisation de la plateforme [redacted]

[redacted]

Il est prévu de passer en revue l'ensemble des comptes utilisateurs de la plateforme [redacted] afin de s'assurer que la vulnérabilité n'a pas été exploité via d'autres liens orphelins créés pendant la période d'exposition.

Une mise à jour de la notification de la violation de données à la CNIL est prévue prochainement.

L'ANSSI conduit actuellement un audit lié à la violation de données et n'a pas encore produit de rapport à ce stade.

L'AP-HP a par ailleurs prévu de faire appel à la société [redacted] afin de réaliser un audit d'architecture et un test d'intrusion sur la plateforme [redacted] Un cahier des charges pour cet audit va être réalisé d'ici à la fin de la semaine.

[redacted]

Des réunions de crise ont été organisées avec les différents acteurs intervenant dans la gestion de la crise sanitaire afin d'identifier d'éventuels risques pour l'intégrité des différents traitements. En particulier, il n'est pas apparu de risques spécifiques pour la production des passes sanitaires, des QR codes « SI-DEP » ou pour la sécurité des comptes « Ameli » des personnes.

L'AP-HP a transmis à la CNAM la liste des numéros de sécurité sociale concernées par la violation pour permettre à la CNAM de prendre les mesures de protection appropriées.

En ce qui concerne l'information des personnes

[redacted] *nous informent des éléments suivants :*

Le 17 septembre 2021, l'AP-HP a publié un communiqué de presse sur son site web, qui a été envoyé à l'Agence France-Presse ainsi qu'à plusieurs médias.

Une campagne d'information par courrier électronique et par courrier postal a été lancé auprès des personnes testées le 17 septembre 2021. À ce jour, 853 902 courriers électroniques ont été envoyés aux personnes dont l'adresse électronique apparaissait dans les fichiers.

La campagne d'information par courrier postal a été lancé le 23 septembre 2021. En tout, 475 544 courriers ont été envoyés.

La campagne d'information par courrier électronique et par courrier postal doit s'achever d'ici à la fin de la semaine.

Le ministère des Solidarités et de la Santé n'a pas estimé qu'il était nécessaire d'informer les professionnels de santé, en raison du risque estimé comme restreint pour eux. Le ministère des Solidarités et de la Santé s'est appuyé sur la grille d'analyse proposée par la CNIL relative à l'obligation ou non d'informer les personnes concernées par une violation de données personnelles.

[redacted]

En ce qui concerne les constats sur l'interface

À notre demande, accède à la plateforme Il nous informe avoir créé un compte utilisateur pour les besoins du contrôle, et nous précise que ce compte présente des droits identiques à ceux de n'importe quel utilisateur de la plateforme. Il documente sa navigation au moyen de captures d'écran.

nous informe des éléments suivants :

La plateforme a fait l'objet d'un patch correctif visant à supprimer la vulnérabilité à l'origine de la violation de données.

Constatons que l'accès à la plateforme nécessite la saisie d'un nom d'utilisateur et d'un mot de passe.

L'accès à se fait à partir des utilisateurs présents dans l'Active Directory de l'AP-HP.

Pour les besoins du contrôle, procède au téléversement de plusieurs fichiers dans

Constatons qu'il existe la possibilité de partager les documents, soit au moyen d'un droit accordé à un utilisateur de soit au moyen de liens de partage publics. Ces liens de partage peuvent permettre d'accéder directement aux documents, ou peuvent nécessiter la saisie d'un code d'accès généré par la plateforme.

crée un lien de partage public, sans code d'accès, pour un des documents du répertoire (ci-après « document 1 »).

crée un lien de partage public, avec code d'accès, pour un autre document du répertoire (ci-après « document 2 »).

Constatons que la plateforme invite l'utilisateur à transférer le lien de partage par courrier électronique.

supprime le document 1 du répertoire

accède au lien de partage public précédemment généré pour le document 1.

Constatons l'affichage d'un message d'erreur dans le navigateur.

supprime le document 2 du répertoire

[redacted] accède au lien de partage public précédemment généré pour le document 2.

Constatons l'affichage d'un message d'erreur dans le navigateur.

Nous sommes informés que dans le cadre des envois vers la CNAM pour le *contact tracing*, le code d'accès était transmis dans un courrier électronique distinct de celui contenant le lien de partage.

Lorsqu'un utilisateur supprime un document de son répertoire [redacted] celui-ci est déplacé vers une corbeille temporaire de [redacted] où il reste accessible pendant trente jours avant d'être supprimé définitivement de façon automatique.

L'AP-HP ne dispose pas des droits pour supprimer les fichiers contenus dans la corbeille.

Précisons n'avoir jamais accédé à des données médicales individuelles durant la mission de contrôle.

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 :

1) les consignes adressées aux équipes « SI-DEP » relative à la suppression des extractions issues de SI-DEP sur la plateforme [redacted], avant la violation de données ;
2) l'information si le ministère des Solidarités et de la Santé a réalisé des audits de l'AP-HP en tant que sous-traitant du traitement « SI-DEP », et le dernier rapport d'audit le cas échéant ;
3) le registre des violations de données de la DGS ;
4) la catégorie et la volumétrie des destinataires de la communication « DGS URGENT ».

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

[redacted]

La mission de contrôle s'est terminée, ce jour, à 20 heures ;

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

[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.

PIECE N°1 : [redacted]

- [redacted]

PIECE N°2 : [redacted]

- [redacted]

PIECE N°3 : [redacted]

- [redacted]

PIECE N°4 : [redacted]

- [redacted]

- [redacted]

PIECE N°5 : [redacted]

- [redacted]
- [redacted]
- [redacted]

PIECE N°6 : [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

PIECE N°7 : [redacted]

- [redacted]
- [redacted]
- [redacted]

PIECE N°8 : [redacted]

PIECE N°9 : [redacted]

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

Paraphes [redacted]

[redacted]

[redacted]
Expert près la Cour d'appel de Paris
[redacted]
75016 PARIS

Paris, le 22 Juillet 2020

Assistance médicale au contrôle du 3 juillet 2020 de 9 h à 19 h dans les locaux du site Broussais de l'AP-HP, situé 8 rue Maria Héléna Vieira Da Silva Paris 14 ème

Suite à décision de la Présidente de la CNIL N° 2020-092 C du 22 mai 2020

Le 9 juillet il m'a été transmis par [redacted] par mail sécurisé 5 captures d'écrans.

1 ère capture d'écran : [redacted]

Ce tableau contient 457 lignes et 18 colonnes dont 10 ne sont pas remplies

[redacted]

Remarques :

[redacted]

2 -ème copie d'écran notée : [redacted]

[redacted]

3 -ème capture d'écran noté

Il y a 5 pages différentes

Dans cette capture d'écran il n'apparaît donc que les noms et prénoms des patients, aucun autre élément d'identification n'apparaît (âge, date de naissance, adresse, sexe)

4 -ème capture d'écran notée [redacted]

Il y a 6 écrans différents

[redacted]

Remarques :

[redacted]

[redacted]

5 -ème Capture d’écran noté

Fin de la visualisation de la capture d'écran

SYNTHESES :

De l'étude de l'ensemble des écrans vus, il ressort de nombreux éléments codés.

La date et l'heure précises du prélèvement sont mentionnées, ainsi que le lieu de prélèvement.

La date et heure du rendu des résultats sont aussi mentionnées.

Une question est de savoir si avec ces codes, la personne qui a effectué le prélèvement peut être identifiée.

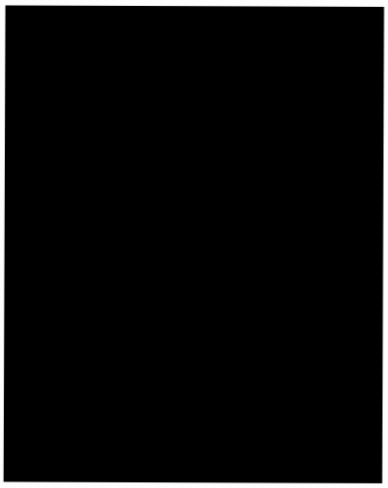
Il est mentionné de façon claire, le nom et le prénom des patients, la date de naissance ainsi que le sexe.

