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 « Contact Covid » résultant de l'adaptation du système d'information « Amelipro » (mai 2020-juin 2021)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

Le 22 mai 2020

Décision n° 2020-091C 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 « Contact Covid », résultant de l'adaptation du système d'information « amelipro » 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 la caisse nationale de l'assurance maladie 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 ;

[redacted]

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
AUDITION SUR CONVOCATION

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°2020-091C en date du 22 mai 2020, l'audition sur convocation a eu pour objet de procéder à la vérification de la conformité du traitement de données à caractère personnel dénommé « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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]
au serv[redacted]ssions de vérification ;

Procédons à l'audition sur convocation, le 16 juin 2020, à partir de 09h30 dans les locaux de la CNIL, de [redacted], a été informée par courrier remis en main propre le 05 juin 2020 et au début de la présente audition, de l'objet des vérifications, de l'identité et de la qualité des personnes chargées de l'audition, ainsi que de son droit de se faire assister par un conseil de son choix ;

[redacted] déclare « je ne souhaite pas me faire assister pour cette audition » ;

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne la CNAM

[redacted] *informent des éléments suivants* :

La Caisse nationale de l'assurance maladie (« CNAM ») est un établissement public qui est la tête du réseau de l'assurance maladie (« AM »). Ce réseau comprend des caisses primaires d'assurance maladie (« CPAM »), qui sont indépendantes de la CNAM et généralement réparties par département.

La responsabilité fonctionnelle de chaque CPAM est dévolue à son directeur général (« DG »).

Depuis 2005, l'Assurance Maladie est organisée, outre la Caisse Nationale, établissement public « tête de réseau », autour d'une part d'un réseau d'organismes locaux, les caisses primaires de l'Assurance Maladie (CPAM), en charge des activités de gestion (indemnités journalières, gestions des assurés, relations avec les professionnels de santé) et d'autre part des directions régionales du service médical (DRSM), dont l'activité principale est le contrôle et l'accompagnement des assurés et des professionnels de santé. Les CPAM sont des organismes de droit privé propres, alors que les DRSM sont des organismes déconcentrés de l'établissement public CNAM.

L'établissement public comprend environ 2 000 personnes et le réseau de l'assurance maladie comprend environ 80 000 salariés.

Demandons un document décrivant les relations juridiques existantes dans le cadre du traitement « CONTACT-COVID » entre la CNAM, la CPAM et les ARS.

En ce qui concerne les relations entre la CNAM et les CPAM

[redacted] *nous informent des éléments suivants* :

La CNAM pilote les CPAM en leur fixant des objectifs définis par des conventions pluriannuelles de gestion. La CNAM signe elle-même, avec son ministère de tutelle (ministère en charge de la santé), une convention d'objectifs et de gestion (COG) qui formalise les engagements pris par l'Assurance Maladie auprès de l'Etat.

En ce qui concerne les relations entre la CNAM et ses partenaires

[redacted] *nous informent des éléments suivants :*

- **Relation entre la CNAM et l'ARS**

Au début de la crise et avant la parution du décret du 12 mai 2020, les agences régionales de santé (« ARS ») avaient la charge de l'activité de « tracing » des patients zéro et des cas contacts car il s'agissait d'une mission traditionnellement dévolue afin de cibler les foyers à risque dans la propagation du virus. Les ARS ont connu une forte activité de tracing des patients zéro et des cas contacts durant les mois de février et mars.

Lorsque la France est rentrée en phase 3 (confinement général), la mission de tracing des patients zéro et des cas contacts dévolue aux ARS a cessé. A compter du déconfinement cette mission a été dévolue à la CNAM.

L'activité de suivi dans le téléservice « CONTACT-COVID » a été répartie en trois niveaux afin notamment que les ARS puissent se concentrer sur les foyers et les établissements sensibles (écoles, prisons, établissements de santé, etc) (niveau 3 du téléservice « CONTACT-COVID »).

Les relations entre la CNAM et les ARS sont encadrées par des conventions conclues entre le DG de la CNAM et chaque DG des ARS (*Pièce n°16 communiquée dans le cadre du questionnaire adressé le 26 mai 2020*). De plus, les CPAM ont conventionné avec les ARS la mise à disposition de postes informatiques permettant l'accès à « CONTACT-COVID ».

Cette convention rappelle les principes de sécurisation des données récupérées par les ARS à partir du téléservice « CONTACT-COVID » et les rôles respectifs des différents acteurs.

Les ARS sont utilisateurs du téléservice « CONTACT-COVID », tout comme les médecins ou les pharmaciens.

En parallèle, les ARS réutilisent les données dont elles sont destinataires dans l'application « CONTACT-COVID » dans le cadre de leur mission d'investigation des foyers de contamination. La CNAM considère qu'il s'agit de nouveaux traitements de données à caractère personnel pour lesquels les ARS sont seules responsables de traitement. Cette relation est encadrée par une convention entre la CNAM et les ARS.

- **Relation entre la CNAM et l'agence nationale de santé publique (Santé publique France « SPF »)**

Avant la mise en œuvre de l'application « CONTACT-COVID », SPF a travaillé avec la CNAM à l'élaboration des consignes sanitaires et le cadrage du « tracing » des patients zéro ou des cas contacts. La CNAM a travaillé avec cet établissement public pour établir le questionnaire des informations à recueillir auprès des personnes concernées dans le cadre de « CONTACT-COVID » afin d'optimiser le « tracing » de ces personnes.

SPF n'est pas utilisateur des données contenues dans l'application « CONTACT-COVID », mais, elle est destinataire des données pour la partie relative aux indicateurs. Ces données sont agrégées.

A ce jour, aucun projet n'a été initié par la CNAM en vue de déléguer les missions qui lui sont dévolues à des organisations volontaires mises en place par les professionnels de santé de ville

dans les territoires (communautés professionnelles territoriales de santé, maisons de santé pluriprofessionnelles, plateformes territoriales d'appui, centres Covid dédiés, etc).

- **Relation entre les ARS et de la direction du numérique (« DNUM »)**

La DNUM est une direction du Ministère des solidarités et de la santé. La DNUM est sous-traitante des ARS. La CNAM est un tiers à cette relation.

- **Relation entre la CNAM et les agents d'autres organisations professionnelles sociales**

La CNAM a rendu possible la mise à disposition d'autres agents organisations professionnelles sociales (branches) (CARSAT, CAF) et d'autres régimes (MSA, etc) au niveau des plateformes pour le niveau 2 du téléservice « CONTACT-COVID ». Le nombre d'agents mis à disposition est marginal. Cette relation est régie par leur contrat de travail et le Code du travail.

Les agents des autres organisations professionnelles accèdent aux mêmes données que les agents directement rattachés à la branche de l'AM.

Demandons le nombre d'agents de chaque branche de la sécurité sociale ayant été mis à disposition pour le suivi épidémiologique.

Demandons la dernière convention d'objectifs et de gestion en la CNAM et le MSS.

Demandons les 3 derniers budgets de fonctionnements de la CNAM.

- **Relation entre la CNAM et le service de santé des armées**

Le Code de la défense implique un régime juridique particulier pour le traitement des données relatives aux militaires, notamment sur la gestion de leurs adresses. A la demande du service de santé des armées, seul ce dernier est habilité à effectuer le « tracing » de niveau 1.

En ce qui concerne les mesures de conformité au règlement général sur la protection des données (RGPD) :

[redacted] *nous informent des éléments suivants* :

Le réseau de l'AM comprend un délégué à la protection des données (« DPO ») désigné pour la CNAM ainsi que des DPO désignés dans chacun des organismes (CPAM) et des DRSM.

Ces DPO, pilotés par la DPO de la CNAM, sont chargés des relations directes avec les professionnels de santé comme les bénéficiaires de l'AM pour la gestion de l'exercice de leurs droits « Informatique et libertés ».

La base légale des données collectées relatives au patient zéro dans le cadre du traitement « CONTACT-COVID » est la mission d'intérêt public.

La base légale de l'identification des cas contacts par le patient zéro est la mission d'intérêt public. Afin de garantir le respect des droits des personnes (patients zéro et cas contacts), la CNAM a choisi de mettre en œuvre un principe d'adhésion au traitement en ne collectant pas l'identité des cas contacts si le patient zéro ne souhaite pas les communiquer.

La base légale de la divulgation de l'identité du patient zéro aux cas contact dans le cadre du traitement « CONTACT-COVID » est le consentement.

Dans le cadre d'un suivi et accompagnement social, les informations demandées aux cas contacts ou patients zéro permettent uniquement à l'agent de l'AM d'orienter la personne vers les services sociaux compétents. Aucune donnée n'est collectée et conservée auprès de ces personnes par les agents de l'AM dans la base de données de « CONTACT-COVID ». (*voir pièce n°1 communiquée dans le cadre du questionnaire adressé le 26 mai 2020*)

La zone de commentaires présente dans l'application « CONTACT-COVID » a été supprimée.

En ce qui concerne l'information des patients zero, des cas contacts et des professionnels de santé

[redacted] *nous informent des éléments suivants* :

Le patient zéro est informé à plusieurs moments du traitement de ses données dans le cadre du téléservice « CONTACT-COVID » :

- lorsqu'il se rend en consultation médicale au moyen d'une affichette mise à disposition des professionnels de santé, notamment des médecins pour un affichage dans leur cabinet ;
- lorsqu'il effectue son test et/ou lorsqu'il reçoit le résultat de celui-ci afin de savoir s'il est atteint du COVID-19, le patient est informé que l'AM sera rendu destinataire de ce résultat ;
- lorsqu'il est contacté par téléphone par le personnel des plateformes dédiées de l'AM, ou assimilé, dans le cadre du niveau 2 du téléservice « CONTACT-COVID » pour compléter l'identification des cas contacts ;
- lorsqu'il se rend sur le site ameli.fr, qui comprend une information exhaustive sous la forme d'une mention « informatique et Libertés » et une information via des articles dédiés au téléservice « CONTACT-COVID » ;
- à l'occasion de campagnes de communication (réseaux sociaux, intervention publique du directeur général de la CNAM…).

Le cas contact est informé à plusieurs moments du traitement de ses données dans le cadre du téléservice « CONTACT-COVID » :

- lorsqu'il est appelé par le personnel des plateformes dédiées de l'assurance maladie, ou assimilé, dans le cadre du niveau 2 du téléservice « CONTACT-COVID » pour déterminer s'il est un contact à risque du patient zéro ;
- lorsqu'il se rend sur le site ameli.fr, qui comprend une information exhaustive sous la forme d'une mention « informatique et Libertés » et une information via des articles dédiés au téléservice « CONTACT-COVID » ;
- à l'occasion de campagnes de communication (réseaux sociaux, intervention publique du directeur général de la CNAM…).

L'ensemble des cas contacts dont l'identité et les coordonnées ont été communiquées par le patient zéro sont contactés par téléphone par le personnel des plateformes dédiées de l'AM, ou assimilé. Les cas contacts sont contactés dans un délai moyen de 24h à 48h après avoir été identifiés par le patient zéro.

La patient zéro peut à tout moment retirer son consentement à la divulgation de son identité au cas contact qu'il a identifié dans le délai moyen de 24h à 48h. Le retrait du consentement sera pris en compte par le personnel des plateformes dédiées de l'AM si les cas contacts n'ont pas encore été appelés. Le retrait du consentement sera sans objet si les cas contacts ont déjà été appelés.

Les professionnels de santé sont informés du téléservice CONTACT-COVID au moyen :

- d'un guide méthodologique intitulé « CONTACT-COVID – guide des fonctionnalités du service » ;
- d'une affichette mise à leur disposition, notamment pour un affichage dans leur cabinet / espace de réception des patients ;
- du site ameli.fr, qui comprend un article dédié pour les professionnels de santé.

La pièce 6, page 2 indique que « *L'entretien* [téléphonique] *doit être mené* [par le personnel des plateformes dédiées de l'assurance maladie, ou assimilé] *en présence du représentant légal ou directement avec lui en fonction de l'âge du mineur* ».

Demandons la signification de l'« âge du mineur » et comment la CNAM s'assure qu'il s'agit bien du représentant légal du mineur.

En ce qui concerne l'exercice des droits des patients zéro et des cas contacts

[redacted] *nous informent des éléments suivants* :

Pour exercer leurs droits « Informatique et Libertés », les patients zéro et les cas contacts peuvent réutiliser les mécanismes courants mis à disposition des bénéficiaires de l'AM :

- par courrier adressé à leur organisme de rattachement ;
- sur place, au sein des CPAM, lorsque les conditions sanitaires permettent un accueil des publics ;
- par message dématérialisé au sein de leur compte Ameli via une rubrique dédiée (le patient zéro et / ou le cas contact doit avoir au préalable créé un compte sur le site ameli.fr afin d'être en mesure d'exercer ses droits « Informatique et Libertés »).

En plus de ces trois possibilités, le patient zéro et / ou le cas contact peut exercer ses droits lors de l'entretien téléphonique (contact tracing de niveau 2) avec le personnel des plateformes dédiées de l'assurance maladie.

Lors de l'entretien téléphonique, le personnel des plateformes dédiées de l'assurance maladie (contact tracing de niveau 2) indique que les données recueillies dans le cadre du téléservice « CONTACT-COVID » pourraient également être utilisées, sauf opposition, pour des études et évaluations.

A ce jour, les données recueillies dans le cadre du traitement « CONTACT-COVID » n'ont pas vocation à être réutilisées pour des études et évaluations : les seules données qui ont du sens en termes de recherche épidémiologique sont les résultats des tests, qui sont intégrés dans SI-DEP et non dans CONTACT-COVID. Si le décret n°2020-551 du 12 mai 2020 a introduit un parallélisme dans la rédaction entre les traitements « SI-DEP » et « CONTACT-COVID » sur ce point, seules les données issues de SI-DEP auraient vocation, à ce jour, à faire l'objet de recherches, d'études et d'évaluations.

A ce jour, la CNAM a reçu une demande écrite d'exercice du droit d'opposition en lien avec le traitement « CONTACT-COVID ».

Demandons copie de la demande d'exercice de droit d'opposition reçue en lien avec le traitement « CONTACT-COVID » et de la réponse apportée par la CNAM.

Demandons le nombre de demandes d'exercice des droits « Informatique et Libertés » effectuées en lien avec le traitement « CONTACT-COVID ».

Demandons copie des demandes d'exercice des droits « Informatique et Libertés » effectuées en lien avec le traitement « CONTACT-COVID » et des réponses apportées par la CNAM.

Demandons copie de tout élément permettant de démontrer le parcours d'un patient zéro et d'un cas contact souhaitant exercer ses droits au sein de son compte Ameli.

Demandons le nombre de patients zéro qui ont souhaité que leur identité ne soit pas divulguée auprès du cas contact sur au moins un contact sur tous les patients dont les coordonnées ont été inscrites dans le téléservice « CONTACT-COVID».

Demandons, sur l'ensemble des cas contacts, combien n'ont pas été informés de l'identité du patient zéro.

En ce qui concerne la suppression des données

[redacted] *nous informent des éléments suivants* :

Il n'est possible de saisir des patients contacts qu'une fois la fiche du patient zéro validée (test positif ou examen radiologique et symptômes caractéristiques).

Lorsqu'un médecin indique sur la fiche d'un patient présumé positif (fiche « brouillon ») que le résultat du test de dépistage est négatif, le patient est supprimé en base de données.

La fonction suppression est présente depuis début juin 2020. Les données collectées entre le début du traitement et la mise en place de la suppression n'ont pas encore été purgées.

Un médecin n'a pas la possibilité de supprimer une fiche patient zéro. En cas d'erreur, le médecin doit contacter le support de la CNAM.

Les données des patients contacts non avérés ou des patients contacts ayant refusé de participer au traitement sont immédiatement supprimés.