Il y a également les coordonnées personnelles sous forme de téléphone portable et d'adresse mail.

Les seuls éléments médicaux connus sont déclaratifs, à savoir si le patient est symptomatique ou asymptomatique.

Il ne ressort donc aucun autre élément médical en particulier de pathologie associée ou de prise de traitement médicamenteux.

Il est enfin à noter qu'il semble que différents intervenants aient accès à l'ensemble des tableaux, à savoir l'administrateur, le biologiste et le préleveur, justifiant de s'assurer du respect du secret médical.



CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

MINISTERE DES SOLIDARITES ET DE LA SANTE
MONSIEUR LE MINISTRE
14, AVENUE DUQUESNE
75350 – PARIS 07 SP

Paris, le 30 juillet 2020

N/Réf : [redacted]/Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 1372 7

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place au sein des locaux de la société [redacted] situés [redacted]

En application de l'article 31 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie de la décision et de l'ordre de mission relatifs à ce contrôle ainsi que du procès-verbal établi 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° 2020-092C
Ordre de mission
Procès-verbal n° 2020-092/4

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

ASSISTANCE PUBLIQUE HOPITAUX DE PARIS
MONSIEUR LE DIRECTEUR GENERAL
3, AVENUE VICTORIA
75004 PARIS

Paris, le 30 OCT. 2020

N/Réf : [redacted]Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 1527 1

Monsieur le Directeur général,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place au sein des locaux de l'Assistance publique – Hôpitaux de Paris situés 33, boulevard Picpus à PARIS (75012).

En application de l'article 31 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie de la décision et de l'ordre de mission relatifs à ce contrôle ainsi que du procès-verbal établi 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 Directeur général, mes salutations distinguées.

[redacted]

P.J. : Décision n° 2020-092C
Ordre de mission
Procès-verbal n° 2020-092/6

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

MINISTERE DES SOLIDARITES ET DE LA SANTE
MONSIEUR LE MINISTRE
14, AVENUE DUQUESNE
75350 – PARIS 07 SP

Paris, le 30 OCT. 2020

N/Réf : [redacted]/Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 1530 1

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place au sein des locaux de l'Assistance publique – Hôpitaux de Paris situés 33, boulevard Picpus à PARIS (75012).

En application de l'article 31 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie de la décision et de l'ordre de mission relatifs à ce contrôle ainsi que du procès-verbal établi 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° 2020-092C
Ordre de mission
Procès-verbal n° 2020-092/6

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

MINISTERE DES SOLIDARITES ET DE LA SANTE
MONSIEUR LE MINISTRE
14, AVENUE DUQUESNE
75350 – PARIS SP 07

Paris, le 24 SEP. 2020

N/Réf : [redacted]**CS201032**
Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 1330 7

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé, le 3 juillet 2020, à un contrôle sur place dans les locaux de l'Assistance Publique des Hôpitaux situés 8, rue Maria Héléna Vieira Da Silva (Hôpital Broussais) à PARIS (75014), dans le cadre de la procédure de contrôle n° 2020-092C « SI-DEP ».

En application de l'article 36 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie du rapport d'expertise établi dans le cadre de ce contrôle par le docteur [redacted] expert près la Cour d'appel de Paris.

La Commission ne manquera pas de vous tenir informé des futures étapes de contrôle qui seront prochainement effectuées sur ce sujet.

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

M-L. D

Marie-Laure DENIS

P.J. : Rapport d'expertise [redacted] expert près la Cour d'appel de Paris.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

ASSISTANCE PUBLIQUE HOPITAUX DE PARIS
MONSIEUR LE DIRECTEUR GENERAL
3, AVENUE VICTORIA
75004 PARIS

Paris, le 08 juillet 2020

N/Réf : [redacted]Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 4407 3

Monsieur le Directeur,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place dans les locaux de l'Assistance Publique des Hôpitaux de Paris situés 33, Boulevard de Picpus à PARIS (75012) et 8, rue Maia Héléna Vieira Da Silva (Hôpital Broussais) à PARIS (75014).

En application de l'article 31 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie de la décision et de l'ordre de mission relatifs à ces contrôles 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 Directeur, mes salutations distinguées.

[redacted]

P.J. : Décision n° 2020-092C
Ordre de mission
Procès-verbaux n° 2020-092/1 ; 2020-092/2 et 2020-092/3

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

MINISTERE DES SOLIDARITES ET DE LA SANTE
MONSIEUR LE MINISTRE
14, AVENUE DUQUESNE
75350 – PARIS SP 07

Paris, le 08 juillet 2020

N/Réf : [redacted] Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 4483 7

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place dans les locaux de l'Assistance Publique des Hôpitaux de Paris situés 33, Boulevard de Picpus à PARIS (75012) et 8, rue Maia Héléna Vieira Da Silva (Hôpital Broussais) à PARIS (75014).

En application de l'article 31 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie de la décision et de l'ordre de mission relatifs à ces contrôles 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° 2020-092C
Ordre de mission
Procès-verbaux n° 2020-092/1 ; 2020-092/2 et 2020-092/3

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

MINISTERE DES SOLIDARITES ET DE LA SANTE
MONSIEUR LE MINISTRE
14, AVENUE DUQUESNE
75350 – PARIS 07 SP

Paris, le 30 juillet 2020

N/Réf : [redacted]/Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 141 002 1368 0

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place au sein des locaux de la société [redacted] situés [redacted]

En application de l'article 31 du décret n°2019-536 du 29 mai 2019, vous trouverez ci-joint copie de la décision et de l'ordre de mission relatifs à ce contrôle ainsi que du procès-verbal établi 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° 2020-092C
Ordre de mission
Procès-verbal n° 2020-092/5

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La Présidente

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

Paris, le 25 mai 2020

N/Réf : [redacted]/DI201160
À rappeler dans toute correspondance
Envoyé par courriel : [redacted]r

Monsieur le Ministre,

Conformément à la décision n°2020-092C, j'ai décidé d'effectuer un contrôle sur pièces afin 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, du traitement de données à caractère personnel dénommé « *SI-DEP* » en vertu de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020 mis en œuvre par le ministre chargé de la santé (direction générale de la santé) et de tout traitement lié.

Les réponses au questionnaire sont à apporter à la Commission :

- **au plus tard le vendredi 5 2020** pour les questions numérotées de 1 à 5 **;**
- **au plus tard le vendredi 12 juin 2020,** pour les questions numérotées de 6 à 11.

La communication des informations demandées pourra s'effectuer par courrier postal ou de manière dématérialisée. L'envoi dématérialisé devra être effectué par un moyen sécurisé (utilisation d'une plateforme d'échange sécurisée ou chiffrement du document de réponse adressé aux adresses électroniques figurant ci-dessous).

Je vous précise qu'en complément des modalités de contrôle ainsi arrêtées, la Commission procèdera, dans un second temps, à des vérifications sur place, afin de parfaire les éléments de réponse apportés.

Mes services [redacted] se tiennent à la disposition de vos services pour toute information complémentaire.

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

M-L. De

Marie-Laure DENIS

P. J : Décision n°2020-092C
Ordre de mission
Questionnaire

Questionnaire portant sur le traitement de données à caractère personnel dénommé « SI-DEP »

Conformément aux dispositions de l'article 4 du Règlement Européen sur la Protection des Données (RGPD) n° 2016/679 du 27 avril 2016 :

Une donnée à caractère personnel : « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » ;

Un traitement de données à caractère personnel : « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, l'interconnexion, la limitation, l'effacement ou la destruction* ».

Vous veillerez en particulier à ce que chacune des réponses apportées au présent questionnaire soit accompagnée d'une pièce justificative (photocopies de documents, copies d'écran, etc.).

A titre liminaire, la CNIL relève que le système d'information national de dépistage, dénommé « SI-DEP » a été autorisé par l'article 11 de la loi n°2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire. Les conditions de mise en œuvre de ce traitement ont été précisées par le décret n°2020-551 du 12 mai 2020.