A partir de la collecte, les données (y compris les fiches « brouillons ») sont conservées 3 mois conformément au décret. A l'issue de cette durée, les données sont supprimées.

Des auto-questionnaires, conçus par la CNAM, au format papiers à destination des patients zéro peuvent être fournis par les médecins. Ces documents n'ont pas vocation à être transmis à l'AM ou aux ARS.

La CNAM précise que chaque médecin est responsable de traitement des données renseignées dans les auto-questionnaires.

Demandons copie de l'auto-questionnaire fourni aux médecins.

En ce qui concerne la sécurité des données et la gestion des habilitations

[redacted] *nous informent des éléments suivants* :

Afin de faciliter le travail de rappel des « patients contact », les agents de l'Assurance maladie peuvent utiliser [redacted] un outil interne à l'Assurance maladie, utilisé pour la gestion des données de contact des assurées [redacted]

Le NIR est obligatoire lors de la création d'une fiche « patient zéro ». Un mécanisme de vérification empêche la création de deux fiches ayant le même NIR.

Il est possible de créer une fiche « patient contact » sans renseigner de NIR.

Si un « patient contact » ne dispose pas de NIR (patients n'ayant pas de droits ouverts dans un des régimes d'assurance maladie), sur la base du SMS envoyé par l'AM que le patient montre au laboratoire/pharmacien, ce dernier facture la prestation à l'AM au moyen d'un NIR fictif.

Le NIR fictif n'est jamais communiqué au patient ni renseigné dans le télé-service « CONTACT-COVID ».

Selon leur profil, les utilisateurs n'ont pas accès aux même patients à travers la fonction recherche :

- un médecin ne peut utiliser la fonction recherche que pour rechercher une fiche parmi celles qu'il a enregistrées ;
- les pharmaciens et les laboratoires peuvent rechercher uniquement les « patients contacts » à l'aide de leurs NIR ;
- les agents de l'AM et des ARS peuvent rechercher parmi l'ensemble des fiches y compris les fiches « brouillons ».

Les agents de l'AM et des ARS ont la possibilité de passer une fiche au statut « clôturé ». Ce statut s'inscrit dans un processus métier et est utilisé pour permettre à l'agent de savoir lorsque son travail de complétion de la fiche est fini.

Lorsque plus de 10 personnes sont présentes dans un même foyer de contamination, la CNAM informe les ARS afin que ces dernières réalisent un suivi particulier de la chaîne de contamination.

L'AM pourra déléguer à un salarié d'un partenaire les droits de création de comptes afin qu'il puisse créer des comptes pour les autres salariés employés par le partenaire. Un processus de validation de ce type d'administrateurs des comptes a été défini et a été communiqué lors du contrôle sur pièce. Cette solution sera mise en place dans les prochaines semaines.

Il est prévu de mettre en place une limitation du nombre de compte créés par chaque administrateur (10 comptes), une matrice d'habilitation spécifique (un profil identique au profil « agent » pour les ARS et deux profils identiques aux profils « médecin » et « laboratoire » pour les établissements de santé) ainsi qu'un indicateur du nombre de comptes créés par chaque administrateur.

L'authentification des salariés des partenaires repose sur un nom d'utilisateur et un mot de passe.

[redacted]

En ce qui concerne les constatations réalisées lors de l'audition

Somme informés que [redacted] se connecte sur l'environnement de recette du traitement « CONTACT-COVID ». Cette version sera en production à partir du 17 juin 2020.

A notre demande [redacted] se connecte au site web du traitement « CONTACT-COVID » avec un profil « agent ».

Sommes informés que ce profil correspond à un agent d'une CPAM assurant le suivi épidémiologique.

Sommes informés que l'authentification repose sur l'utilisation de la carte à puce distribuée à chaque agent de l'assurance maladie et assimilé.

Sommes informés que par défaut le critère géographique est pré-rempli en fonction de la caisse d'affectation de l'agent. Un agent d'une CPAM a la possibilité de rechercher des patients d'un autre département.

Constatons la présence de fiches dont l'état est « en attente de diagnostic ». Somme informé que ce statut correspond à une fiche « brouillon » (voir pièces).

A notre demande [redacted] affiche les fiches cas contacts et le fiches patients zéro présentes dans la base de recette pour le département 75 et documente sa progression à l'aide de captures d'écran (voir pièces).

A notre demande [redacted] crée une fiche patient zéro et documente sa progression à l'aide de captures d'écran (voir pièces).

Sommes informés que les champs avec un astérisque sont obligatoires.

Constatons qu'une fois le champ NIR renseigné, une liste déroulante apparait dans le champ « choix du bénéficiaire ». Sommes informés que cette liste est alimentée par le référentiel des identités des assurés de la CNAM (RFI) (voir pièces).

Constatons que si la liste déroulante « le patient peut-il exposer ou avoir exposé une collectivité ? » n'est pas sur « non », un champ apparait permettant d'indiquer le nom de la collectivité (voir pièces).

A notre demande [redacted] valide la fiche sans cocher la case indiquant que l'utilisateur a informé le patient de la finalité du traitement et de ses droits. Constatons qu'il n'est pas possible de valider la fiche (voir pièces).

A notre demande [redacted] coche la case indiquant que l'utilisateur a informé le patient de la finalité du traitement et de ses droits et valide la fiche.

A notre demande [redacted] passe la fiche à diagnostic confirmé et valide la fiche sans renseigner la date de prélèvement. Constatons qu'il est possible de valider la fiche (voir pièces).

A notre demande [redacted] crée une fiche « patient contact » et documente sa progression à l'aide de captures d'écran (voir pièces).

Constatons que, par défaut, la case « le patient zéro accepte de communiquer son identité à ce contact » est décochée (voir pièces).

A notre demande [redacted] accède au site web « CONTACT-COVID » avec un compte ayant le profil « laboratoire » et documente sa progression à l'aide de captures d'écran (voir pièces).

A notre demande [redacted] effectue une recherche en laissant le champ « NIR » vide. Constatons qu'aucun résultat n'est affiché (voir pièces).

A notre demande [redacted] recherche le « patient zéro » créé plus tôt à l'aide de son NIR. Constatons que le compte n'est pas affiché (voir pièces).

A notre demande [redacted] recherche un « patient contact » et documente sa progression à l'aide de captures d'écran (voir pièces).

A notre demande [redacted] accède au site web CONTACT-COVID avec le profil « pharmacien » et documente sa progression à l'aide de captures d'écran (voir pièces).

A notre demande [redacted] effectue une recherche en laissant le champ « NIR » vide. Constatons qu'aucun résultat n'est affiché (voir pièces).

A notre demande [redacted] recherche un « patient contact » et documente sa progression à l'aide de captures d'écran (voir pièces).

A notre demande [redacted] accède au site web CONTACT-COVID avec le profil « médecin » et documente sa progression à l'aide de captures d'écran (voir pièces).

A notre demande [redacted] recherche le « patient zéro » créé plus tôt à l'aide de son NIR. Constatons que le compte n'est pas affiché (voir pièces).

Avez-vous quelque chose à ajouter ?

Réponse :

[redacted] est invitée à faire part de ses observations et déclare :
« Je n'ai rien à rajouter ».

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 :

Paraphes

L'audition s'est terminée, ce jour, à 18h50, sans incident ;

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

Signature des agents de la CNIL	Signature des personnes auditionnées
[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.

La personne auditée a été mise en mesure de consulter les pièces copiées.

PIECE N°1 : [redacted]

PIECE N°2 : [redacted]

Signature des agents de la CNIL	Signature des personnes auditionnées
[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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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 ;

[redacted]

CNIL, dûment habilités à procéder à des missions de vérification sur place ;

En présence du [redacted] médecin expert 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 22 juin 2020, à 09h30, dans les locaux de Caisse primaire d'assurance maladie de la Seine Saint Denis, situés 2 avenue de la Convention à Bobigny (93000) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité, en la personne de [redacted] de la CPAM de Bobigny, 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 :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert.

En ce qui concerne la CPAM de la Seine-Saint-Denis

[redacted] *nous informent des éléments suivants :*

La CPAM de la Seine Saint Denis a été créée en 1982. Elle comprend 1300 salariés.

Son budget de fonctionnement pour l'année 2019 est de 80 millions d'euros.

La CPAM de la Seine Saint Denis dispose de plusieurs activités :

- le service des prestations (prestations en nature, en espèce, risque accidents maladies professionnelles ...) ;
- le service des relations clients (agence d'accueil) ;
- une mission de régulation du système de santé et de prévention (facilitation de l'accès aux soins des assurés, régulation des dépenses et centre de soin) ;
- les services supports aux activités précitées (service relation-humaine, service informatique...).

Le rôle de la CPAM de la Seine Saint Denis dans le traitement « CONTACT-COVID » est d'organiser le «contact tracing» dans le département de la Seine Saint Denis.

La CPAM de la Seine Saint Denis traite uniquement les patients zéro et les cas contacts dont la caisse de rattachement est la CPAM de la Seine Saint Denis.

Le «contact tracing» est organisé en « plateau » au sein de la CPAM. Le plateau a été mis en œuvre à compter de la publication du décret n°2020-551, c'est-à-dire le 13 mai 2020. Le plateau est composé de managers et d'agents qui sont appelés des enquêteurs. Le nombre d'agents était initialement d'environ 170 agents de la CPAM recrutés sur la base du volontariat. A ce jour, le plateau est composé de 4 managers et 12 enquêteurs.

Ce dimensionnement initial a été calculé sur la base du traitement dans le téléservice « CONTACT-COVID » de 140 patients zéro par jour et d'une vingtaine de cas contacts par

patient zéro. Au jour du contrôle, la moyenne est de traiter dans le téléservice « CONTACT-COVID » environ 20 patients zéro par jour et 3 cas contacts par patients zéro.

Chaque agent enquêteur dispose de plusieurs outils :

- un accès à l'application « CONTACT-COVID » ;
- un téléphone pour contacter les patients zéro et les cas contacts ;
- un accès à l'outil d'envoi de courriel CLOE si l'assuré dispose d'un compte « ameli » ;
- un accès à l'outil d'envoi de sms CAMPUS ;
- un accès à MEDIALOG qui est l'outil de gestion des relations avec le public. Cet outil permet aux agents enquêteurs de rechercher les coordonnées des patients zéro et des cas contacts.

Les courriels et les sms envoyés par les outils CLOE et CAMPUS sont issus de modèles personnalisables. La personnalisation permet uniquement d'ajouter des coordonnées téléphoniques du Dispositif d'Appui à la Coordination concernée (DAC). Il ne s'agit pas d'un canal d'interaction. Les agents qui envoient ces courriels et / ou courriels ne sont pas identifiables. Il n'est attendu aucun retour du patient zéro ou du cas contact en réponse à ces courriels ou sms.

Le département de la Seine Saint Denis comprend trois DAC, qui sont des dispositifs visant à fluidifier les parcours de santé complexe en organisant leur prise en charge sur un territoire (accompagnement médico-social). Selon la commune du patient zéro ou du cas contact, la CPAM indique à ce dernier d'appeler la cellule d'appui compétente.

L'accompagnement médico-social n'est réalisé qu'à la demande du patient zéro ou du cas contact.

Pour assurer le «contact tracing», un appel au volontariat au sein de la CPAM de la Seine Saint Denis a été effectué (salariés du centre de santé, agents du service prévention de la Caisse, agents d'accueil dans les agences ou de la plateforme téléconseiller). Un second appel au volontariat a été réalisé auprès de la CRAM d'Ile de France. A ce jour, au regard de l'activité décroissante du «contact tracing», aucune suite n'a été donné à ces candidatures.

Les agents enquêteurs ont la possibilité de transférer un appel d'un patient zéro ou d'un cas contact directement au DAC compétent de Seine Saint Denis.

En ce qui concerne le « service du contrôle médical »

[redacted] *nous informent des éléments suivants :*

Le service du contrôle médical est dirigé par des médecins conseils, qui sont des agents de la CNAM.

La mission du service du contrôle médical dans le cadre du niveau 1 du «contact tracing» du patient zéro et / ou du cas contact est le suivant :

Lorsque des patients sont diagnostiqués positifs au COVID-19 au sein du système d'information « SI-DEP », le service du contrôle médical vérifie qu'il existe bien une fiche patient zéro dans l'application « CONTACT-COVID » pour l'ensemble de ces derniers. En l'absence de fiche créée et de médecin ayant prescrit le test, le service du contrôle médical peut également créer une fiche de patient zéro à la place du médecin. Dès lors qu'un médecin ayant prescrit le test existe, le service médical se rapproche du médecin de manière à ce que dernier mette à jour la fiche du patient zéro.

[redacted] [redacted]

La mission du service du contrôle médical dans le cadre du niveau 2 du «contact tracing» du patient zéro et / ou du cas contact est le suivant :

- prescrire un arrêt de travail pour le cas contact avéré qui doit s'isoler ;
- si dans l'échange entre l'enquêteur et le patient zéro et / ou cas contact, ce dernier a des questions d'ordre médical.

En ce qui concerne la procédure de «contact tracing»

[redacted] *nous informent des éléments suivants :*

L'ensemble des agents enquêteurs de la CPAM de la Seine Saint Denis appellent l'ensemble des patients zéro et cas contact du département de la Seine Saint Denis afin de créer (cas contact) ou compléter (patient zéro et cas contact) les fiches de «contact tracing».

Le «contact tracing» du patient zéro est considéré comme terminé lorsque les deux conditions suivantes sont remplies :

- l'ensemble des cas contacts d'un patient zéro sont joints par téléphone par les agents enquêteurs ;
- l'ensemble des fiches des cas contacts associées à ce patient zéro sont complétées.

Chaque appel donne lieu à l'envoi d'un courriel type et / ou d'un sms type au patient zéro et / ou cas contact par les applications CAMPUS et / ou CLOE.

En ce qui concerne l'information

[redacted] *nous informent des éléments suivants :*

L'ensemble des agents enquêteurs de la CPAM de la Seine Saint Denis ont bénéficié d'une formation générale sur le secret médical, le secret professionnel et la protection des données.

Demandons copie du support de formation des agents enquêteurs de la CPAM de la Seine Saint Denis à cette formation.

Prenons copie de la fiche de présente des agents enquêteurs de la CPAM de la Seine Saint Denis à cette formation.

Les agents enquêteurs de la CPAM de la Seine Saint Denis bénéficient régulièrement de « brief » sur le respect des principes de protection des données dans le cadre du téléservice « CONTACT-COVID ».

Ces « brief » ont par exemple donné lieu à des tableaux généraux de management visuel auxquelles les agents enquêteurs de la CPAM de la Seine Saint Denis peuvent se reporter (voir pièces).

En ce qui concerne l'exercice des droits

[redacted] *nous informent des éléments suivants :*

Si le patient zéro s'est opposé à la communication de son identité aux cas contact, ses nom et prénom apparaissent de la même manière au sein du téléservice « CONTACT-COVID » que

s'il l'avait accepté. Dans ce cas, un message de couleur rouge informe l'agent enquêteur qu'il ne doit pas communiquer le nom du patient zéro au cas contact.

Si le patient zéro et / ou le cas contact souhaite s'opposer à l'utilisation de ses données à des fins de recherches, d'études et d'évaluations auprès d'un agent enquêteur, ce dernier transmet par écrit sur une feuille les nom et prénom du demandeur à son manager. Celui-ci envoie un courriel au DPO de la CPAM de la Seine Saint Denis qui peut, en cas de besoin, contacter le DPO de la CNAM. Le DPO de la CPAM de la Seine Saint Denis conserve ces mails au sein d'un dossier informatique dédié.