La CNIL prend acte que le décret précité désigne le ministre chargé de la santé (direction générale de la santé) comme le responsable du traitement « SI-DEP ». Elle relève également que le traitement est mis en œuvre sur le fondement de l'exécution d'une mission d'intérêt public, conformément aux dispositions du e) du 1. de l'article 6 du RGPD et pour les motifs d'intérêt public mentionnés au i) du 2. de l'article 9 de ce même règlement.

Dans le cadre de l'exercice des pouvoirs de contrôle de la CNIL concernant la mise en œuvre des traitements, il vous est demandé de répondre aux questions listées ci-après.

Pour les questions 1 à 5, vous veillerez à apporter une réponse avant le vendredi 5 juin 2020

1. Demande d'ordre général relative au traitement « SI-DEP » : documentation et contacts

1.1 Veuillez fournir une extraction du registre des activités de traitement liées à la mise en œuvre de « SI-DEP ».

1.2 Veuillez fournir la dernière version de l'analyse d'impact relative à la protection des données (AIPD) réalisée dans le cadre de la mise en œuvre de « SI-DEP ».

1.3 Veuillez communiquer tout document permettant de décrire l'architecture du système d'information « SI-DEP ».

1.4 Veuillez indiquer, à l'aide de tout document, le parcours de la donnée dans le cadre des traitements « SI-DEP ».

1.5 Veuillez communiquer le calendrier du déploiement du traitement « SI-DEP » en précisant les dates effectives de mise en œuvre.

1.6 Veuillez préciser si la mise en œuvre du traitement a été ou sera déployée de manière différenciée selon les territoires.

2. <u>S'agissant des catégories de données enregistrées dans le cadre du traitement « SI-DEP »</u> (article 9 du décret 2020-551 du 12 mai 2020)

2.1 Listez de manière exhaustive les données enregistrées dans le traitement (identité, coordonnées, diagnostics médicaux, antécédents,…) en précisant, le cas échéant, si ces données sont au préalable pseudonymisées, hachées et/ou chiffrées. Veuillez fournir un exemple type de « fiche » telle que présentée dans le traitement (en masquant les données individuelles si elles n'étaient pas fictives).

2.2 Veuillez préciser ce que recouvre la notion de « *lieu d'hébergement collectif* » prévue à l'article 9 du décret 2020-551 du 12 mai 2020.

2.3 Veuillez préciser ce que recouvre la notion de « *personne de confiance* » (représentant légal ? chef d'établissement ? personne que le patient désigne ?...). Veuillez apporter des précisions sur les modalités de recueil de ces données et préciser quand la collecte est nécessaire.

2.4 Veuillez préciser ce que recouvrent les « *données d'identification et coordonnées des médecins* », s'agit-il du médecin préleveur, du médecin traitant, du médecin prescripteur ?

2.5 L'article 9 du décret précité ne fait pas mention d'un QR code. Veuillez préciser si les résultats des analyses biologiques ne prévoient plus la création d'un QR code et si, en conséquence, le QR code ne constitue plus une donnée enregistrée dans le cadre du traitement SI-DEP.

2.6 Concernant le compte-rendu d'analyse prévu à l'alinéa 6 de l'article 9 du décret précité, veuillez préciser les données personnelles susceptibles d'y figurer.

2.7 Veuillez préciser si des champs de texte libre sont prévus.

3. <u>S'agissant de l'information des personnes concernées dans le cadre du traitement « SI-DEP »</u>

Veuillez indiquer, pour chaque catégorie de personne concernée, les modalités selon lesquelles elles sont informées du traitement de leurs données dans le cadre du traitement « SI-DEP ». Veuillez communiquer les supports d'informations fournies aux personnes concernées ;

4. <u>S'agissant de la confidentialité et de la traçabilité des données</u>

4.1 Listez les catégories de personnes habilitées à accéder aux données comprises dans le traitement « SI-DEP », ainsi que dans les services externes, en distinguant au besoin les données auxquelles peuvent accéder différents profils d'utilisateurs (données complètes ou partielles, pseudonymisées ou non…) et en précisant le type d'accès (consultation, modification, effacement).

Précisez pour chaque catégorie de personne la finalité de leur accès aux données.

4.2 Concernant les accès aux données, indiquez quelles mesures de sécurité sont mises en œuvre, en fonction des différents profils d'utilisateurs et en distinguant le cas échéant selon qu'il s'agisse des patients ou des personnels des organismes en charge ou destinataires des données :

- Comment sont créés les identifiants et les facteurs d'authentification (par l'utilisateur, par le système, quels critères de complexité, authentification à plusieurs facteurs…) ?

- Comment sont-ils transmis à l'utilisateur le cas échéant ?

- Quelles sont les mesures complémentaires mises en place (blocage des comptes en cas d'échec, validité temporaire des identifiants, sécurisation de l'interface d'authentification…) ?

- Comment les identifiants et les facteurs d'authentification sont-ils stockés (base distincte, mesures de chiffrement, de hachage…) ?

En cas de délégation de gestion des accès aux données, vous préciserez comment cette délégation d'habilitation est mise en œuvre et les mesures mises en œuvre par le délégant aux fins de contrôle des habilitations délivrées par le délégataire.

4.3 Listez les opérations faisant l'objet d'une procédure de traçabilité, détaillez le contenu des fichiers journaux ainsi que l'hébergement, le chiffrement éventuel et les mesures garantissant la disponibilité et l'intégrité de ces fichiers ;

5. S'agissant des opérations de sous-traitance

Veuillez communiquer la liste des sous-traitants (nom et adresse) intervenant dans la mise en œuvre du traitement et fournir, pour chacun d'eux, tout document encadrant la relation de sous-traitance.

Pour les questions 6 à 11, vous veillerez à apporter une réponse avant le vendredi 12 juin 2020

6. S'agissant des missions dévolues à l'AP-HP

Précisez les missions dévolues à l'AP-HP dans la mise en œuvre du traitement en sa qualité de sous-traitant (par exemple, hébergement des données) ; veuillez communiquer tout document encadrant la relation de sous-traitance entre la Direction générale de la santé et l'AP-HP.

7. S'agissant de la volumétrie des données traitées

7.1 Veuillez communiquer le nombre de personnes concernées par le traitement, à la date de réception du présent questionnaire ; précisez le volume de données traitées par catégories de personnes concernées (personnes ayant fait l'objet d'un examen de biologie médicale de dépistage du covid-19, les personnes de confiance, les médecins). Veuillez préciser le nombre de tests effectués à la date de réception du présent questionnaire.

7.2 Veuillez préciser si des données à caractère personnel relatives à des personnes ayant fait l'objet d'un dépistage préalablement à la mise en œuvre du traitement « SI-DEP » ont été intégrées dans le traitement « SI-DEP ».

7.3 Veuillez communiquer le nombre global de laboratoires de biologie médicale appelés à alimenter le dispositif « SI-DEP » ainsi que le nombre de laboratoires ayant déjà alimenté le dispositif à la date de la réception du présent questionnaire.

8. S'agissant de l'exercice des droits des personnes concernées dans le cadre du traitement « SI-DEP »

8.1 Indiquez les modalités d'exercice des autres droits « Informatique et Libertés », notamment les droits d'accès, de rectification et de limitation.

8.2 Indiquez quelles sont les modalités d'exercice du droit d'opposition.

8.3 Précisez, lorsqu'il est fait droit à une demande d'opposition, les modalités d'effacement des données correspondantes.

8.4 L'article 13 du décret prévoit que le droit d'opposition ne « *s'applique au présent traitement qu'en ce qui concerne la transmission des données à des fins de recherche au groupement d'intérêt public mentionné à l'article L. 1462-1 du code de la santé publique et à la Caisse nationale de l'assurance maladie, telle que prévue au 3° du III de l'article 10 du présent décret. Il s'exerce auprès de la direction générale de la santé* ».

Précisez, dans l'hypothèse où le droit d'opposition est exercé, ce qu'il en est de la transmission de données vers les plateformes susvisées (Health Data Hub et CNAM).

9. S'agissant des durées de conservation

Précisez, pour chaque catégorie de données conservées :

- les règles de conservation des données (durée, modalité de stockage, procédure de purge, d'archivage et/ou d'anonymisation) ;

- la finalité de conservation de ces données.