En ce qui concerne les patients mineur et les majeurs protégés

[redacted] *nous informent des éléments suivants :*

Une personne mineure est considérée comme telle dès lors que son âge est inférieur à 18 ans. Le NIR d'un patient mineur est rattachée à celui de ses ouvrants droit, qui dans la plupart des cas sont les représentants légaux. Lorsqu'un agent enquêteur prend contact avec un mineur, il demande en principe à être mis en contact avec ses représentants légaux. Si la personne est proche de la majorité, l'agent peut décider de s'entretenir directement avec elle.

Les agents de la CPAM de la Seine Saint Denis ne disposent pas d'un référentiel répertoriant les représentants légaux des personnes mineures.

Il n'y a pas de procédure formalisée spécifique au traitement « CONTACT-COVID » pour la prise en charge de majeurs protégés.

En ce qui concerne la prise en charge des patients ne disposant pas de NIR

[redacted] *nous informent des éléments suivants :*

Le NIR fictif est utilisé uniquement par les pharmaciens et les laboratoires afin de facturer les tests de dépistage au COVID-19 et délivrer des masques. Il n'est pas renseigné au sein du téléservice « CONTACT-COVID » pour créer des fiches de «contact tracing».

Avons procédé à une recherche du NIR fictif utilisé par la CPAM de Seine Saint Denis et avons constaté que la recherche ne renvoie aucun résultat.

En ce qui concerne la suppression des fiches de type « contact non avéré »

[redacted] *nous informent des éléments suivants :*

Les managers effectuent chaque jour une suppression manuelle des fiches concernant des cas contacts non avérés.

Constatons la présence d'une unique fiche datant du 19 juin 2020 relative à un cas contact non avérés étant affilié à la CPAM de la Seine Saint Denis ; que cette fiche est verrouillée. Sommes informés qu'il s'agit d'une fiche en cours de modification par un médecin.

Dans le cadre de l'appel d'un cas contact, dès lors que celui-ci indique ne pas avoir été en contact avec le patient zéro, sa fiche est passée à l'état « contact non avéré ». L'avis du cas contact prime sur celui du patient zéro.

En ce qui concerne l'information de l'ARS d'une collectivité exposée

[redacted] *nous informe des éléments suivants :*

Lorsqu'une collectivité et / ou un groupe de plus de 11 personnes (foyer de contamination) présente un risque d'exposition au COVID-19, un courriel contenant le nom et la date de naissance des personnes concernées est adressé à l'ARS.

Lorsqu'il s'agit d'une collectivité, l'application « CONTACT-COVID » permet de le renseigner au moyen d'une liste déroulante.

Lorsqu'il s'agit d'un patient zéro ayant été en contact avec au moins 11 personnes, l'application « CONTACT-COVID » ne permet pas d'identifier ces cas de manière directe. Dans ce cas, seule l'ouverture de la fiche du patient zéro permet de constater le nombre total de cas contact associés à cette dernière.

Avons été informé que la CPAM de la Seine Saint Denis a pris contact avec un centre d'hébergement pour mineurs qui hébergeait un patient zéro testés positifs au COVID-19 afin de commencer le «contact tracing» du patient zéro. La CPAM de la Seine Saint Denis a parallèlement transmis l'information selon laquelle il y avait un potentiel « cluster » au sein de ce centre d'hébergement pour mineurs à l'ARS pour qu'elle assure la prise en charge.

En ce qui concerne le dénombrement des fiches présentes dans l'application « CONTACT-COVID »

Avons constaté la présence au sein de l'application « CONTACT-COVID » pour la France métropolitaine de :

- 2 139 fiches ayant l'état « non avéré », dont le plus ancien en date du 13 mai 2020 ;
- 6 020 fiches ayant l'état « en attente de diagnostic », dont la plus ancienne en date du 13 mai 2020 ;
- 7 376 fiches ayant l'état « clôturé », dont la plus ancienne en date du 3 juin 2020.

En ce qui concerne le contenu du champ adresse

Constatons que le champ adresse est utilisé par les agents enquêteurs de la CPAM afin d'y inscrire différentes informations : le suivi de l'envoi de sms, un numéro de téléphone secondaire, l'opposition d'un patient zéro à la divulgation de son identité au cas contact.

Sommes informés que des pratiques locales visant à fluidifier et éviter les réitérations d'envois d'informations sont tolérées. Ces pratiques prévoient que le champ adresse soit utilisé afin d'y indiquer si des SMS ont été envoyés ou y ajouter un numéro de téléphone secondaire.

Sommes informés par [redacted] CPAM n'est pas amenée à envoyer des courriers postaux dont l'adresse serait renseignée à partir de ce champ.

En ce qui concerne l'habilitation d'accès aux postes de travail

[redacted]

[redacted]

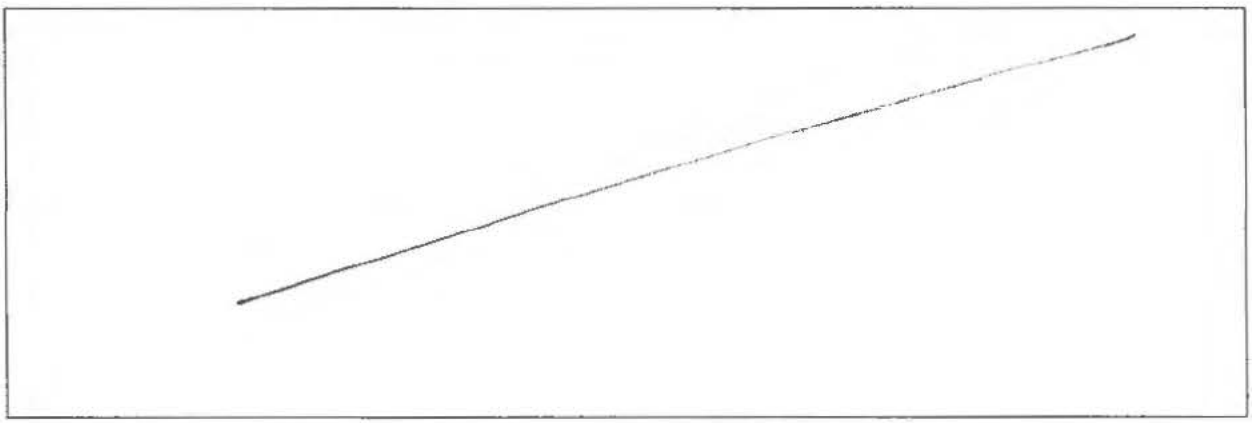
[redacted]

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]
-

À l'issue du contrôle, [redacted] ...rait les observations suivantes :



La mission de contrôle s'est terminée, ce jour, à 18h00;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé par [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]

PIECE N°3 : [redacted]

PIECE N°4 : [redacted]

PIECE N°5 : [redacted]

PIECE N°6 : [redacted]

PIECE N°7 : [redacted]

PIECE 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 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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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] dûment habilités à procéder à des missions de vérification sur place ;

En présence du [redacted] médecin expert 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 22 juillet 2020, dans les locaux de l'AGENCE REGIONALE DE SANTE ILE DE FRANCE, situés MILLENAIRE 2, 35 RUE DE LA GARE à PARIS (75019) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité, en la personne [redacted] de l'AGENCE REGIONALE DE SANTE ILE DE FRANCE, 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 :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle d[redacted] médecin expert.

En ce qui concerne l'ARS d'ILE DE FRANCE

[redacted] *ous informe des éléments suivants :*

Les ARS ont été créées par la loi HPST en avril 2010. Les ARS sont des établissements publics autonomes de l'Etat.

Elles assurent notamment la veille et la sécurité sanitaire ainsi que la prévention dans la santé.

Le budget de fonctionnement de l'ARS IDF est d'environ de 107 millions d'euros.

Elle compte 1 042 postes équivalents temps plein répartis à 55 % au siège de l'ARS IDF situé 35 RUE DE LA GARE à PARIS (75019) et 45 % au sein des délégations départementales.

[redacted]

Prenons copie de la présentation de l'ARS IDF.

En ce qui concerne le traitement de données à caractère personnel réalisé à partir de « contact covid »

[redacted] *nous informent des éléments suivants :*

L'ARS IDF intervient dans le « contact tracing » au niveau 3. Leur rôle est de prendre en charge les cas nécessitant une prise en charge spécifique (chaîne de transmission en milieu scolaire, établissements de santé, foyers…). L'ARS IDF définit également la période de contagiosité du patient zéro signalé et procède à la recherche des cas contacts de ce dernier.

Ce suivi mobilise entre 80 et 120 personnes à l'ARS IDF. L'ARS IDF reçoit quotidiennement entre 20 et 40 signalements de l'assurance maladie de nouveaux cas testés positifs. Elle reçoit quelquefois des signalements de l'assurance maladie concernant des « cas contacts » (passagers de transports aériens).

En ce qui concerne les modalités de réalisation du suivi dans le cadre du traitement de données à caractère personnel réalisé à partir de « contact covid »

[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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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 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 22 juillet 2020, dans les locaux de l'AGENCE REGIONALE DE SANTE ILE DE FRANCE, situés MILLENAIRE 2, 35 RUE DE LA GARE à PARIS (75019) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité, en la personne [redacted] de l'AGENCE REGIONALE DE SANTE ILE DE FRANCE, 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]

[redacted]

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert.

En ce qui concerne l'ARS d'ILE DE FRANCE

[redacted] *nous informe des éléments suivants :*

Les ARS ont été créées par la loi HPST en avril 2010. Les ARS sont des établissements publics autonomes de l'Etat.

Elles assurent notamment la veille et la sécurité sanitaire ainsi que la prévention dans la santé.

Le budget de fonctionnement de l'ARS IDF est d'environ de 107 millions d'euros.

Elle compte 1 042 postes équivalents temps plein répartis à 55 % au siège de l'ARS IDF situé 35 RUE DE LA GARE à PARIS (75019) et 45 % au sein des délégations départementales.

[redacted]

Prenons copie de la présentation de l'ARS IDF.

En ce qui concerne le traitement de données à caractère personnel réalisé à partir de « contact covid »

[redacted] *nous informent des éléments suivants :*

L'ARS IDF intervient dans le « contact tracing » au niveau 3. Leur rôle est de prendre en charge les cas nécessitant une prise en charge spécifique (chaîne de transmission en milieu scolaire, établissements de santé, foyers…). L'ARS IDF définit également la période de contagiosité du patient zéro signalé et procède à la recherche des cas contacts de ce dernier.

Ce suivi mobilise entre 80 et 120 personnes à l'ARS IDF. L'ARS IDF reçoit quotidiennement entre 20 et 40 signalements de l'assurance maladie de nouveaux cas testés positifs. Elle reçoit quelquefois des signalements de l'assurance maladie concernant des « cas contacts » (passagers de transports aériens).

En ce qui concerne les modalités de réalisation du suivi dans le cadre du traitement de données à caractère personnel réalisé à partir de « contact covid »

[redacted]

[redacted] *ous informent des éléments suivants :*

La cellule régulation reçoit les signalements de l'assurance maladie et des établissements de santé par courriel aux adresses suivantes :

- Pour l'assurance maladie : [redacted]
- Pour les établissements de santé : [redacted]

Chaque nouveau patient zéro nécessitant l'intervention de l'ARS IDF est à l'origine d'un nouveau signalement à cette dernière.

[redacted]

La cellule régulation transmet ensuite les signalements à des secteurs d'enquête territoriaux :

- le secteur d'enquête territorial de l'ouest regroupe les signalements provenant des départements suivants : 95, 78 et 92 ;
- le secteur d'enquête territorial du centre regroupe les signalements provenant des départements suivants : 75 et 93 ;
- le secteur d'enquête territorial de l'est regroupe les signalements provenant des départements suivants : 77, 91 et 94.

Le coordinateur du secteur d'enquête territorial correspondant va, à réception du signalement, faire une première lecture du signalement et ensuite l'affecter à un enquêteur.

Le courriel initial contenant très peu d'information, l'enquêteur va ensuite effectuer une recherche dans le logiciel SI-DEP puis dans le logiciel CONTACT COVID pour confirmer l'identité du patient zéro et sa positivité au test PCR.

Le nombre de dossiers journaliers attribués à l'enquêteur provient d'un tableau établi dans un fichier word ou dans un courriel contenant les signalements non traités de la veille et / ou de la boîte mail contenant les signalements du jour. Les enquêteurs priorisent les « clusters » les plus urgents qui doivent être traités dans la journée ainsi que les signalements non traités de la veille.

Prenons copie du tableau de signalements non traités du 21 juillet 2020 (courriel du mardi 21/07 à 18h37).

L'enquêteur peut être assisté d'un expert de la veille sécurité sanitaire (référent expert métier).

L'enquêteur propose des mesures de gestion individuelle (ex : arrêt de travail, prescription de PCR) et collective (ex : fermeture d'école, recommandation d'arrêt des festivités / rassemblements, prise d'un arrêté préfectoral) validées par l'expert de la veille sécurité sanitaire.

En cas de doute sur la mesure de gestion individuelle ou collective à prendre, le référent veille sécurité sanitaire, qui est souvent un infirmier, peut solliciter un médecin de veille pour valider son expertise.

S'agissant des signalements provenant de l'assurance maladie, un courriel est adressé à l'ARS IDF contenant *a minima* le nom et prénom du patient zéro.

[redacted]

S'agissant des signalements provenant d'un établissement de santé, l'application CONTACT COVID n'est pas utilisée par ce dernier. Les signalements sont transmis par des équipes dédiées de l'établissement de santé. Aucune donnée nominative n'apparait dans le courriel de transmission du signalement mais seulement le nombre de patients zéro et le nombre de cas contacts.

Une fois que le patient zéro est confirmé, l'enquêteur renseigne dans un fichier Excel, propre à chaque département, le résumé de l'enquête de suivi sans la présence de données nominatives. L'ARS IDF attribue un numéro identifiant (« ID ») à chaque foyer de contamination (« cluster »). L'ARS IDF nous informe que ce fichier ne contient aucune donnée médicale individuelle.

Prenons copie des fichiers de « suivi des clusters_75.xlsx » et « suivi des clusters _93.xlsx ». Demandons copie des fichiers de suivi des clusters des départements 77, 78, 91, 92, 94 et 95.

Chaque enquête donne lieu à l'ouverture d'un dossier par foyer de contamination (« cluster ») sur un serveur avec accès restreint. Chaque dossier comprenant notamment les éléments suivants : un questionnaire d'enquête sous un format Word, un tableau Excel qui recense l'identité du patient zéro et de l'ensemble de ses cas contacts ainsi qu'un fichier chiffré à destination de la collectivité reprenant ces informations [redacted] Le fichier est adressé à l'assurance maladie par l'intermédiaire de la messagerie sécurisée de santé pour que cette dernière renseigne les cas contacts dans l'application CONTACT COVID et procède, le cas échéant, à leur suivi individuel (mise en oeuvre des mesures individuelles de gestion).

L'ARS IDF utilise uniquement l'application CONTACT COVID en mode lecture et non en mode écriture. C'est la raison pour laquelle l'ARS IDF transmet le fichier à l'assurance maladie pour que cette dernière renseigne les cas contacts dans l'application CONTACT COVID.

La procédure de suivi dans le cadre du tracing de niveau 3 est considérée comme close lorsqu'aucun nouveau signalement n'est remonté dans un délai de 14 jours à compter du dernier signalement reçu.

En ce qui concerne le questionnaire d'enquête complété par les enquêteurs de l'ARS IDF

[redacted] *nous informent des éléments suivants :*

L'ARS IDF prend contact avec le :

- patient zéro lorsqu'il s'agit d'un « cluster » d'un vol aérien ;
- avec le patient zéro puis le médecin du travail lorsqu'il s'agit d'une entreprise ;
- avec le service de médecine préventive lorsqu'il s'agit d'établissement scolaire sans contacter au préalable le patient zéro. Ce service a la charge de déterminer les cas contacts et de les informer de la collecte de leur données dans le cadre du traitement « CONTACT COVID ». Pour cela, un document d'information rédigé par l'ARS IDF leur est remis par le médecin.