10. S'agissant de la sécurité et de la confidentialité des données

10.1 Détaillez les éventuelles mesures suivantes mises en place concernant l'hébergement des données :

- localisation des serveurs et prestataires en charge de l'hébergement ;

- chiffrement de la base de données (le cas échéant précisez la méthode et les algorithmes employés) ;

- pseudonymisation et/ou anonymisation de données (le cas échéant précisez la méthode et les algorithmes employés) ;

- moyens de surveillance renforcée des fichiers journaux afin de détecter toute utilisation anormale du traitement et de déclencher une alerte le cas échéant.

Pour les fichiers journaux, fournissez des exemples documentés basés sur une extraction réelle (en masquant les données individuelles si elles n'étaient pas fictives).

10.2 Veuillez indiquer, pour les différents organismes dont les agents seront habilités à accéder au traitement, les moyens d'information et de sensibilisation des agents habilités au regard de leurs obligations (protection des données à caractère personnel, respect du secret professionnel et sanctions pénales encourues, dispositifs de traçage des accès) ainsi que les modalités de formalisation de leur engagement à respecter ces obligations, préalablement à leur habilitation.

11. Concernant les transferts de données et interconnexions

11.1 Listez, pour chaque destinataire des données, les données issues du système « SI-DEP » transférées vers le destinataire ou accessibles à celui-ci. Précisez s'il s'agit :

- d'un flux de données à sens unique, à double sens, d'un envoi de fichier plat ou d'un accès au système « SI-DEP » par le destinataire via une interface, et la fréquence de transfert le cas échéant ;

- la manière dont ces flux sont sécurisés ;

- les catégories de personnes habilitées à accéder aux données ;

- si ces données sont complètes, partielles, pseudonymisées ou anonymisées, en précisant la méthode employée pour ces deux derniers cas.

Détaillez en particulier les interactions avec le dispositif « Contact Covid » et avec le dossier médical partagé le cas échéant.

Fournissez, le cas échéant, des exemples documentés basés sur une extraction réelle (en masquant les données individuelles si elles n'étaient pas fictives) de ces flux de données.

11.2 Décrivez si une interconnexion est prévue avec le dispositif « StopCovid » (données transmises, mode de transmission…).

11.3 Indiquez pour chaque type de transfert sous quelle forme les données sont transférées (données brutes, pseudonymisées, agrégées… en précisant le cas échéant la méthode de pseudonymisation ou d'anonymisation).

11.4 Existe-t-il d'autres sources pour les données que celles fournies par les laboratoires (système de données santé, assurance maladie…) ?

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

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

Paris, le 11 SEP. 2020

N/Réf : [redacted]DI201262
LRAR n° : 2C 141 002 1594 3
À rappeler dans toute correspondance

Monsieur le Ministre,

Conformément à la décision n° 2020-092C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué plusieurs contrôles auprès du ministère des Solidarités et de la Santé.

Ces contrôles avaient pour objet 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 du traitement de données à caractère personnel dénommé « **SI-DEP** » en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020.

Des contrôles complémentaires ont également été effectués les 1er et 2 juillet dans les locaux de l'Assistance Publique – Hôpitaux de Paris (AP-HP) situés 33 boulevard de Picpus à Paris (75012), le 3 juillet, dans les locaux de l'AP-HP, situés 8 rue Maria Héléna Vieira Da Silva, à Paris (75014), le 28 juillet, dans les locaux de la société [redacted] situés [redacted] et le 28 juillet dans les locaux de la société [redacted] situés [redacted]

Sans préjuger des suites qui seront apportées à cette procédure de contrôle et des vérifications complémentaires que la CNIL pourra être amenée à réaliser à l'avenir, les constatations effectuées, ainsi que les compléments apportés par courriel les 9, 10 et 30 juillet 2020, me conduisent d'ores et déjà à vous faire part des observations suivantes.

À titre liminaire, je précise que les missions de contrôle menées jusqu'à présent ont permis de constater un niveau global de conformité satisfaisant. Je tiens également à souligner la volonté de collaboration et de transparence des personnes rencontrées au sein de vos services et de l'AP-HP, laquelle a permis la réalisation de ces contrôles dans des conditions optimales, malgré le contexte sanitaire. Je vous en remercie.

Toutefois, des améliorations doivent être apportées sur les points suivants afin de garantir une sécurité optimale des données traitées.

Tout d'abord, la délégation a constaté que le compte utilisé pour assurer le support patient au sein du laboratoire du site Broussais de l'AP-HP est un compte partagé par tous les utilisateurs et qui dispose d'un profil d'administrateur local. D'une part, les droits conférés par un tel profil vont au-delà des tâches dévolues aux personnes assurant le support patient, à savoir la visualisation et l'édition des informations administratives du patient et le déclenchement du renvoi du courriel permettant de se connecter au portail. D'autre part, si les utilisateurs du compte partagé doivent émarger lors de l'utilisation du compte, il leur est malgré tout possible d'être plusieurs à utiliser ce compte au même moment. Cela ne permet donc pas de s'assurer de l'identité de l'utilisateur effectuant une tâche au moyen du compte partagé, et rend donc plus difficiles des contrôles en cas d'utilisation abusive du fichier.

Il a également été relevé que les administrateurs de la base de données « SI-DEP » partagent un compte d'administration pour accéder à celle-ci. Une telle configuration ne permet pas d'assurer une traçabilité effective des connexions à la base, et risque ainsi de compromettre la confidentialité des données qu'elle contient.

Par ailleurs, s'agissant de la journalisation des opérations, il a été précisé à la délégation qu'il n'y avait pas de traces techniques permettant le suivi des opérations réalisées dans la base de données (création, suppression, édition, etc.), en dehors des événements de connexion à la base. L'absence de traces techniques ne permet pas d'identifier les actions faites par une personne sur un fichier.

Enfin, la délégation a été informée de l'existence d'une base de données, dite « de qualification », utilisée pour réaliser différents tests et développement dans un environnement équivalent à la production. Elle a constaté que le script de pseudonymisation destiné à créer cette base opère la suppression de certaines colonnes de la base de données ainsi qu'au mélange des données situées dans d'autres colonnes, afin de créer un jeu de données représentatif de la production ne faisant pas apparaître l'identité des patients. Le script utilisé fait appel à la méthode « Randomize » du langage VisualBasic afin de générer des nombres aléatoires sur lesquels est basé le mélange des colonnes. Or, l'éditeur de ce langage déconseille son utilisation à des fins cryptographiques. En effet, cette méthode n'est pas suffisamment robuste pour opérer une génération de nombres aléatoires destinée à des opérations de cryptographie. Par conséquent, un attaquant, disposant d'informations externes, telle que l'heure d'exécution du script de pseudonymisation, et de moyens techniques adéquats, serait en mesure de reconstituer l'identité des personnes présentes dans la base de données de qualification ainsi que le résultat de leur test PCR.

De même, la présence de l'adresse non modifiée des patients dans la base de qualification peut, dans l'hypothèse où cette adresse peut être associée à une unique personne, révéler immédiatement la présence de cette personne dans la base de données SI-DEP.

Dans ces conditions, j'appelle votre attention sur les dispositions de l'article 32 du RGPD qui prévoient que « *le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

En conséquence, pour satisfaire aux exigences précitées, il conviendrait de :

- ne pas permettre plusieurs connexions simultanées à un même compte utilisateur ;
- assigner des permissions adéquates aux comptes utilisateurs utilisés dans le but de fournir du support téléphonique ;
- mettre en œuvre un accès aux bases de données à l'aide de comptes administrateurs nominatifs ;
- mettre en place un dispositif permettant de tracer toutes les opérations effectuées en base de données aux fins d'imputabilité des modifications pouvant intervenir sur des données à caractère personnel ;
- mettre en œuvre un mécanisme d'anonymisation de la base de données de qualification pour qu'il ne soit pas possible d'inférer la présence d'une personne dans la base de données SI-DEP ni de reconstruire tout ou partie de la base de données SI-DEP à partir de la base de qualification, sauf à ce que les personnes accédant à la base de qualification et les mesures de sécurité mises en place pour y accéder soient strictement les mêmes que pour la base de données de production.

Je relève en outre qu'un certain nombre de ces points sont mentionnés dans le rapport d'audit de l'ANSSI transmis à la délégation de contrôle le 30 juillet 2020.

Les exigences rappelées ci-dessus, ou des solutions équivalentes assurant un niveau de sécurité du traitement conforme aux exigences du RGPD, devront être respectées à l'avenir. Je vous remercie de bien vouloir me communiquer dans les plus brefs délais, les mesures qui seront prises par vos services concernant l'ensemble de ces points pour assurer votre mise en conformité au RGPD.

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

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]**CS201046**
LRAR n° 2C 156 060 2428 2
À rappeler dans toute correspondance

Monsieur le Ministre,

Conformément à la décision n° 2021-092C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué plusieurs contrôles auprès du ministère des Solidarités et de la Santé.

Ces contrôles avaient pour objet de vérifier la conformité à la loi du 6 janvier 1978 modifiée et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 du traitement de données à caractère personnel dénommé « **SI-DEP** » mis en œuvre en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020.

En premier lieu, à la suite de la première série de contrôles effectués au mois de juillet 2020 et en réponse au courrier d'observation qui vous a été adressé le 11 septembre 2020, vous avez fait état auprès de la CNIL de mesures correctives par courrier électronique du 18 novembre 2020.

À cet égard, je prends bonne note des mesures destinées à garantir une sécurité optimale des données traitées et dont l'échéance de déploiement était prévue le 30 novembre dernier. Je vous invite à tenir la Commission informée de l'effectivité de ces mesures ou à défaut, des modifications apportées au calendrier qui avait été initialement défini.

En second lieu, un nouveau contrôle a été effectué le 23 octobre 2020 dans les locaux de l'Assistance Publique – Hôpitaux de Paris (AP-HP) situés 33 boulevard de Picpus à Paris (75012).

Sans préjuger des suites qui seront apportées à cette procédure de contrôle et des vérifications complémentaires que la CNIL pourra être amenée à réaliser à l'avenir, les constatations effectuées, ainsi que les compléments apportés par courrier électronique le 30 octobre 2020, me conduisent à vous faire part dès à présent des observations suivantes.

D'une manière générale, le contrôle du 23 octobre dernier a permis de constater à nouveau un niveau global de conformité satisfaisant. Je tiens également à souligner la bonne coopération de l'AP-HP, ainsi que la clarté des explications fournies par les personnes rencontrées, lors de cette journée.

Toutefois, ces investigations ont également permis de constater que les utilisateurs de l'équipe d'exploitation de SI-DEP se connectaient à l'interface d'administration de l'outil « ETL [redacted] » au moyen d'un compte utilisateur générique, partagé par dix personnes.

Or, l'article 32 du RGPD prévoit que « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : [...] b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* ».

Ainsi, j'attire à nouveau votre attention sur la nécessité que chaque utilisateur dispose d'un compte individuel, dont il est le seul à connaître les identifiants. Ce procédé constitue une mesure essentielle de confidentialité en ce qu'il permet d'assurer la traçabilité des accès aux données à caractère personnel ainsi que l'imputabilité de ces traces.

Dès lors, je vous invite à mettre en place de façon systématique des comptes utilisateurs individuels pour l'accès à l'interface d'administration de l'outil « ETL [redacted]

Je vous remercie de bien vouloir me communiquer, **avant le 1er février 2021**, les mesures qui seront prises par vos services concernant l'ensemble de ces points pour assurer votre mise en conformité au RGPD.

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. De

Marie-Laure DENIS

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

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 09 JUIN 2021

N/Réf. : [redacted]/CS211045
À rappeler dans toute correspondance
LRAR n° 2C 141 002 4026 6

Monsieur le Ministre,

Conformément à la décision n° 2020-092C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué plusieurs contrôles auprès du ministère des Solidarités et de la Santé.

Ces contrôles avaient pour objet d'apprécier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) du traitement de données à caractère personnel dénommé « **SI-DEP** » mis en œuvre en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020.

Les constatations effectuées le 12 mars 2021 dans les locaux de l'AP-HP ainsi que les compléments apportés le 24 mars et le 12 avril 2021 ont montré, pour les éléments sur lesquels ont porté le contrôle, une conformité à la majorité des obligations posées par le RGPD.

Néanmoins, et sans préjuger des suites qui seront apportées à cette procédure de contrôle et des vérifications complémentaires que la CNIL pourra être amenée à réaliser à l'avenir, je souhaite vous faire part dès à présent des observations suivantes.

En premier lieu, la délégation a constaté, sur le guide d'information SI-DEP (version 1.8.0 du 12 décembre 2020) à destination des professionnels de santé habilités à réaliser des tests antigéniques, la présence d'une rubrique visant à les informer du traitement des données les concernant dans le dispositif « SI-DEP ». Il apparait que ce guide, dont l'objet est plus large, constitue également le vecteur permettant d'informer les professionnels de santé sur le traitement de leurs données à caractère personnel dans le cadre de l'utilisation de SIDEP.

Or, cette information est incomplète au regard des dispositions prévues à l'article 13 du RGPD en ce qu'elle ne précise pas la finalité et la base légale du traitement, les destinataires des données ainsi que leurs durées de conservation. Elle ne détaille pas davantage explicitement les droits des personnes.

Dès lors, je vous invite à bien vouloir compléter l'information des professionnels de santé en ce sens.

En second lieu, la délégation a été informée que dans le cadre du transfert de données du traitement « SI-DEP » vers les plateformes dédiées de la CNAM, « SAFE » et « PETRA », les extractions de données issues du traitement « SI-DEP » sont temporairement enregistrées en local sur le poste informatique des personnels habilités de l'AP-HP. Il a été précisé à la délégation que lesdits fichiers sont supprimés des postes de travail concernés à l'issue du transfert. Il a également été indiqué que les postes de travail utilisés n'étaient pas chiffrés. Or, une telle configuration ne permet pas de garantir de façon optimale la sécurité des données traitées.

Je vous rappelle les dispositions de l'article 32 du RGPD qui prévoient que « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : [...] b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* ».

Dès lors, je vous invite à prévoir un chiffrement des postes de travail des administrateurs en charge de réaliser des extractions du traitement « SI-DEP ». En effet, la suppression simple des fichiers présents sur un ordinateur, y compris en incluant la suppression du contenu de la « corbeille » du système d'exploitation, n'empêche pas leur restauration ultérieure grâce à des programmes spécialisés. Une autre possibilité serait l'utilisation d'un poste de travail dédié uniquement à la réalisation de ces opérations d'extraction et de versement de fichiers, ce poste de travail étant conservé dans un coffre par ailleurs. Ces modalités permettraient un suivi plus fin des actions réalisées, et limiteraient ainsi le risque de fuite de données.

Je vous remercie de bien vouloir me communiquer, **au plus tard 15 jours à compter de la réception du présent pli**, les mesures envisagées par vos services concernant l'ensemble de ces points pour assurer votre mise en conformité au RGPD.

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.

Marie-Laure DENIS

Copie adressée par courrier électronique [redacted]
déléguée à la protection des données

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

MONSIEUR LE DIRECTEUR GÉNÉRAL
CAISSE NATIONALE DE L'ASSURANCE MALADIE
26-50 AVENUE DU PROFESSEUR ANDRÉ LEMIERRE
75020 PARIS

Paris, le 30 JUIN 2021

N/Réf. : [redacted]/CS211053
À rappeler dans toute correspondance
LRAR n° 2C 141 002 1333 8

Monsieur le Directeur général,

Comme vous le savez, la Commission Nationale de l'Informatique et des Libertés (CNIL) conduit depuis le mois de mai 2020 des contrôles ayant pour objet d'apprécier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) du traitement de données à caractère personnel dénommé « **SI-DEP** » mis en œuvre en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020.

À cette occasion, la délégation de la CNIL a notamment procédé à des vérifications sur les modalités de transmission des données du traitement « SI-DEP » à la Caisse nationale de l'assurance maladie aux fins de versement dans la plateforme des données de santé visée à l'article L. 1462-1 du code de la santé publique (dite « *Health Data Hub* »).