Dans le cadre de son enquête, l'enquêteur appelle les personnes à partir d'un tableau rédigé sous Word ou dans un courriel synthétisant les signalements non traités de la veille.

En ce qui concerne le responsable des traitements mis en œuvre par l'ARS IDF dans le cadre des traitements de « contact tracing » de niveau 3

[redacted] *nous informe des éléments suivants :*

[redacted]

Chaque ARS est responsable des traitements des données qu'elle collecte et traite dans le cadre du « tracing » de niveau 3 du traitement « CONTACT COVID » et de tous traitements liés.

Chaque ARS gère l'organisation et le détail de la mise en œuvre du « tracing » de niveau 3 dans le cadre du traitement « CONTACT COVID » et de tous traitements liés.

Prenons copie d'une extraction du registre des activités de traitement liées à la mise en œuvre de « CONTACT COVID » et de tous traitements liés.

Prenons copie de la procédure de gestion des habilitations.

En ce qui concerne la base légale des traitements de « contact tracing » de niveau 3

[redacted] *nous informe des éléments suivants :*

L'ARS IDF considère que la base légale du traitement « CONTACT COVID » et de tous traitements liés est la mission d'intérêt public (L.1431-2 1)-b du Code de la santé publique).

En ce qui concerne les relations de sous-traitance avec l'ARS IDF

[redacted] *nous informe des éléments suivants :*

L'ARS IDF a recours à SANTE PUBLIQUE FRANCE (SPF) afin d'effectuer du suivi épidémiologique (le but est d'identifier / expliquer des phénomènes de circulation de l'épidémie).

Prenons copie de la convention entre l'ARS IDF et SPF.

L'ARS IDF a ouvert des droits à des agents de SPF. Ces derniers disposent de droits d'accès aux dossiers où sont stockés les signalements. Ainsi, les agents de SPF ont accès à toutes les données prévues par l'article 2 du décret n°2020-551 du 12 mai 2020. Les agents de SPF sont dans les locaux de l'ARS IDF. Les agents de SPF accèdent à « CONTACT COVID ».

Une convention de sous-traitance a été signée entre l'ARS IDF et SPF.

La DNUM est sous-traitante de l'ARS IDF car il y a un projet en cours pour donner l'accès au logiciel [redacted] L'ARS IDF nous informe que ce projet n'est pas opérationnel à ce jour et que les agents de l'ARS IDF n'ont pas accès au logiciel [redacted] Le logiciel [redacted] a pour objet l'enregistrement, l'investigation et le suivi épidémiologique par les ARS des cas confirmés de COVID-19 et des cas contacts, en vue d'identifier les chaînes et cas groupés de contamination et de prendre les mesures destinées à limiter la propagation de l'épidémie.

Une convention de sous-traitance a été signée entre l'ARS IDF et la DNUM.

Prenons copie du projet de convention entre l'ARS IDF et la DNUM en cours de rédaction.

L'AP-HP est sous-traitante de l'ARS IDF pour le suivi de l'isolement dans le cadre du « contact tracing » de niveau 3.

Prenons copie de la convention conclue entre l'ARS IDF et l'AP-HP.

L'ARS IDF a recours au groupement de coopération sanitaire SESAN.

[redacted]

Prenons copie de la convention conclue entre l'ARS IDF et GCS SESAN.

En ce qui concerne les logiciels utilisés par l'ARS IDF aux fins de mettre en œuvre les traitements de données « CONTACT COVID » :

[redacted] *nous informent des éléments suivants :*

L'ARS IDF utilise les logiciels « CONTACT COVID » et « SI-DEP » dans le cadre du « contact tracing » de niveau 3.

L'ARS IDF utilise le logiciel « SI-VIC » pour dénombrer les victimes en réanimation atteintes du COVID-19 mais cette tâche intervient hors du cadre du « contact tracing » de niveau 3.

En ce qui concerne les durées de conservation des fichiers Excel qui recensent les cas contacts et patient zéro

[redacted] *nous informent des éléments suivants :*

Les fichiers utilisés dans le cadre du suivi des cas contact (données nominatives) sont stockés sur un serveur de fichier hébergé par l'ARS IDF.

La suppression des fichiers est prévue à l'issue d'un délai de trois mois à compter de la collecte des données sauf si l'évènement est encore ouvert (continue d'avoir des signalements).

Cette suppression est prévue manuellement dans un premier temps. L'ARS IDF est dans l'attente des travaux du service des archives du MSS afin de déterminer les modalités de suppressions et d'archivage définitif des données.

Les fichiers de suivi EXCEL ont vocation à être conservés sans limite de temps.

En ce qui concerne l'information

[redacted] *nous informent des éléments suivants :*

Lorsque l'enquêteur contacte le patient zéro ou le médecin du travail ou le service de médecine préventive, il s'appuie sur l'instruction de la DGS « MIN SANTE 99 version 2 », une formation initiale établie par l'ARS IDF ainsi que sur le questionnaire d'enquête. Une information orale a également été délivrée par les coordinateurs aux agents enquêteurs.

Prenons copie du support de formation initial établi par l'ARS IDF, de l'instruction « MIN SANTE 99 version 2 » ainsi que sur le questionnaire d'enquête.

Le consentement du patient zéro à la divulgation de son identité à la structure qui l'emploie ou du médecin du travail, est recueilli auprès de celui-ci.

Le consentement du patient zéro à la divulgation de son identité aux cas contacts n'est pas recueilli par l'ARS IDF. [redacted] nous informe que l'ARS IDF ne divulgue jamais l'identité du patient zéro aux cas contact dans leurs processus.

[redacted] [redacted] [redacted]

Par principe, l'ARS IDF ne contacte pas directement les cas contacts sauf par exception lorsqu'il s'agit de cas contacts ayant pris l'avion et ayant été en contact avec un patient zéro. Ces derniers sont contactés par [redacted] qui adresse à l'ARS IDF les fiches de traçabilité préalablement remplies par tous les voyageurs dans le cadre du règlement sanitaire international.

Le médecin du service de médecine préventive a la charge de déterminer les cas contacts et d'informer ces derniers de la collecte de leurs données dans le cadre du traitement « CONTACT COVID ». Pour cela, un document d'information rédigé par l'ARS IDF leur est remis par le médecin.

En ce qui concerne l'exercice des droits des personnes

[redacted] *nous informent des éléments suivants :*

Aucune procédure d'exercice des droits « Informatique et Libertés » des personnes n'a été formalisée au sein de l'ARS IDF concernant les traitements de « contact tracing » de niveau 3.

Une information sur les droits des personnes est disponible sur le site internet de l'ARS IDF.

Cette information comprend la mention d'une adresse électronique dédiée.

Avons procédé aux constatations suivantes :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert.

A notre demande, [redacted] accède au serveur de fichier utilisé dans le cadre du « contact tracing ».

Constatons qu'un poste dédié est utilisé pour accéder à l'application CONTACT COVID.

Constatons qu'un compte non nominatif, spécifique à chaque poste dédié, est utilisé afin d'ouvrir une session WINDOWS. Ce compte est également utilisé afin d'accéder à l'application CONTACT COVID.

Sommes informés que l'ASSURANCE MALADIE a configuré et installé les postes dédiés.

Sommes informés que les fichiers de traçabilité « Suivi des clusters_75.xlsx » et « Suivi des clusters_93.xlsx » ne contiennent pas de données de santé nominatives (voir pièces).

Constatons que les informations relatives aux patients zéro, issues des signalements, sont retranscrites sur un cahier.

Sommes informés que les documents papiers sont ultérieurement détruits au broyeur.

Constatons que le courriel de signalement, transmis en clair et envoyé depuis l'adresse [redacted] vers l'adresse [redacted] contenu dans le fichier « TR Objet Passage niveau 2 à niveau 3.msg » pris en copie par [redacted] contient le nom, prénom et la date de naissance du patient zéro.

Constatons que le courriel envoyé depuis l'adresse [redacted] vers l'adresse [redacted] contenu dans le fichier « RE Contact-

[redacted]

tracing Oran Paris.msg » pris en copie par [redacted] contient le mot de passe du fichier chiffré contenant l'identité d'un cas confirmé envoyé précédemment par le même biais.

Constatons la présence de références au logiciel [redacted] dans le fichier « Suivi des clusters_75.xlsx » (voir pièces).

Sommes informés qu'une instance du logiciel [redacted] propre à l'ARS IDF, a été utilisée brièvement mais n'est plus utilisée dans l'attente du déploiement de l'instance [redacted] nationale.

Sommes informés qu'en l'absence de médecin du travail, l'enquêteur peut être amené à contacter directement l'établissement dans lequel un patient zéro a été identifié.

Mentionnons que [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées [redacted] sur un support chiffré [redacted]

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 :

- copie des fichiers de suivi des clusters des départements 77, 78, 91, 92, 94 et 95.

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

La mission de contrôle s'est terminée, ce jour, à 19h40 ;

[redacted] [redacted] [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]

[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.

Mentionnons que le [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, par le [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.

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]

PIECE N°10 : [redacted]

PIECE N°11 : [redacted]

PIECE N°12 : [redacted]

PIECE N°13 : [redacted]

PIECE N°14 : [redacted]

PIECE N°15 : [redacted]

PIECE N°16 : [redacted]

PIECE N°17 : [redacted]

[redacted]

PIECE N°18 : [redacted]

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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] habilités à procéder à des missions de vérification sur place ;

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

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 14 octobre 2020, à 9h30, au sein des locaux de l'AGENCE REGIONALE DE SANTE GRAND EST, situés 3 Boulevard Joffre à Nancy (54000) et avons été reçus immédiatement ;

Le responsable des lieux au sens du décret précité, en la personne [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'AGENCE REGIONALE DE SANTE GRAND EST

Sommes informés des éléments suivants :

L'ARS GRAND EST est issue de la fusion de 3 régions en janvier 2016. Elle est répartie sur trois sites : NANCY, qui est le siège de l'ARS, ainsi que STRASBOURG et CHALONS EN CHAMPAGNE. Elle regroupe 10 délégations territoriales.

Dès le début de l'épidémie, l'ARS GRAND EST s'est appuyée sur la cellule « POINT FOCAL REGIONAL » afin de centraliser les signalements relatifs au COVID-19.

A partir du mois de mai 2020, une organisation complémentaire a été mise en place afin de tester, tracer, isoler les patients positifs au COVID-19. Chaque action est réalisée par une cellule dédiée.

Une mission COVID a été créée au sein de l'ARS GRAND EST afin d'assurer le suivi de l'épidémie tout en poursuivant ses autres missions.

L'ARS GRAND EST a un effectif de 676 équivalents temps plein et une dotation récente en 2020 de 12 équivalents temps plein temporaires hors plafond.

Le budget d'intervention pour l'année 2019 de l'ARS GRAND EST est de 383,7 millions d'euros. Ce budget d'intervention est issu du FIR.

Le « contact tracing » de niveau 3 mis en œuvre par l'ARS GRAND EST consisté à :

- réceptionner des signaux centralisés au niveau du point focal régional ;
- effectuer une analyse de risque pour déterminer le périmètre du contact tracing à réaliser à l'intérieur de la structure où un patient 0 a été identifié ;
- réaliser un appui aux mesures de gestion (ex : conseil sur la fermeture des locaux, faut-il faire un dépistage étendu sur l'ensemble du campus etc).

S'agissant des indicateurs régionaux de l'évolution du COVID-19 relevés ces dernières semaines, ceux-ci sont inférieurs aux indicateurs nationaux pour la région GRAND EST.

Durant l'été 2020, l'ARS GRAND EST recevait environ 15 à 20 signaux par jour qui nécessitaient une investigation de niveau 3.

Un signal est un signalement d'un patient zéro ou d'une situation sanitaire nécessitant de réaliser un « contact tracing » de niveau 3. Un signal est analysé au titre du niveau 3 lorsqu'il y a un nombre de contact à risque élevé ou une situation de cluster au-delà de trois cas positifs.

Depuis la rentrée scolaire, le nombre de signaux reçus par l'ARS GRAND EST a évolué très rapidement de 60 signaux à 100 signaux par jour. A ce jour, l'ARS GRAND EST reçoit environ 100 à 120 signaux par jour, ce qui mobilise entre 100 à 140 personnes.

Prenons copie de la convention d'objectif, de la présentation de l'ARS, de l'organigramme de l'ARS GRAND EST, du schéma d'organisation du « contact tracing » de niveau 3.

En ce qui concerne le responsable des traitements mis en œuvre par l'ARS GRAND EST dans le cadre des traitements de « contact tracing » de niveau 3 et la base légale des traitements de « contact tracing » de niveau 3

Sommes informés des éléments suivants :

L'ARS GRAND EST se considère responsable des traitements liés à la mise en œuvre de toutes les données d'identification qui permettent de mener le travail d'investigation des agents enquêteurs dans le cadre du « contact tracing » de niveau 3.

La base légale des traitements liés à la mise en œuvre du « contact tracing » de niveau 3 est l'exécution d'une mission d'intérêt public.

L'ARS GRAND EST n'a pas, à ce jour, réalisé d'AIPD sur les traitements liés à la mise en œuvre du « contact tracing » de niveau 3 en raison de la charge de travail engendrée par l'épidémie du COVID-19. L'ARS GRAND EST a identifié la nécessité de rédiger une AIPD sur ces traitements.

Prenons copie d'une extraction du registre des activités de traitement liées à la mise en œuvre de « CONTACT COVID » et du tracing de niveau 3.

En ce qui concerne l'activité de « tracing » de l'ARS GRAND EST :

Sommes informés des éléments suivants :

Les signaux transmis à l'ARS GRAND EST sont reçus par deux canaux :

- les signalements émanent de la DRSM sont réceptionnés sur une messagerie sécurisée de santé à l'adresse suivante : [redacted] Le signalement se présente sous la forme d'un courriel comprenant un certain nombre d'informations sur le patient zéro : nom, prénom, date de naissance, numéro de téléphone, raisons qui nécessitent le passage du dossier au niveau 3 du dispositif de « contact tracing ».

  Depuis environ 10 jours, la CNAM a changé son organisation et transmet uniquement le numéro de la fiche du patient zéro dans l'application « Contact Covid ». Cette transmission ne contient pas de données directement nominatives. Ces transmissions ne sont plus systématiquement adressées par une messagerie sécurisée de santé.

  L'échange en interne sur le patient zéro et l'identification des cas contacts du patient zéro (régulation des signalements) se fait au moyen d'une boite aux lettres interne de régulation : [redacted]

 Paraphes [redacted]

- une autre boîte aux lettre réceptionne l'ensemble des alertes de droit commun et pas seulement celles relatives aux signalements du COVID-19 à l'adresse suivante : [redacted] Elle réceptionne notamment les signalements reçus par l'Education nationale, les entreprises et les établissements de santé.

  Depuis une dizaine de jours, les fichiers nominatifs émanant des établissements scolaires et universitaires ne sont plus transmis à l'ARS GRAND EST. Ils sont directement transmis aux CPAM.

Chaque signal entrant via ces deux canaux donne lieu à la création d'un numéro par le SI-VSS, qui est reporté dans un tableau de monitoring (application « MONITORING CLUSTER »). Ce numéro va suivre le cycle de vie du signalement.

Le SI-VSS est un outil de traitement des signalements de la veille sanitaire. Il s'agit d'un outil qui n'est pas spécifique au COVID-19 et qui était déjà utilisé avant le COVID-19. Cet outil a été mis à disposition de l'ARS GRAND EST par le ministère des Solidarités et de la Santé.

Le tableau de monitoring a été mis en place et développé spécifiquement pour la gestion du COVID-19 par l'ARS GRAND EST.