Les opérations de contrôle ont mis en évidence que les données du traitement « SI-DEP » sont tout d'abord transmises à la CNAM aux fins de versement des résultats des tests dans ladite plateforme. Ainsi, la CNAM reçoit les informations issues de la base de données « SI-DEP » via deux flux séparés, l'un contenant les données des tests « pseudonymisées », et l'autre permettant de réconcilier le pseudonyme avec le numéro d'inscription au répertoire des personnes. La délégation a constaté, à l'occasion des contrôles réalisés au sein des locaux de l'AP-HP, que ces informations sont versées au moyen de deux interfaces mises à disposition par la CNAM nommées respectivement « PETRA » et « SAFE ».

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

En premier lieu, la délégation a été informée que les modalités d'accès aux deux interfaces « SAFE » et « PETRA » imposent aux personnels habilités de l'AP-HP de réaliser des manipulations manuelles de téléchargement de fichiers contenant des données issues du traitement « SI-DEP » sur leurs postes de travail avant de les verser sur les différentes interfaces, puis de suppression desdits fichiers une fois le versement réalisé.

Ces différentes opérations manuelles sont autant de sources potentielles de vulnérabilités, mettant notamment en péril la traçabilité des données une fois ces dernières téléchargées. Je vous recommande donc de mettre à disposition des différentes entités utilisatrices des services précitées une interface de programmation (API) permettant d'automatiser le versement des données dans ces deux interfaces, tout en continuant de prendre des mesures pour assurer un bon niveau de sécurité du processus permettant l'authentification à ces services, comme exposé ci-après.

En deuxième lieu, en ce qui concerne l'accès à l'interface « PETRA » permettant le versement des données issues des résultats des tests, la délégation de la CNIL a été informée que celui-ci est réalisé au moyen d'un lien hypertexte envoyé par courrier électronique par la CNAM aux personnels habilités de l'AP-HP en charge du versement, sans autre forme d'authentification. Ce lien permet le versement jusqu'à deux gigaoctets de données avant de nécessiter un renouvellement, et expire au bout de 420 jours.

Par ailleurs, la délégation a été informée que l'accès à l'interface « SAFE », permettant la réconciliation des pseudonymes employés avec les numéros d'inscription au répertoire des personnes concernées, est opéré au moyen d'un mot de passe communiqué par téléphone, sans possibilité d'en changer autrement que par téléphone.

Or, de telles configurations ne permettent pas de garantir de façon optimale la sécurité des données traitées.

En effet, concernant les modalités d'accès à « PETRA », la compromission de la boîte aux lettres électronique d'un des personnels habilités de la base de données « SI-DEP » est susceptible de faire courir un risque de compromission de l'accès à l'interface « PETRA », et ainsi permettre le versement de données erronées par des tiers malveillants.

S'agissant de l'accès à « SAFE », la transmission du mot de passe par téléphone n'apporte pas les garanties suffisantes de confidentialité. La personne concernée devrait également être en mesure de définir elle-même son mot de passe. Un mot de passe temporaire pourrait lui être attribué, en lui imposant de changer ce mot de passe lors de sa première connexion.

À cet égard, je vous rappelle les dispositions de l'article 32 du RGPD qui prévoient que *« le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins : [...] b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ».*

Dès lors, afin de garantir la sécurité des données traitées, je vous invite à revoir les modalités d'accès à l'interface « PETRA », par exemple en réduisant la durée de validité des liens hypertextes envoyés par courrier électronique à quelques heures, en les transformant en lien à usage unique ou en

mettant en place une modalité d'authentification avec un identifiant et un mot de passe. Il est entendu que ces différentes suggestions ne sont ni mutuellement exclusives, ni exhaustives.

Je vous invite également à revoir les modalités d'accès « SAFE », en revoyant notamment la politique de gestion des mots de passe. Afin de vous aider dans votre démarche de conformité sur ce point, vous pouvez consulter la délibération de la CNIL n° 2017-012 du 19 janvier 2017 modifiée le 22 juin 2017 portant adoption d'une recommandation relative aux mots de passe.

Enfin, la délégation a été informée que la CNAM n'avait pas encore initiée le versement des données issues du traitement « SI-DEP » dans le « *Health Data Hub* », alors même que vos services sont destinataires depuis maintenant plusieurs mois de données y étant destinées. Je vous remercie de bien vouloir me tenir informée de la date à laquelle le versement des données dans le « *Health Data Hub* » sera effectif.

Je vous remercie de bien vouloir me communiquer, **au plus tard un mois à compter de la réception du présent pli**, les mesures envisagées par vos services concernant l'ensemble de ces points pour assurer votre mise en conformité au RGPD, ainsi que toute observation pertinente au regard des différents points abordés.

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

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

Marie-Laure DENIS

Copie adressée par courrier électronique [redacted] déléguée à la protection des données.

l'Assurance Maladie
Agir ensemble, protéger chacun

Caisse nationale

Le Directeur Général

Madame Marie-Laure DENIS
Présidente de la CNIL
3 place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

Date : 28 JUIL. 2021

N/Réf. : Dir-CABDIR-D-2021-2557

Madame la Présidente,

A l'occasion de contrôles réalisés par votre Commission afin d'apprécier la conformité du traitement de données SI-DEP, vous avez souhaité me faire part de demandes et observations dont j'ai pris connaissance avec attention.

Le décret n°2020-551 du 12 mai 2020 fixant le cadre juridique du traitement SI-DEP prévoit la transmission de données issues du traitement Si-DEP sous forme pseudonymisée à la Caisse nationale de l'Assurance Maladie (Cnam) d'une part, et à la Plateforme des données de santé (PDS) d'autre part, « *aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus* ». Il s'agit du cadre fixé par l'article 36 de l'arrêté du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de la sortie de crise sanitaire.

C'est dans ce cadre que des travaux ont été engagés pour mettre en œuvre le flux de données entre l'AP-HP, en charge de la mise en œuvre du traitement SI-DEP et la Cnam. Les premiers envois ont été réalisés sur la base des outils Safe Https pour les données identifiantes, et Petra pour les données dites « métiers » qui correspondent aux résultats des tests. Ces deux outils constituent des plateformes de dépôt permettant la transmission de données à la Cnam.

Ils sont habituellement utilisés pour des dépôts ponctuels, concernant des projets de petite et moyenne envergure, les flux réguliers et volumineux s'appuyant sur d'autres processus. La nécessité de mettre en œuvre ces transmissions de données dans des délais courts afin de produire rapidement des résultats utiles pour la gestion de la crise sanitaire a conduit à l'utilisation transitoire de ces outils dans l'attente d'une automatisation des transferts sur laquelle des travaux ont été engagés dès le début du mois de février 2021.

Cette automatisation est intervenue en juin dernier et depuis, la transmission des données identifiantes et métier est réalisée de serveur à serveur, via l'outil Safe (qui est différent de Safe https) : les sujets d'authentification et de mots de passe sont donc résolus pour ce traitement.

La combinaison des outils Safe https/Petra est toujours utilisée pour la transmission de données liées à des appariements ponctuels, pour des projets autorisés par la CNIL, dont la Cnam assure la mise en œuvre en tant que responsable de traitement du SNDS. Dans ce cadre, la gestion des mots de passe est assurée différemment : les durées des mots de passe sont plus courtes et ils sont différents pour chaque utilisateur et chaque projet.

Ces outils ont vocation à évoluer à échéance 2022 : des travaux ont en effet été lancés par la Cnam pour assurer la refonte globale des normes entrantes et des circuits de pseudonymisation associés, qu'il s'agisse de l'alimentation du SNDS ou de la gestion des flux liés aux autorisations.

Je vous prie d'agréer, Madame la Présidente, l'expression de mes salutations distinguées.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

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

Paris, le 29 septembre 2021

N/Réf : [redacted]/Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 156 060 2316 2

Monsieur le Ministre,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place dans les locaux de l'Assistance Publique – Hôpitaux de Paris situés 33 boulevard de Picpus 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 du procès-verbal établi 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° 2020-092C
Ordre de mission
Procès-verbal n° 2020-092/10
Synthèse de la charte des contrôles de la CNIL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

ASSISTANCE PUBLIQUE – HÔPITAUX
DE PARIS
MONSIEUR LE DIRECTEUR GÉNÉRAL
3 AVENUE VICTORIA
75004 PARIS

Paris, le 29 septembre 2021

N/Réf : [redacted]/Décision n° 2020-092C
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 156 060 2318 6

Monsieur le Directeur général,

La Commission nationale de l'informatique et des libertés a procédé à un contrôle sur place dans les locaux de l'Assistance Publique – Hôpitaux de Paris situés 33 boulevard de Picpus 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 du procès-verbal établi 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 Directeur général, mes salutations distinguées.

[redacted]

P.J. : Décision n° 2020-092C
Ordre de mission
Procès-verbal n° 2020-092/10
Synthèse de la charte des contrôles de la CNIL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

ASSISTANCE PUBLIQUE – HÔPITAUX DE PARIS (AP-HP)
MONSIEUR LE DIRECTEUR GÉNÉRAL
3 AVENUE VICTORIA
75004 PARIS

Paris, le - 6 DEC. 2021

N/Réf. : [redacted]**/RAL211056**
À rappeler dans toute correspondance

Lettre recommandée AR n° 2C 156 060 2256 1

Monsieur le Directeur général,

Conformément à la décision n° 2020-092C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, le 28 septembre 2021, un contrôle dans les locaux de l'AP-HP situés 33 boulevard de Picpus à Paris (75012).

Ce contrôle avait pour objet d'apprécier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) du traitement de données à caractère personnel dénommé « **SI-DEP** » mis en œuvre en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020.

En particulier, ce contrôle fait suite à la violation de données à caractère personnel notifiée à la CNIL par le Ministère des solidarités et de la santé le 15 septembre 2021 (notification n° FR2109151400003 du 15 septembre 2021) faisant état d'une fuite de données à caractère personnel du traitement SI-DEP pour lequel l'AP-HP intervient en qualité de sous-traitant.

Les constatations effectuées ainsi que les compléments apportés le 8 octobre 2021 me conduisent **à rappeler l'ASSISTANCE PUBLIQUE – HÔPITAUX DE PARIS à ses obligations sur les points qui suivent, conformément aux dispositions de l'article 58.2.b) du Règlement Général sur la Protection des Données (RGPD).**

En premier lieu, il a été précisé à la délégation que l'AP-HP utilisait une plateforme d'envoi et de partage de documents nommée « [redacted] » jusqu'au 10 juillet 2021, comme solution de secours permettant la transmission de données issues de SI-DEP aux destinataires prévus par le décret n° 2021-551 du 12 mai 2021 dans le cadre du suivi des contacts, en cas de défaillance des outils nominaux prévus pour les transferts. Il a également été indiqué que la plateforme [redacted] a été utilisée pour faciliter l'analyse des incidents par les membres de l'équipe « SI-SEP » de l'AP-HP. Dans ce contexte, [redacted] a été utilisée pour l'hébergement et le partage de ces données de santé.

Il ressort des échanges avec mes services lors du contrôle sur place que les données de SI-DEP ont été compromises en raison d'une vulnérabilité de la plateforme [redacted] utilisée par l'AP-HP. Cette vulnérabilité, introduite en juin 2021 à l'occasion d'une mise à jour de ladite plateforme, a eu pour effet de rendre librement accessibles des données à caractère personnel qui n'auraient pas dû l'être, ainsi que des documents de travail liés au projet SI-DEP.

Au cas d'espèce, ce sont des fichiers du traitement SI-DEP stockés sur [redacted] qui se sont retrouvés exposés sur le web et qui ont par la suite été mises en ligne sur le site web « [redacted]. Ainsi, ce sont huit millions d'enregistrements, concernant près d'un million et demi de personnes testées au Covid-19 entre août et septembre 2020, qui ont été compromis. Ces enregistrements contenaient notamment le numéro de sécurité sociale, le nom, le prénom, la date de naissance, l'adresse de courrier électronique et le résultat du test de dépistage.

Il a été précisé à la délégation que la plateforme [redacted] ne permet pas de paramétrer un effacement automatique des fichiers qui y sont déposés, la suppression desdits fichiers n'étant alors possible que par l'utilisateur qui les y a déposés. Dans le cas où un utilisateur supprime un fichier de son répertoire [redacted] celui-ci est déplacé vers une corbeille temporaire de [redacted] où il reste accessible pendant trente jours avant d'être supprimé définitivement de façon automatique. Il a été précisé que l'AP-HP ne dispose pas des droits sur la plateforme permettant de rendre immédiate cette suppression définitive.

La délégation a également constaté que le partage de documents vers des destinataires extérieurs à l'AP-HP ne peut se faire qu'au moyen de liens de partage publics, pouvant nécessiter dans certains cas la saisie d'un code d'accès.

Par ailleurs, la délégation a constaté que la plateforme [redacted] ne permet pas une journalisation facilement exploitable de l'usage qui est fait des liens de partage, ainsi que des accès qui sont réalisés aux fichiers présents dans les espaces personnels.

Enfin, il ressort des pièces transmises à la délégation qu'aucune consigne écrite n'a été adressée aux agents en charge des extractions et des transferts des données de SI-DEP, sur la nécessité de supprimer les documents dès confirmation de leur bonne réception par leur destinataire.

J'appelle votre attention sur les dispositions de l'article 32 du RGPD qui prévoient que « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* y compris *entre autres, selon les besoins, [...] d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement* » et que « *Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite* ».

Or, il m'apparait que les modalités de fonctionnement de [redacted] ne permettent pas de satisfaire aux exigences de l'article précité.

En effet, les données de santé hébergées sur [redacted] ne faisaient pas l'objet d'un chiffrement dédié, en dehors de celui inhérent à la plateforme et de celui intervenant lors des connexions sécurisées avec le protocole TLS. Cela avait pour effet de permettre à n'importe quelle personne réussissant à contourner les mécanismes d'authentification, comme cela s'est produit dans le cas d'espèce, d'accéder à des données de santé. Sur ce point, la politique de sécurité des systèmes d'information de l'État précise dans sa règle relative à la protection des informations (référence RES-PROT) que « *dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par chiffrement adapté* ».

Par ailleurs, il n'est pas exigé des personnes accédant aux documents au moyen des liens de partage qu'elles s'authentifient de manière suffisamment forte. En effet, l'utilisation d'un code d'accès qui n'est pas rattaché à un utilisateur spécifique ne permet pas de garantir l'identité des personnes consultant ces documents qui contiennent des données sensibles. De plus, la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) précise que « *tout accès au système dispositif connecté [doit nécessiter] une authentification préalable* »[1].

Cette absence d'authentification des personnes a pour autre conséquence l'impossibilité de journaliser les accès réalisés sur ces fichiers, ce que ne permet pas [redacted] y compris de façon pseudonymisée. L'authentification des utilisateurs permettrait, d'une part, de garantir que seules les personnes autorisées ont effectivement pu consulter les documents mis en ligne ; d'autre part, de quantifier facilement l'étendue des incidents de sécurité comme cela s'est produit lors de la violation de données. Ainsi, le temps nécessaire à l'éditeur de la plateforme [redacted] pour exploiter les journaux techniques de votre installation est le témoin des difficultés que cette configuration pose. La PGSSI-S confirme par ailleurs cette exigence en indiquant que « *Le dispositif connecté doit comporter une fonction de journalisation locale permettant de conserver une trace des accès au dispositif connecté et de tout événement pouvant avoir un impact critique sur son fonctionnement* »[2].

De surcroît, l'absence de mécanisme de purge automatique des fichiers dans la plateforme [redacted] conduit à méconnaître la durée de conservation des données « SI-SEP » fixée dans le décret n° 2020-551 du 12 mai 2020, ce qui a eu pour effet d'accroître la portée de la violation de données lors de sa survenance, et donc l'étendue des risques pour les personnes concernées. En effet, la divulgation des données issues de SI-DEP, qui comporte de nombreuses données d'identification, fait peser un risque important d'usurpation d'identité pour les personnes concernées et les exposent à des tentatives d'hameçonnage ciblées. La présence des résultats des tests de dépistage au Covid-19 fait en plus peser un risque réputationnel, d'autant plus fort pour les personnes testées positives.