Ces signalements sont ensuite transférés à une boite aux lettres dite de « REGULATION » [redacted] Un régulateur est ensuite chargé d'adresser le signalement à des investigateurs au sein de l'ARS GRAND EST ou à un sous-traitant, la société [redacted]

Dans le cas où le signalement est adressé à un investigateur de l'ARS GRAND EST, celui-ci est adressé sur sa boite de messagerie professionnelle nominative.

Dans le cas du recours à la société sous-traitante [redacted] le signalement est adressé sur une boîte aux lettres dédiée. [redacted] réceptionne et traite le signalement, si besoin avec l'appui d'un superviseur de l'ARS qui est quotidiennement en place pour fluidifier le traitement réalisé par le prestataire.

Une fois que le signalement a été adressé à un investigateur (en interne à l'ARS ou à la société [redacted], celui-ci contacte le patient zéro ou le cas contact.

Dans le cas de l'appel à un patient zéro, l'investigateur est chargé d'identifier les cas contacts du patient zéro au sein de l'évènement ayant le « contact tracing » de niveau 3.

Les informations sur les cas contacts du patient zéro sont répertoriées dans un fichier Excel. Ce fichier Excel est ensuite adressé à la CNAM. L'ARS GRAND EST dispose de droit d'écriture dans l'application « CONTACT COVID » mais ne l'utilise qu'en lecture. L'ARS GRAND EST précise que le fait de remplir les cas contacts du patient zéro directement dans l'application « CONTACT COVID » serait plus chronophage que d'utiliser un fichier Excel et de le transmettre à la CNAM.

L'entretien téléphonique a également pour objet de rappeler les règles de sécurité sanitaire à adopter (isolement) et pour orienter, le cas échéant, les personnes concernées vers la cellule technique d'appui à l'isolement mise en œuvre par la Préfecture (ci-après CTAI).

L'ARS GRAND EST et la société [redacted] ne transmettent pas les coordonnées des personnes concernées à la CTAI. C'est la personne concernée qui doit faire la démarche de contacter la CTAI.

En ce qui concerne le recours au sous-traitant SERENITY MEDICAL SERVICES

Sommes informés des éléments suivants :

Le choix d'externaliser une partie du « contact tracing » de niveau 3 auprès de la société [redacted] a été fait pendant l'été car l'ARS GRAND EST a été touchée plus précocement et plus fortement que les autres régions. Il s'agit d'un choix qui est réversible à tout moment en cas de problème de qualité ou si le contexte ne le justifie plus.

Le recours à un prestataire est autorisé par l'article 14 du décret n°2020-551 du 12 mai 2020.

L'ARS GRAND EST a établi un cahier des charges à destination de la société [redacted] Ce cahier des charges a été soumis au ministère des Solidarités et de la Santé. Ce dernier a validé le principe de recourir à un sous-traitant.

Afin de créer des comptes dédiés aux investigateurs salariés de la société [redacted] l'ARS GRAND EST a notifié la CNAM. Cette dernière a validé le principe de recourir à un sous-traitant et a autorisé la création de ces comptes.

Demandons la copie du contrat avec [redacted] et du cahier des charges.

En ce qui concerne l'utilisation du logiciel [redacted] dans la cadre des traitements de « contact tracing » de niveau 3

Sommes informés des éléments suivants :

L'ARS GRAND EST dispose d'accès au logiciel [redacted] mais ne l'utilise pas à ce jour.

L'ARS GRAND EST précise que le logiciel [redacted] ne répond pas à l'ensemble de ses besoins dans le cadre du « contact tracing » de niveau 3. Des demandes d'évolution ont été effectuées auprès du ministère des Solidarités et de la Santé.

Demandons une copie du tableau des demandes d'évolution de l'outi[redacted]

En ce qui concerne le recueil du consentement à la divulgation de l'identité du patient zéro au cas contact

Sommes informés des éléments suivants :

L'ARS GRAND EST recueille le consentement du patient zéro à la divulgation de son identité au cas contact même si cette information figure déjà dans l'application « CONTACT COVID ».

L'ARS GRAND EST a mis en œuvre un questionnaire et plusieurs procédures (intitulées « conduites à tenir » par type d'établissement) pour assister l'investigateur dans le cadre de son entretien téléphonique au patient zéro / cas contact.

Le questionnaire ainsi que le fichier Excel prévoient le recueil du consentement à la divulgation de l'identité du patient zéro au cas contact.

Les circulaires « MIN 99 », « MIN 155 » et « MIN 156 » prévoient la répartition du recensement des cas contacts entre les ARS, la CNAM et les CPAM. Ces circulaires prévoient

notamment la possibilité de renvoyer à la CNAM ou aux CPAM la tâche d'appeler les cas contact lorsqu'il y a un nombre trop important d'appels à effectuer. Il n'y a pas de procédure établie qui a fixé un nombre à partir duquel le dossier doit être renvoyé à l'assurance maladie.

Demandons copie des circulaires « MIN 99 », « MIN 155 » et « MIN 156 », du questionnaire et des procédures intitulées « conduites à tenir » par type d'établissement.

En ce qui concerne l'information des personnes sur le traitement de leurs données dans le cadre du « contact tracing » de niveau 3 et l'exercice de leurs droits « Informatique et Libertés »

Sommes informés des éléments suivants :

Les investigateurs de l'ARS GRAND EST s'appuient sur une procédure générale de conduite d'entretien complétée par plusieurs procédures spécifiques (intitulées « conduites à tenir » par type d'établissement) pour mener l'entretien téléphonique avec le patient zéro / cas contact.

L'ARS GRAND EST indique qu'elle ne délivre pas l'ensemble de l'information à fournir au titre du RGPD et du décret n°2020-551 du 12 mai 2020 sur le traitement des données à caractère personnel dans le cadre du « contact tracing » de niveau 3. Elle précise que cela est dû à un manque de temps au regard du grand nombre d'appels à effectuer et à un objectif de pédagogie à atteindre vis-à-vis des patients zéro et cas contact qui impliquent de simplifier le propos pour passer les messages principaux.

Un courriel est envoyé au patient zéro / cas contact à l'issu de l'entretien téléphonique. Celui-ci contient une fiche relative aux consignes sanitaires à respecter.

En ce qui concerne les durées de conservation

Sommes informés des éléments suivants :

L'ARS GRAND EST est en cours de formalisation d'une procédure de durées de conservation des données relatives aux traitements mis en œuvre par l'ARS GRAND EST dans le cadre des traitements de « contact tracing » de niveau 3. Cette procédure prévoit à ce jour les durées suivantes :

- trois mois à compter de la collecte pour les données nominatives ;
- six mois à compter de la collecte pour les données anonymes.

Cette procédure n'est pas implémentée à ce jour. Les données collectées depuis le 14 mai 2020, date de la mise en œuvre de l'activité de « contact tracing » de niveau 3, n'ont pas été supprimées.

Des travaux sont en cours avec le ministère des Solidarités et de la Santé afin de déterminer quels types de données seront archivés définitivement à l'issue des durées de conservation définies.

En ce qui concerne la relation de l'ARS GRAND EST avec la DNUM

Sommes informés des éléments suivants :

Le tableau de monitoring est hébergé sur un serveur de fichiers de l'ARS GRAND EST.

Les fichiers Excel contenant les données des patients zéro et de ses cas contacts sont stockés sur un serveur « SHAREPOINT » mis à disposition par la DNUM.

La DNUM ne dispose pas d'une certification d'hébergeur de données de santé. Des travaux ont été menés avec la DNUM afin de faire héberger le tableau de monitoring ainsi que les fichiers Excel par un organisme certifié.

Demandons copie de la certification d'hébergeur de données de santé de l'organisme retenu pour héberger le tableau de monitoring ainsi que les fichiers Excel.

En ce qui concerne la relation de l'ARS GRAND EST avec SANTE PUBLIQUE FRANCE (ci-après SPF)

Sommes informés des éléments suivants :

SPF intervient auprès de l'ARS GRAND EST pour apporter notamment son expertise dans le traitement des cas complexes. Dans ce cadre-là, des réunions téléphoniques spécifiques sont organisées entre l'ARS GRAND EST et SPF pour superviser les mesures prises par l'ARS GRAND EST.

Avant d'être communiqué publiquement, l'existence d'un cluster est validée conjointement par l'ARS GRAND EST et SPF.

En ce qui concerne la sécurité des données

Sommes informés des éléments suivants :

Depuis le mois de juillet 2020, la CNAM a fourni un accès à l'application « CONTACT COVID » accessible à partir d'une URL dédiée permettant l'accès à distance. Avant la mise en œuvre de cet accès, l'accès à l'application « CONTACT COVID » nécessitait un poste dédié.

L'authentification à l'application « CONTACT COVID » repose sur un mot de passe et un nom d'utilisateur.

Un administrateur dans chaque département renseigne l'adresse de l'agent pour lequel il souhaite créer un compte. Un lien de validation valable 24 heures est envoyé par courriel à l'agent. Ce lien permet à l'agent de définir son mot de passe. Chaque administrateur peut créer 10 comptes utilisateurs.

Chaque utilisateur et administrateur est habilité par une décision du directeur général de l'ARS GRAND EST.

Toutes les deux semaines, une revue des comptes est réalisée au sein de l'ARS GRAND EST.

L'ARS GRAND EST met à disposition de la société [redacted]s postes informatiques pour l'accès aux applications « SI-DEP » et « CONTACT COVID ». Huit comptes nominatifs à destination des investigateurs de la société [redacted] au sein de l'application « CONTACT COVID » sont également créés.

Le tableau de monitoring est accessible depuis un dossier partagé à accès restreint administré et hébergé par l'ARS GRAND EST. Aucune authentification supplémentaire n'est nécessaire pour accéder au tableau de monitoring. Le tableau de monitoring ne dispose pas de profil utilisateur.

Les comptes « WINDOWS » permettant l'accès au dossier contenant le tableau de monitoring sont nominatifs [redacted]

Avons procédé aux constatations suivantes :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert.

A notre demande [redacted] accède à la boîte aux lettres « veille sanitaire » et recherche les courriels qui lui sont des destinées par le régulateur.

Sommes informés qu'à compter du 15 octobre 2020, seuls les régulateurs auront accès à la boîte aux lettres dédiée à la régulation des signaux : [redacted]

Sommes informés qu'à compter du 15 octobre 2020, les signalements reçus sur cette nouvelle boîte aux lettres seront directement transmis par les régulateurs aux investigateurs dans leur boîte aux lettres personnelles.

A notre demande, [redacted] affiche différents signaux reçus de la part :

- de deux crèches ;
- d'une CPAM.

Constatons que, par l'intermédiaire de la boîte aux lettres « alerte », un courriel a été reçu pour un cas positif d'une salariée d'une crèche. La directrice de la crèche a contacté par téléphone et par courriel l'ARS GRAND EST afin de communiquer l'identité de la salariée testée positive au COVID-19.

A notre demande, [redacted] se connecte au tableau de monitoring et documente sa progression à l'aide de captures d'écran.

A notre demande, [redacted] se connecte à l'application « CONTACT CIVID » et documente sa progression à l'aide de captures d'écran.

Constatons qu'entre le 1er mai 2020 et le 14 octobre 2020, 4 131 fiches ont été enregistrées dans le tableau de monitoring.

A notre demande, [redacted] se connecte à l'application SI-VSS et documente sa progression à l'aide de captures d'écran.

Constatons qu'entre le 20 mai 2020 et le 22 mai 2020, 69 fiches ont été enregistrées dans l'application SI-VSS pour la région GRAND EST.

Constatons qu'au jour du contrôle, 3 563 fiches liées au COVID-19 sont « ouvertes » dans l'application SI-VSS pour la région GRAND EST.

A notre demande, [redacted] se connecte au serveur « SHAREPOINT » hébergeant les fichiers Excel contenant les patients zéro ainsi que leurs cas contact et documente sa progression à l'aide de captures d'écran.

Constatons que la présence de 10 dossiers pour chaque département de la région Grand Est. Chaque dossier contient des fichiers Excel recensant les patients zéro ainsi que leurs cas contact.

Constatons que les plus anciens fichiers Excel recensant les patients zéro ainsi que leurs cas contact au sein du département 55 datent du 13 juin 2020.

Mentionnons que [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe ;

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 :

- tout document encadrant les relations contractuelles entre l'ARS GRAND EST et le ministère des Solidarités et de la Santé s'agissant de l'application SI-VSS ;
- certification d'hébergeur de données de santé de l'organisme retenu pour héberger le tableau de monitoring ainsi que les fichiers Excel.

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 19h40 ;

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

 Paraphes [redacted]

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

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

ANNEXE 1 :

INVENTAIRE DES PIÈCES RECUEILLIES

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

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

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

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

Mentionnons que le [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, par le [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.

PIECE N°1 : [redacted]

- [redacted]

PIECE N°2 : [redacted]

Paraphes [redacted]

[redacted]

PIECE N°3 : [redacted]

[redacted]

Paraphes [redacted]

- [redacted]

PIECE N°4 : [redacted]

- [redacted]

PIECE N°5 : [redacted]

- [redacted]

PIECE N°6 : [redacted]

- [redacted]

Paraphes [redacted]

- [redacted]

PIECE N°7 : [redacted]

- [redacted]

PIECE N°8 [redacted]

- [redacted]

PIECE N°9 : [redacted]

Paraphes [redacted]

- [redacted]

PIECE N°10 : [redacted]

- [redacted]

PIECE N°11 : [redacted]

- [redacted]

Paraphes [redacted]

- [redacted]

PIECE N°12 : [redacted]

- [redacted]

PIECE N°13 : copie sur support informatique d'un dossier intitulé "Procedures" contenant 19 documents :

- [redacted]

- [redacted]

PIECE N°14 : [redacted]

- [redacted]

PIECE N°15 : [redacted]

- [redacted]

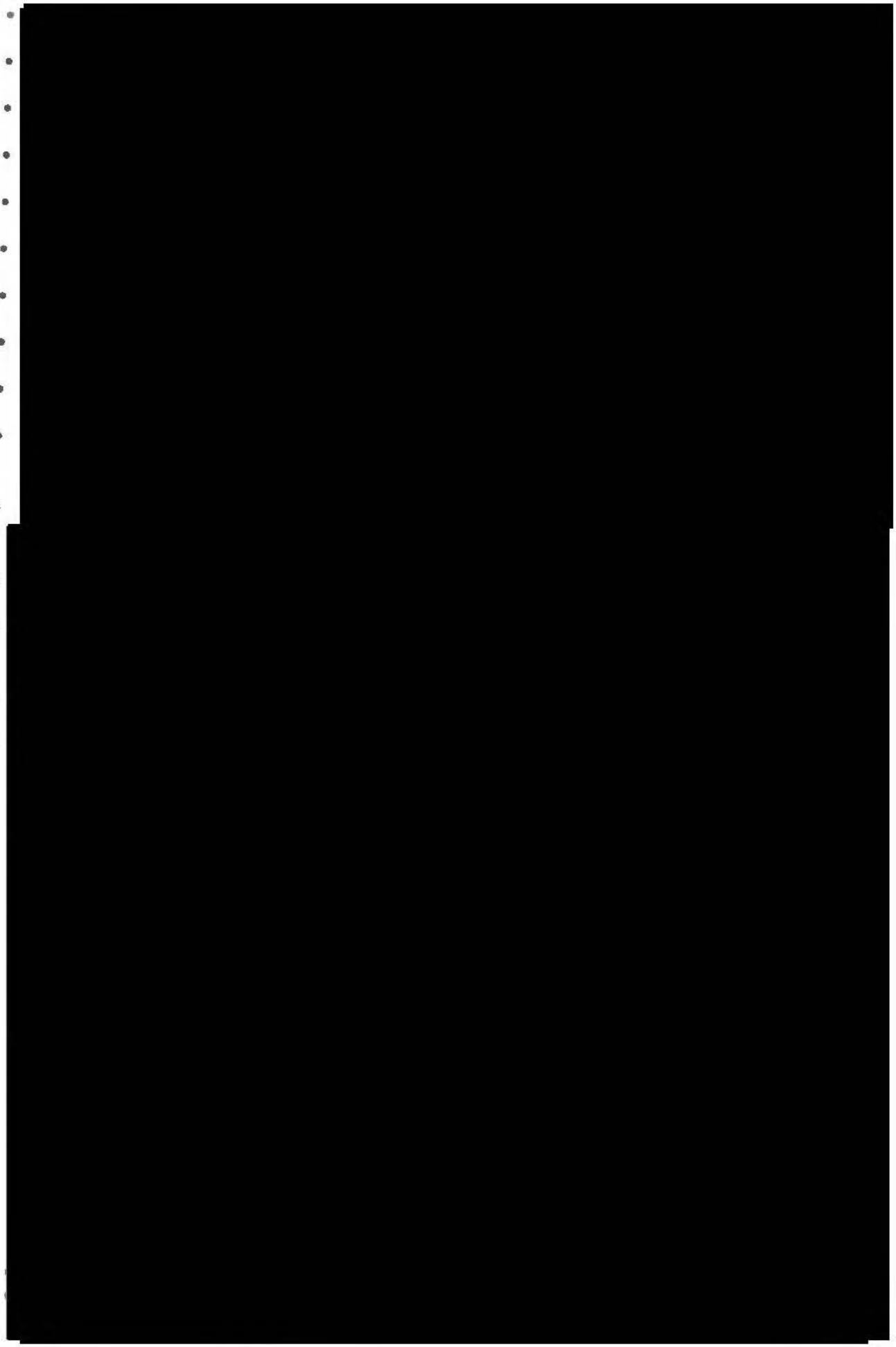
PIECE N°16 : [redacted]

- [redacted]

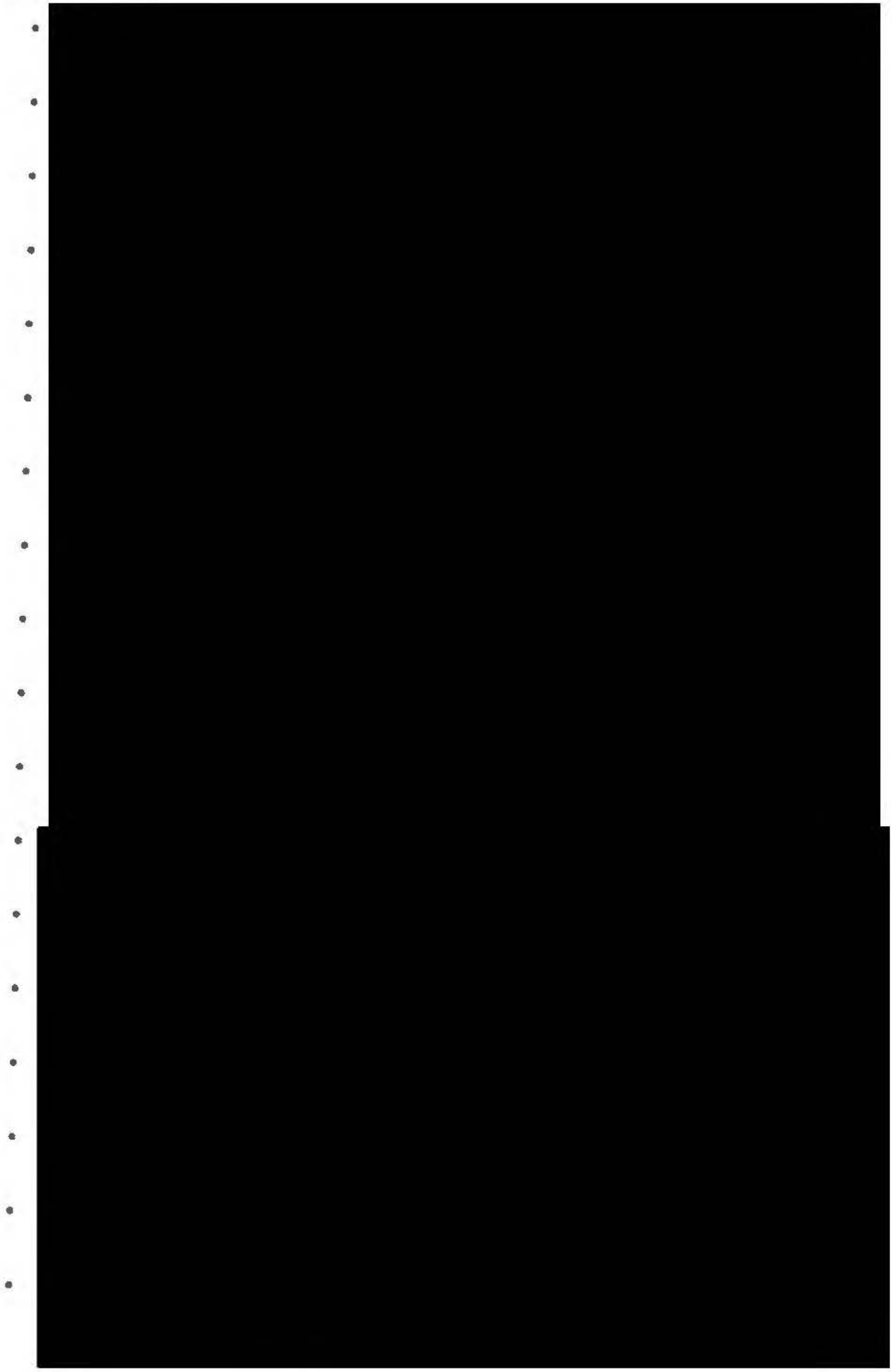
PIECE N°17 : [redacted]

- [redacted]

Paraphes NS TG BAH nc AR



Paraphes



Paraphes

- [redacted]

PIECE N°18 : [redacted]

- [redacted]

PIECE N°19 : [redacted]

Paraphes [redacted]

- [redacted]

PIECE N°20 : [redacted]

- [redacted]

Paraphes [redacted]

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

Paraphes [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

REÇU

À l'issue du contrôle, je reconnais avoir reçu une copie du procès-verbal de ce jour n° 2020-091/..5.., annexe comprise.

À NANCY

Le 14/10/2020

[redacted]

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

PROCÈS-VERBAL
AUDITION SUR CONVOCATION

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°2020-091C en date du 22 mai 2020, l'audition sur convocation a eu pour objet de procéder à la vérification de la conformité du traitement de données à caractère personnel dénommé « CONTACT COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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] dûment habilités à procéder à des missions de vérification ;

Procédons à l'audition sur convocation, le 10 novembre 2020, à partir de 9 heures 30 dans les locaux de la CNIL, [redacted] a été informée par courrier avec accusé réception le 22 octobre 2020 et au début de la présente audition, de l'objet des vérifications, de l'identité et de la qualité des personnes chargées de l'audition, ainsi que de son droit de se faire assister par un conseil de son choix ;

[redacted] déclare « je ne souhaite pas me faire assister pour cette audition » ;

[redacted]

[redacted]

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

Sommes informés des éléments suivants par [redacted]

En ce qui concerne la volumétrie des fiches créées dans l'outil CONTACT COVID

Lors de la création de l'outil CONTACT COVID, la CNAM envisageait la possibilité, au regard des prévisions épidémiologiques, de créer au maximum 60 000 fiches (patients zéros et cas contacts) par jour dans cet outil.

Depuis l'augmentation de la propagation du covid-19, les agents de la CNAM et des CPAM locales procèdent désormais à la création d'environ 120 000 fiches par jour. (*voir pièce*)

En ce qui concerne la suppression des données contenues dans CONTACT COVID

Conformément au décret du 12 mai 2020, les données contenues dans l'outil CONTACT COVID sont conservées trois mois à compter de leur collecte.

Depuis le 28 juillet 2020, un système de purge automatique des données contenues dans l'outil CONTACT COVID est mis en œuvre chaque jour. Ce système de purge supprime les données de plus de trois mois.

Les fiches des cas contacts ayant le statut « non avéré » sont supprimées

- soit manuellement, par un agent d'une CPAM sur initiative (après analyse de la nature du contact ayant permis de déterminer que la personne n'était pas cas contact au sens des recommandations sanitaires) ou sur demande de la personne concernée,
- soit automatiquement, par l'intermédiaire d'un système de purge quotidienne, au plus tard 24h à compter de leur changement de statut, depuis le 29 septembre 2020.

Les fiches créées ayant le statut « en attente de diagnostic » (patient 0 « supposé » créé par un médecin dans l'attente du résultat du test) sont supprimées automatiquement quinze jours à compter de leur création.

 [redacted] [redacted]

Il n'est pas possible de distinguer, en cas de suppression d'une fiche « cas contact non avéré », entre un cas contact non avéré réel et une personne ayant exercé son droit d'opposition au traitement.

En ce qui concerne l'envoi de SMS aux cas contacts contenant un lien URL [redacted]

Compte tenu de la recrudescence du nombre de personnes ayant été diagnostiquées positives au Covid-19, la CNAM a priorisé l'appel téléphonique à destination des patients zéros afin notamment de leur délivrer les informations utiles et de procéder à l'identification de leurs cas contacts.

Lorsque des personnes ayant été identifiées comme cas contacts n'ont pas pu être contactées par l'agent de la CPAM en charge de leur fiche, leur statut dans CONTACT COVID apparait comme « à contacter ».

Au regard de l'accroissement des volumes, les CPAM n'ayant plus la possibilité de procéder à l'appel téléphonique dans la journée, de tous les cas contacts (dont la fiche a le statut « à contacter »), la CNAM a pris l'initiative, entre le 23 octobre 2020 et 2 novembre 2020 inclus, de procéder à l'envoi d'un SMS identique aux cas contacts qui n'ont pas pu être joints dans la journée de la création de leur fiche.

Le SMS contenait un lien URL qui redirigeait vers une fiche relative à la conduite à tenir lorsque la personne a été contact à risque d'une personne avec une personne malade du COVID-19, rédigée par santé publique France et disponible sur le site web ameli.fr.

L'utilisation de la solution [redacted] a été choisie par la CNAM pour une question d'efficacité afin de raccourcir l'URL contenue dans le SMS. La CNAM précise que l'utilisation de la solution [redacted] n'avait pas pour objectif de tracer la prise de connaissance de la fiche par la personne destinataire du SMS. Qu'à ce titre, une seule URL raccourcie de type [redacted] a été utilisée, identique pour l'ensemble des SMS envoyés durant cette période.

En ce qui concerne le « nouveau » système d'envoi de SMS aux cas contacts

Dans le cadre de l'adaptation de sa stratégie au regard de l'accroissement des volumes de cas contacts, la CNAM a décidé de modifier ses modes de contacts en systématisant l'envoi des SMS aux cas contacts, à compter du 3 novembre 2020.

Lorsque la personne a été identifiée comme cas contact dans l'application CONTACT COVID, un SMS lui est adressé contenant un lien URL personnalisé (ou au représentant – ouvrant droit – d'une personne mineure). Cette URL contient un identifiant propre à l'utilisateur (chaque URL est unique pour un cas contact donné).

Cette URL redirige la personne concernée vers le site web « *declare.ameli.fr/sms* », développé spécifiquement par les services de la CNAM.

Par l'intermédiaire de plusieurs boutons de validation consécutifs, le site web vise à délivrer, aux cas contacts, l'ensemble des informations relatives à la conduite à tenir après avoir été en contact avec une personne malade du COVID-19.

Après avoir pris connaissance de ces informations, la personne destinataire du SMS (ou son représentant légal – ouvrant droit), doit cliquer sur le bouton « Terminer », après avoir coché la case « J'ai bien pris connaissance des consignes et je m'engage à les appliquer », contenu sur le site web « *declare.ameli.fr/sms* » pour qu'une information de bonne prise en compte remonte

 [redacted] [redacted]

vers l'outil CONTACT COVID. Les personnes n'ayant pas complété la démarche sont appelées par un agent des plateformes de contact-tracing.

Le statut de la fiche de la personne destinataire du SMS n'apparaît comme « appel abouti » que si cette dernière va jusqu'au bout de la démarche de validation prévue sur le site web « *declare.ameli.fr/sms* ».

Après avoir coché le bouton « Terminer », le site web précité affiche :

- un renvoi vers le site web *https://sante.fr/recherche/trouver/DepistageCovid* sur lequel figurent les centres de dépistages du Covid-19 ;
- les consignes pour solliciter un arrêt de travail et un renvoi vers le site web dédié à la déclaration d'un arrêt de travail ;
- les consignes relatives au retrait de masques en pharmacie.

La CNAM peut envoyer jusqu'à 5 SMS sur deux jours et demi à destination des personnes n'ayant pas cliqué sur le bouton « Terminer ».

La CNAM nous informe qu'elle n'a mis en œuvre aucun mécanisme d'opposition au rappel par SMS car elle considère que cela ne contrevient pas au droit d'opposition à figurer dans l'outil CONTACT COVID. Le droit d'opposition étant possible auprès du DPO ou via le conseiller d'une CPAM (pas de droit d'opposition « général » sur le traitement CONTACT COVID).

[redacted] se connecte successivement sur l'environnement de recette puis sur l'environnement de production relatif aux pages « declare.ameli.fr/sms » et documente sa navigation à l'aide de captures d'écran dont nous prenons copie.

Constatons, sur l'environnement de production des pages « declare.ameli.fr/sms » la présence d'un logiciel de « CAPTCHA » de la société [redacted] Prenons copie du code source de la page concernée.

Sommes informés que la version 3 de l'outil [redacted] est utilisée. Le code JavaScript inséré dans la page est le code fourni par la société [redacted] La CNAM ne transmet pas l'adresse IP de l'internaute. Au jour du contrôle, la CNAM utilise la version gratuite de l'outil [redacted]

La CNAM étudie la possibilité d'utiliser une autre solution, telle que [redacted] pour l'ensemble des outils mis en œuvre par la CNAM. Une étude comparative des différents outils de type « Captcha » est en cours.

<u>En ce qui concerne la création des comptes superadministrateurs, administrateurs et utilisateurs ayant accès à CONTACT COVID (portail partenaire)</u>

La CNAM a créé plusieurs profils de comptes permettant la création et l'accès à l'outil CONTACT COVID, à savoir des comptes superadministrateurs, des comptes administrateurs locaux et des comptes utilisateurs.

Un utilisateur superadministrateur est rattaché à une CPAM ou à la CNAM. Ce profil d'accès permet de visualiser l'ensemble des profils superadministrateurs, administrateurs locaux et utilisateurs, au niveau national.

Les comptes administrateurs locaux sont destinés aux établissements de santé et aux Agences régionales de santé (« ARS »). Ces comptes ont la possibilité de créer des profils « utilisateurs » (jusqu'à 10 comptes utilisateurs par administrateur local) destinés à utiliser l'application CONTACT COVID.

Le superadministrateur a lui seul la possibilité de créer un compte administrateur local. Il a la charge de former l'administrateur local à la création des comptes utilisateurs. Le superadministrateur s'assure de la prise de connaissance des CGU par l'administrateur local.

Avant la création d'un compte administrateur local, le superadministrateur contacte la structure, pour laquelle un accès au portail CONTACT COVID est nécessaire, afin de désigner un administrateur local, lui fait remplir une fiche d'information et vérifie son identité après avoir reçu copie de sa pièce d'identité. La copie de la pièce d'identité est immédiatement supprimée après la vérification de l'identité.

Afin d'avoir une meilleure maitrise de la création des comptes utilisateurs, la CNAM a exigé des ARS et des établissements de santé que le nom de domaine attaché à l'adresse de courriel de l'administrateur local et de ses utilisateurs soit identique.