Dès lors, je vous invite à prévoir des modalités d'échanges de fichiers qui permettent de garantir la sécurité des données traitées. En particulier, ces modalités devront requérir une authentification forte des personnes destinataires des données, permettre la bonne journalisation des accès qui sont réalisés auprès des documents ainsi hébergées et forcer l'effacement des données partagées après l'expiration d'une durée prédéfinie.

À ce titre, la délégation a été informée que la plateforme [redacted] n'avait plus vocation à être utilisée pour le traitement SI-DEP mais qu'il n'était toutefois pas exclu de l'utiliser en cas de nouveau dysfonctionnement, en faisant appel à un surchiffrement au moyen d'un conteneur Zed!. Cette modalité d'utilisation de la plateforme, si elle est bien de nature à renforcer la confidentialité des données traitées,

---

[1] *Règles pour les dispositifs connectés d'un Système d'Information de Santé* (PGSSI-S, novembre 2013, v1.0), page 13, Exigence A5, https://esante.gouv.fr/sites/default/files/media_entity/documents/Guide_Pratique_Dispositif_Connecte.pdf

[2] *Ibidem*, page 12, Exigence E20

en protégeant ainsi les informations dans l'hypothèse d'un nouvel incident de même nature, ne saurait pour autant répondre aux autres problématiques liées aux durées de conservation et à la journalisation des accès aux données.

En outre, ce surchiffrement devrait être appliqué systématiquement, pour tous les fichiers hébergés sur la plateforme [redacted] afin de répondre efficacement aux risques posés par un incident du type de celui que vous avez rencontré. Or, l'absence de contraintes techniques pour sa mise en œuvre exposera là-encore cette solution au risque d'erreur humaine.

En second lieu, la délégation a été informée que la plateforme [redacted] est éditée par la société [redacted] Cette société peut intervenir ponctuellement sur la plateforme, à la demande de l'AP-HP, pour des besoins de support et de maintenance. Il a également été indiqué à la délégation que des audits de test d'exposition sur internet sont réalisés par l'AP-HP et l'ANSSI sur la plateforme.

Il ressort des constats que le marché public conclu en 2014 et ayant conduit au déploiement de la plateforme [redacted] au sein de l'AP-HP n'a pas été mis à jour afin de tenir compte des obligations prévues à l'article 28, paragraphe 4, du RGPD, aux termes duquel « *Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le contrat ou un autre acte juridique entre le responsable du traitement et le sous-traitant conformément au paragraphe 3, sont imposées à cet autre sous-traitant par contrat ou au moyen d'un autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées[...]* ».

À cet égard, l'article 28.3 du RGPD prévoit notamment la réalisation d'audits de sécurité afin de garantir le respect par un sous-traitant de ses obligations au titre de l'article 32 du RGPD.

Aussi, des audits de la plateforme [redacted] auraient dû être réalisés par l'AP-HP. En effet, les tests d'exposition sur internet menés par l'AP-HP et l'ANSSI, s'ils permettent une mise en évidence rapide de certaines vulnérabilités, ne sauraient suffire à apprécier pleinement le niveau de sécurité de la plateforme [redacted] notamment à la vue de l'usage qui en a été fait dans le cadre des transferts de fichiers. Vous veillerez également à prévoir un avenant afin de mettre le marché public en conformité avec les exigences de l'article 28.3 du RGPD.

Nonobstant ce qui précède, je prends acte des mesures qui ont été prises visant à retirer les fichiers objets de la violation de données du site web « [redacted] » dès les jours qui ont suivi sa découverte et du déploiement d'un correctif par l'éditeur de la plateforme [redacted] mettant ainsi fin à la violation de données à caractère personnel. Je relève également que l'accès à la plateforme [redacted] depuis internet a été promptement coupé et que les mots de passes des membres de l'équipe SI-DEP ont été modifiés.

Je note aussi que l'ensemble des personnes testées concernées par la violation de données en ont été rapidement informées de manière individuelle et que l'information fournie dans ce cadre était de nature à renseigner de manière adéquate les personnes quant à la nature de l'incident et aux risques associés.

Les exigences rappelées ci-dessus devront impérativement être respectées à l'avenir. La CNIL procédera au besoin à des vérifications ultérieures. La Commission se réserve en effet la possibilité de faire usage de l'ensemble des pouvoirs qui lui sont attribués par le RGPD et par la loi du 6 janvier 1978 modifiée.

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

Je vous prie d'agréer, Monsieur le Directeur général, l'expression de mes salutations distinguées.

Marie-Laure DENIS

Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'État dans un délai de deux mois à compter de sa notification.

Copie adressée par courrier électronique [redacted] déléguée à la protection des données auprès du Ministère des solidarités et de la santé.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Le Secrétaire général

DIRECTION GENERALE DE LA SANTE
MONSIEUR LE DIRECTEUR GENERAL
14 AVENUE DUQUESNE
75350 PARIS SP 07

Paris, le 23 DEC. 2021

N/Réf. : [redacted]CS211070
À rappeler dans toute correspondance

Monsieur le Directeur général,

Conformément à la décision **n° 2020-092C en date du 22 mai 2020**, la Commission nationale de l'informatique et des libertés (CNIL) a effectué plusieurs contrôles auprès du ministère des Solidarités et de la Santé.

Ces contrôles avaient pour objet d'apprécier la conformité à la loi n° 78-17 du 6 janvier 1978 modifiée et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) du traitement de données à caractère personnel dénommé « **SI-DEP** » mis en œuvre en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020 et du décret n° 2020-551 du 12 mai 2020.

Sans préjuger des suites qui seront apportées à cette procédure, la série de contrôles effectuée depuis 2020 dans les locaux de l'AP-HP ainsi que les compléments apportés par courrier électronique le 14 septembre 2021 et le 20 octobre 2021 me conduisent à vous faire part des observations suivantes.

La délégation a été informée qu'un dispositif de pare-feu et anti-DDoS, mis en œuvre par la société [redacted] est utilisé afin de filtrer l'ensemble des requêtes qui sont adressées aux serveurs de la plateforme « SI-DEP » et d'y détecter d'éventuelles attaques. Ces requêtes incluent les connexions des personnes souhaitant récupérer le résultat de leur test de dépistage, ainsi que celles des professionnels de santé venant alimenter la base de données.

La mise en place de cette mesure de sécurité est une bonne chose. Les documents transmis par vos services font apparaître que la prestation technique précitée est fournie par la société [redacted] établie en Israël. Il ressort également des éléments fournis que les serveurs hébergeant les services rendus dans le cadre de cette prestation sont situés en Europe.

Dans ce contexte, je comprends que la société [redacted] a accès à l'ensemble des données à caractère personnel contenues dans « SI-DEP », et notamment les informations de santé.

Si l'Etat d'Israël est reconnu comme garantissant un niveau de protection adéquat en matière de protection des données personnelles, il apparaît, selon les informations disponibles publiquement sur son site web, que la société [redacted] dispose également d'un siège social aux Etats-Unis, la société [redacted]

Dans ces conditions, et sans préjuger des liens capitalistiques et organisationnels entre les sociétés [redacted] je vous invite à évaluer la possibilité d'accès aux données du dispositif « SI-DEP » par les autorités américaines. En effet, dans une telle hypothèse, cet accès serait constitutif d'un transfert de données à caractère personnel sans décision d'adéquation et dès lors, il devrait respecter les termes des autres articles du Chapitre V du RGPD, et particulièrement de l'article 46.

Cet article dispose qu' « *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* ». À 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 du FISA et l'Exécutive Order 12 333, ne fournissait pas une protection essentiellement équivalente à celle fournie par la législation européenne et ne permettait pas le respect en pratique des garanties minimums fournies par des outils de transferts de nature contractuelle, ce qui implique notamment, préalablement à de tels transferts, de prendre des mesures techniques supplémentaires afin de rendre l'accès à ces données par les autorités américaines impossible ou ineffectif.

A toutes fins utiles, je vous informe que l'EDPB, dans ses recommandations 01/2020, a précisé des exemples de mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE.

[redacted]

Je vous prie d'agréer, Monsieur le Directeur général, l'expression de mes salutations distinguées.

L. Dutheillet de Lamothe

Louis DUTHEILLET de LAMOTHE

[redacted]