Lors de la création de comptes utilisateurs, la CNAM considère qu'il appartient à l'administrateur local de délivrer à l'utilisateur les informations quant à l'usage de l'outil CONTACT COVID en lui faisant notamment signer un engagement unilatéral de confidentialité.

L'administrateur local ne voit que les comptes utilisateurs qu'il a créés.

Il y a au moins trois à quatre comptes superadministrateurs au sein de chaque CPAM.

Les comptes utilisateurs locaux sont liés au compte administrateur local ayant procédé à leur création.

La CNAM a formalisé un diaporama à destination des superadministrateurs et deux modes d'emploi à destination des administrateurs locaux d'une part et à destination des utilisateurs de l'outil CONTACT COVID d'autre part.

Les ARS sont responsables de comptes utilisateurs qu'ils créent conformément aux conventions conclues entre la CNAM et chaque ARS.

<u>En ce qui concerne l'authentification des superadministrateurs, administrateurs et utilisateurs à l'outil CONTACT COVID</u>

Pour les superadministrateurs, un système d'authentification forte est mis en œuvre (identifiant et carte agent).

[redacted]

[redacted]

[redacted]

Au jour du contrôle, il n'existe pas de supervision active des journaux aux fins d'identification de tentatives frauduleuses de connexion à un compte utilisateur sur le portail partenaire. En cas de suspicion de mésusage, il est possible de consulter les journaux pour procéder à des vérifications de sécurité.

Les règles de sécurité appliquées au portail partenaire sont les règles de sécurité générales mises en œuvre pour les applicatifs de l'Assurance Maladie.

Une étude a été conduite sur la faisabilité de la mise en œuvre d'une authentification forte des comptes partenaires. Cette étude conclut que les solutions envisagées, tant d'un point de vue technique que d'un point de vue organisationnel, en particulier dans les établissements de santé, présentent des difficultés de déploiement. Par exemple, la mise à disposition d'un téléphone portable ou d'un système de mot de passe à usage unique à chaque utilisateur du portail partenaire serait difficilement réalisable. Cela conduirait à limiter l'adoption de l'outil CONTACT COVID.

En ce qui concerne le déploiement des accès partenaires à l'outil CONTACT COVID

Depuis la mise en œuvre d'un portail partenaire à disposition des établissements de santé et des ARS, la CNAM a adressé des guides méthodologiques à ces derniers selon le type de profil utilisateur.

La CNAM a organisé une réunion auprès des fédérations hospitalières afin de leur rappeler d'une part, que les tableurs (fichiers « Excel ») créés par les établissements de santé à destination des CPAM locales avant l'accès au portail CONTACT COVID devaient être supprimés et, d'autre part, que les mentions d'information relatives à CONTACT COVID devaient être affichées au public au sein des établissements de santé.

Des affichettes d'information mises à jour vont être prochainement adressées par la CNAM aux fédérations hospitalières.

En ce qui concerne le traçage des cas contacts dans les établissements scolaires et les universités

À la suite de la mise en œuvre d'un nouveau protocole au niveau des établissements scolaires (lycée et collèges) définissant les modalités de recensement des cas contacts à risque, le traçage des cas contacts est désormais réalisé par l'établissement scolaire lui-même, sous le contrôle du ministère de l'Éducation nationale.

L'information à destination des patients zéros et des cas contacts est désormais réalisée par l'établissement scolaire lui-même.

Lorsque les cas contacts ont été identifiés, la liste de ces cas est adressée par l'établissement scolaire à la CPAM locale par l'intermédiaire d'un lien PÉTRA. La CPAM crée ensuite les fiches des cas contacts identifiés dans l'outil CONTACT COVID. Ces fiches sont immédiatement clôturées dès lors que l'information a déjà été délivrée par l'établissement scolaire sous le contrôle de l'Éducation nationale.

La personne chargée de lister les cas contacts n'est pas définie par l'Éducation nationale ni par la CNAM mais est placée sous la responsabilité du chef d'établissement. Elle est désignée en fonction de la taille de l'établissement scolaire et conformément au protocole ministère des Solidarités et de la Santé et ministère de l'Éducation nationale.

[redacted]

[redacted]

En milieu scolaire, le traçage des cas contacts d'un patient zéro doit être réalisé par l'établissement scolaire, sous le contrôle de l'Éducation nationale, ou de l'ARS en cas de suspicion de foyer de contamination. Le traçage des cas contacts d'un patient zéro hors de l'établissement scolaire est réalisé par la CNAM ou les CPAM locales.

Pour les universités, le système de traçage des cas contacts d'un patient zéro est réalisé par les ARS. La CNAM envisage prochainement la création de comptes partenaires pour des personnels des universités afin qu'ils puissent accéder directement à l'application CONTACT COVID, afin de tenir compte des modifications législatives et réglementaires à venir.

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 :

- Nombre de SMS envoyés par l'Assurance Maladie sur la période du 23 octobre au 2 novembre 2020, contenant un lien [redacted] aux personnes cas contact dont le statut dans l'application CONTACT COVID est « à contacter » ;
- Contenu et présentation du SMS envoyé à compter du 3 novembre 2020 jusqu'au 10 novembre inclus ;
- Nombre de personnes ayant cliqué sur le bouton « terminé » à la suite de leur visite de l'URL declare.ameli.fr/sms (sur la période du 3 novembre au 10 novembre inclus) ;
- Étude relative à la mise en place d'un système d'authentification forte des comptes utilisateurs sur le portail partenaire de l'application CONTACT COVID ;
- Matrice actualisée d'habilitation des profils utilisateurs créés dans CONTACT COVID ;
- Bilan des audits réalisés (par l'ANSSI, par un prestataire d'audit en sécurité des systèmes d'information, en interne, etc.) sur l'application CONTACT COVID et corrections apportées ;
- Analyse de risque actualisée pour l'application CONTACT COVID ;
- Résultat de l'étude relative à l'utilisation d'un captcha sur declare.ameli.fr./sms et, le cas échéant, calendrier de mise en œuvre d'un système de captcha alternatif à celui utilisé au jour du contrôle ;
- Message adressé, le cas échéant, aux fédérations hospitalières relatif à l'utilisation de tableurs dans la gestion des foyers de contamination ;
- Diaporama explicatif, *workflow*, modes d'emploi administrateurs locaux et utilisateurs d'utilisation de CONTACT COVID. ;
- Guide actualisé à destination des établissements de santé (médecins et laboratoires) et des ARS ;
- Modèle d'affichette mis à jour transmis aux établissements de santé ;
- Modalités d'échange (documentation, procédure) des tableurs contenant les cas contacts pour les foyers de contamination au sein des écoles, collèges et lycées *via* Petra ;
- Nombre de comptes « super-admin » dans l'application CONTACT COVID ; nombre de comptes « administrateurs locaux » dans l'application CONTACT COVID ; nombre de comptes « utilisateurs » dans l'application CONTACT COVID ;

- Algorithme de génération des identifiants contenues dans les URL declare.ameli.fr/SMS ;

L'audition s'est terminée, ce jour, à 17 heures 30 ;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé [redacted]

Signature des agents de la CNIL	Signature de la personne auditionnée
[redacted]	[redacted]

[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.

La personne auditée a été mise en mesure de consulter les pièces copiées.

PIÈCE N°1 : [redacted]

PIÈCE N°2 : [redacted]

PIÈCE N°3 : [redacted]

Signature des agents de la CNIL	Signature des personnes auditionnées
[redacted]	[redacted]

Paraphes [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

REÇU

À l'issue du contrôle, je reconnais avoir reçu une copie du procès-verbal de ce jour n° 2020-091/6, annexe comprise.

À Paris
Le 10/11/2020

Nom, prénom, fonction, signature

[redacted]

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

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

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

Conformément à la décision de la présidente de la CNIL **n°2020-091C** en date du **22 mai 2020**, la mission de contrôle a pour objet de procéder à la vérification de la **conformité du traitement de données à caractère personnel "CONTACT COVID", résultant de l'adaptation du système d'information "amelipro" 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 la Caisse nationale de l'assurance maladie et de tout traitement lié** ou portant sur des données à caractère personnel collectées à partir de ce dernier auprès de tout organisme concerné par leur mise en œuvre aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée et du règlement (UE) 2016/679 susvisés ;

Disons débuter la mission de contrôle le 12 novembre 2020, à 9h15, depuis les locaux de la CNIL, situés 3, Place de Fontenoy à PARIS (75007) ;

Plaçons en annexe n°1 (réf. 2018-001R) et annexe n°2 (réf. 2019-002M) de ce procès-verbal le descriptif de l'environnement technique utilisé (machine virtuelle) ;

Disons nous assurer, par les opérations placées en annexe n°3 (réf. 2020-091/7V) du présent procès-verbal, de l'environnement informatique utilisé ;

Disons débuter les constatations décrites ci-après le 12 novembre 2020, à 10h30, dans le prolongement immédiat des opérations de vérification de l'environnement technique, depuis les locaux de la CNIL, situés 3, Place de Fontenoy à PARIS (75007).

Saisissons dans la barre de navigation du navigateur Mozilla Firefox l'URL « declare.ameli.fr/sms/ » ;

Affichons les en-têtes html de la page précitée ; prenons copie de ces derniers que nous plaçons en pièce n°01 du procès-verbal ;

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/ », est immédiatement affichée dans le navigateur :

Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°02 du présent procès-verbal ;

Disons ouvrir les outils de développement du navigateur en appuyant sur la touche « F12 » et cliquons sur l'onglet « Réseau » ;

Disons cliquer sur la roue crantée en haut à droite des outils de développement et activons l'option « Conserver les journaux » ;

Cliquons sur le bouton « COMMENCER » ;

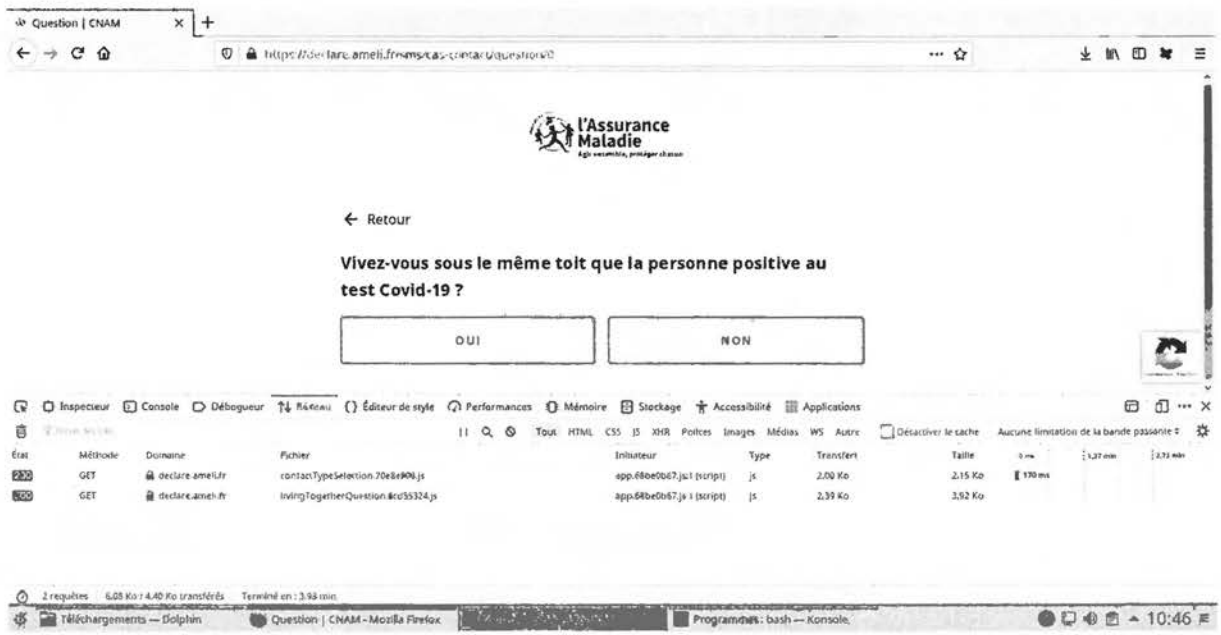
[redacted]

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/selection-type-contact », est immédiatement affichée dans le navigateur :

Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°03 du présent procès-verbal ;

Cliquons sur le bouton « Je suis cas contact » ;

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/cas-contact/question/0 », est immédiatement affichée dans le navigateur :

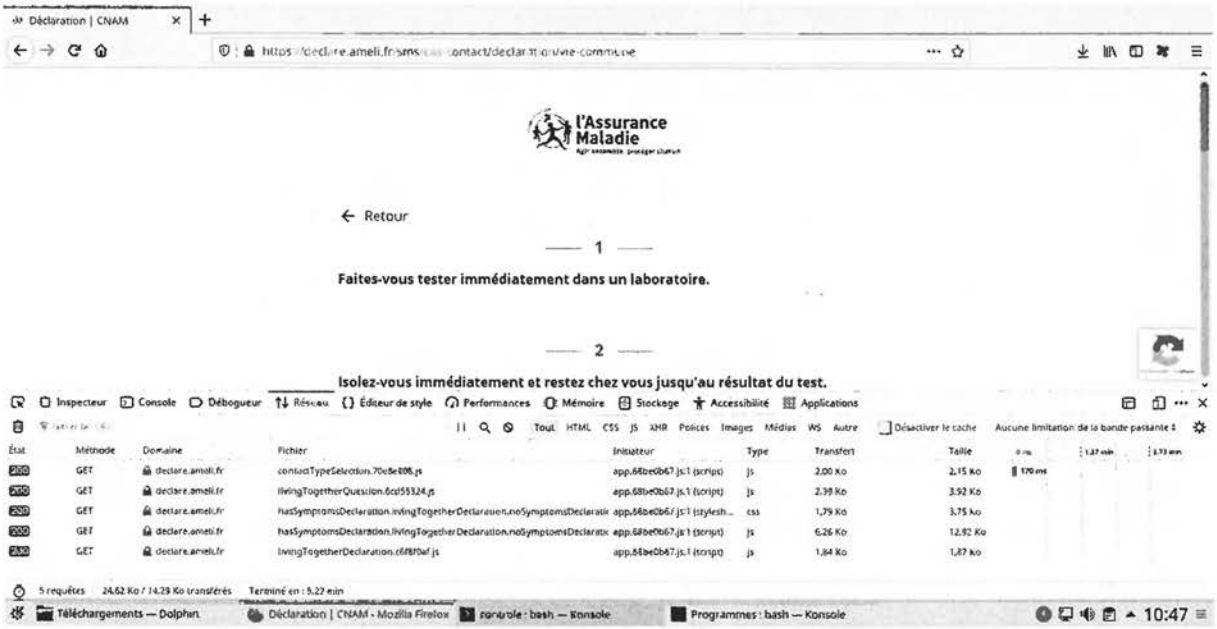


Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°04 du présent procès-verbal ;

Cliquons sur le bouton « OUI » ;

[redacted]

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/cas-contact/declaration/vie-commune », est immédiatement affichée dans le navigateur :

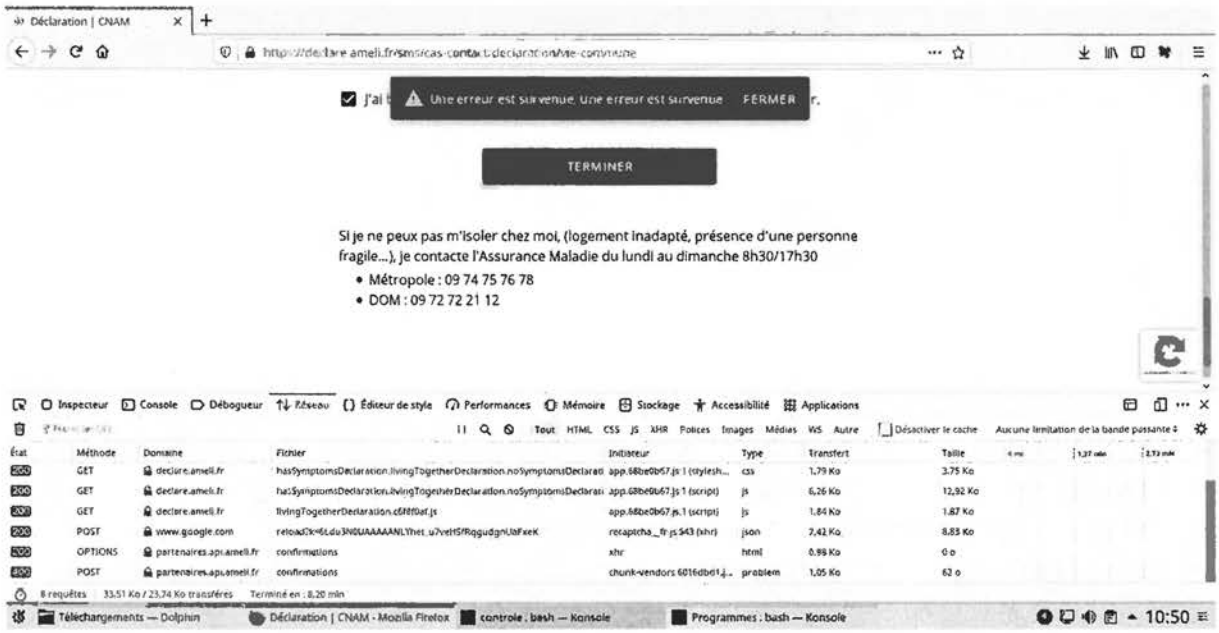


Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°05 du présent procès-verbal ;

Cochons la case « J'ai bien pris connaissance des consignes et je m'engage à les appliquer »

Cliquons sur le bouton « TERMINER » ;

Constatons l'apparition d'une fenêtre surgissante contenant le message d'erreur « Une erreur est survenue, Une erreur est survenue FERMER » :



Cliquons sur la roue crantée en haut à droite des outils de développement, cliquons sur « Tout enregistrer en tant que HAR » et enregistrons le fichier résultant en pièce n°06 ;

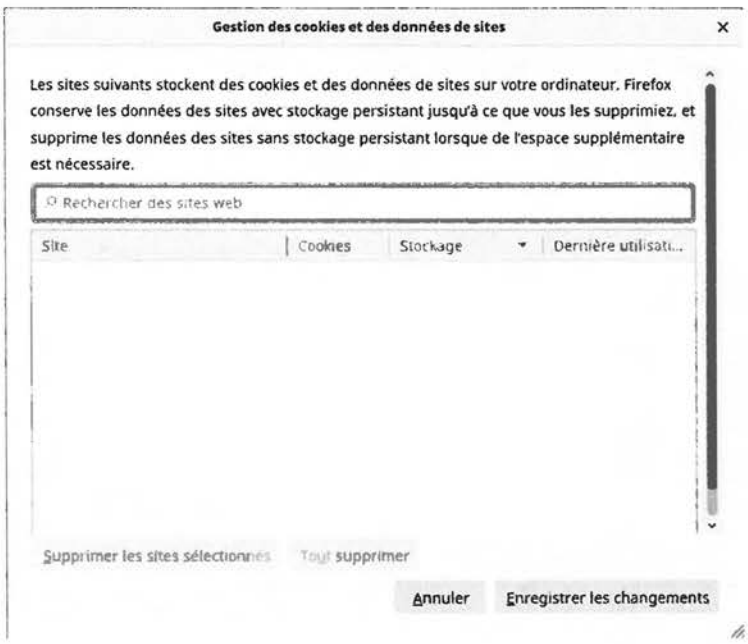
[redacted]

Cliquons sur la corbeille en haut à gauche des outils de développement et constatons que l'historique des requêtes a été vidé ;

Disons effacer les éléments suivants du navigateur :

- Historique de navigation et des téléchargements ;
- cookies ;
- cache ;
- connexions actives ;
- historique des formulaires et des recherches ;
- données de sites web hors connexion ;
- préférences de sites.

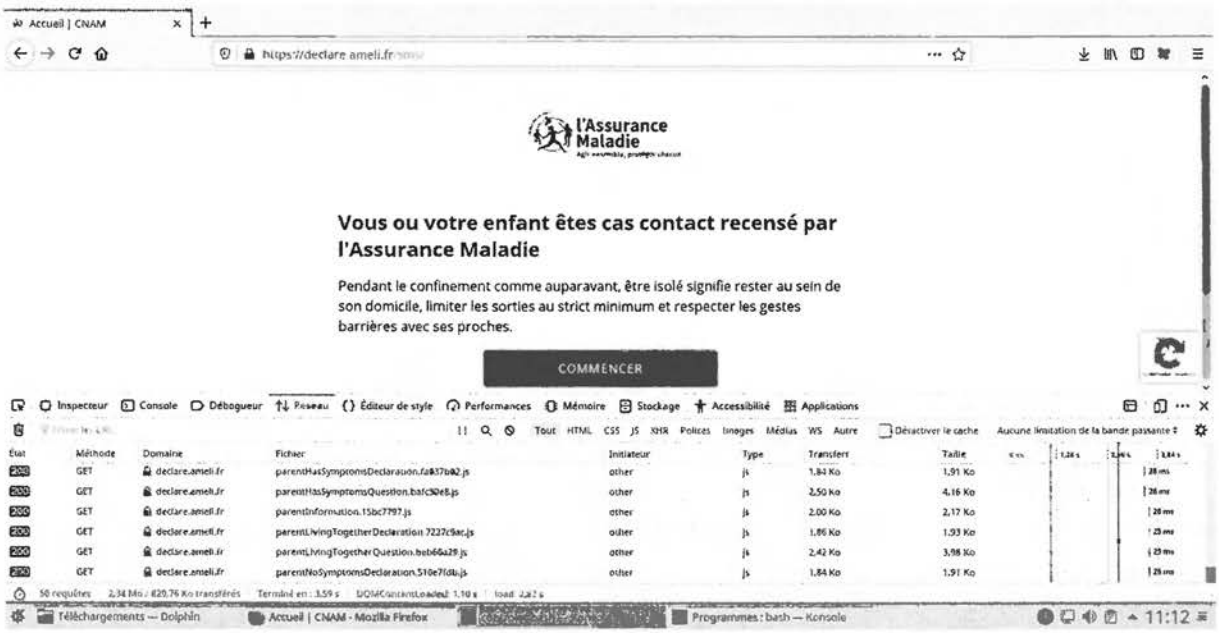
Constatons l'absence de cookies enregistrés dans le navigateur :



Saisissons dans la barre de navigation du navigateur Mozilla Firefox l'URL « declare.ameli.fr/sms/ » ;

[redacted]

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/ », est immédiatement affichée dans le navigateur :



Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°07 du présent procès-verbal ;

Cliquons sur le bouton « COMMENCER » ;

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/selection-type-contact », est immédiatement affichée dans le navigateur :

Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°08 du présent procès-verbal ;

Cliquons sur le bouton « Je suis parent d'un enfant cas contact » ;

[redacted]

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/parent-enfant-cas-contact/informations », est immédiatement affichée dans le navigateur :

Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°09 du présent procès-verbal ;

Cliquons sur le bouton « CONTINUER » ;

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/parent-enfant-cas-contact/question/0 », est immédiatement affichée dans le navigateur :

Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°10 du présent procès-verbal ;

Cliquons sur le bouton « NON » ;

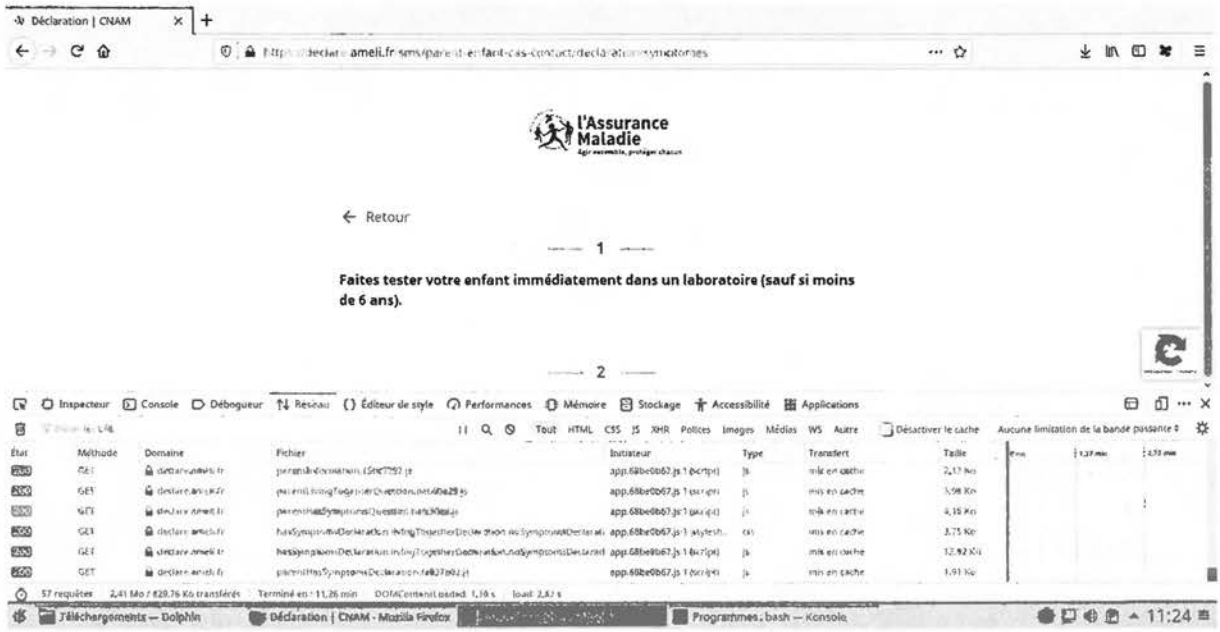
[redacted]

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/parent-enfant-cas-contact/question/1 », est immédiatement affichée dans le navigateur :

Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°11 du présent procès-verbal ;

Cliquons sur le bouton « OUI » ;

Constatons que la page suivante, ayant pour URL « https://declare.ameli.fr/sms/parent-enfant-cas-contact/declaration/symptomes », est immédiatement affichée dans le navigateur :

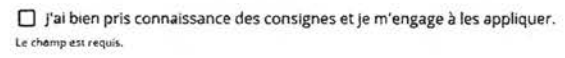


Enregistrons une copie écran de l'intégralité de cette page, référencée en pièce n°12 du présent procès-verbal ;

Cliquons sur le bouton « TERMINER » ;

[redacted]

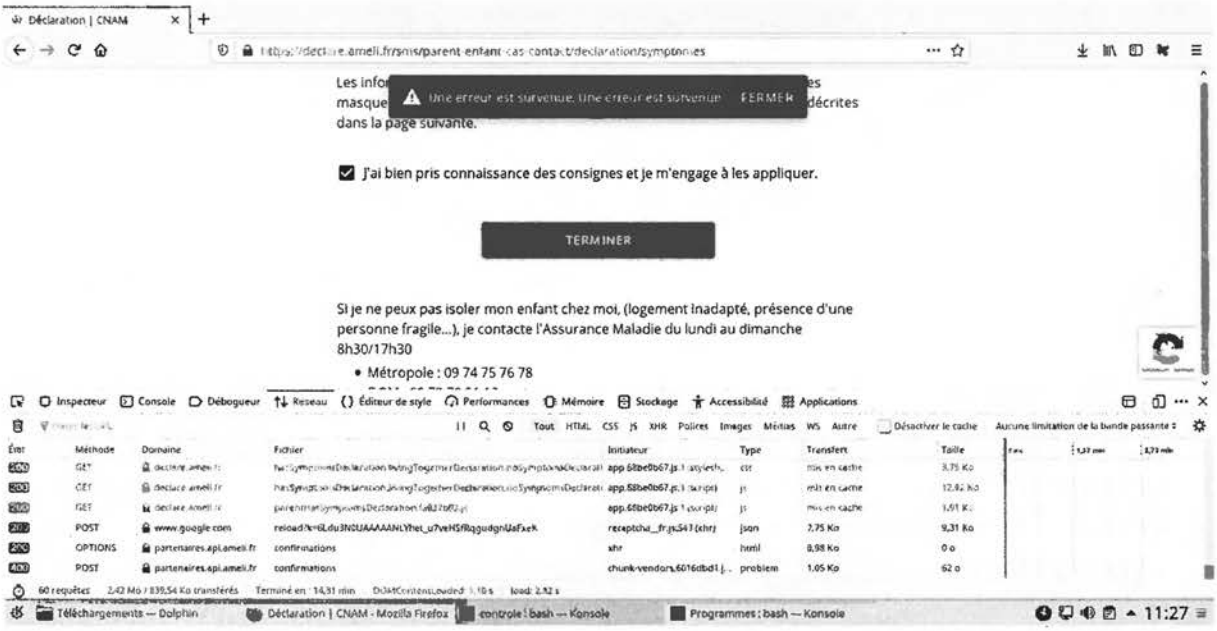
Constatons l'apparition du message d'erreur « Le champ est requis » :



Cochons la case « J'ai bien pris connaissance des consignes et je m'engage à les appliquer »

Cliquons sur le bouton « TERMINER » ;

Constatons l'apparition d'une fenêtre surgissante contenant le message d'erreur « Une erreur est survenue, Une erreur est survenue FERMER » :



Cliquons sur la roue crantée en haut à droite des outils de développement, cliquons sur « Tout enregistrer en tant que HAR » et enregistrons le fichier résultant en pièce n°13 ;

Disons fermer les outils de développement en cliquant sur la croix en haut à droite de ces derniers.

Disons passer le curseur sur le logo situé en bas à droite de la page.

Constatons l'apparition d'une fenêtre surgissante « protection par reCAPTCHA » ;

Disons mettre fin à nos constatations, le 12 novembre 2020 à 11h40 ;

[redacted]

Par ailleurs, demandons au responsable des traitements, dans un délai de 8 jours ouvrés à compter de la notification par courrier lettre recommandée avec avis de réception du présent procès-verbal :

- de communiquer le registre des activités de traitement relatif au site « declare.ameli.fr/sms/ » ;
- d'indiquer qui détermine les finalités et les modalités de mise en œuvre des traitements de données à caractère personnel du site web « declare.ameli.fr/sms/ » ;
- de communiquer un plan détaillé des différentes étapes du parcours utilisateur ;
- d'indiquer à quelle étape de la navigation est utilisé le système « reCAPTCHA » ;

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

La mission de contrôle s'est terminée, ce jour, à 14h30 ;

Signature des agents chargés de la mission de contrôle
[redacted]

[redacted]

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

INVENTAIRE DES PIÈCES DU PROCÈS-VERBAL DE CONSTATATIONS EN LIGNE

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

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

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

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]

PIECE N°10 : [redacted]

PIECE N°11 : [redacted]

PIECE N°12 : [redacted]

PIECE N°13 : [redacted]

Signature des agents chargés de la mission de vérification
[redacted]

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS 3, place de Fontenoy – TSA 80715 75334 PARIS Cedex 07 www.cnil.fr	**ANNEXE N°1 : RECETTE DE L'ENVIRONNEMENT TECHNIQUE**

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 19 et 44 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 dispositions du décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 précitée ;

Nous soussignés, [redacted] agents de la CNIL, dûment habilités dans les conditions prévues à l'article 44 de la loi ;

Procédons à la création d'une machine virtuelle, dite « de référence », le 31 mai 2018 ;

Disons préparer et décrire l'environnement informatique utilisé par les opérations suivantes, débutées ce jour à 11 heures 35 ;

Description de la configuration du poste et du système hôte utilisés :

Paraphes [redacted]

Constatons que la fenêtre « Informations systèmes générales » délivre les informations suivantes :

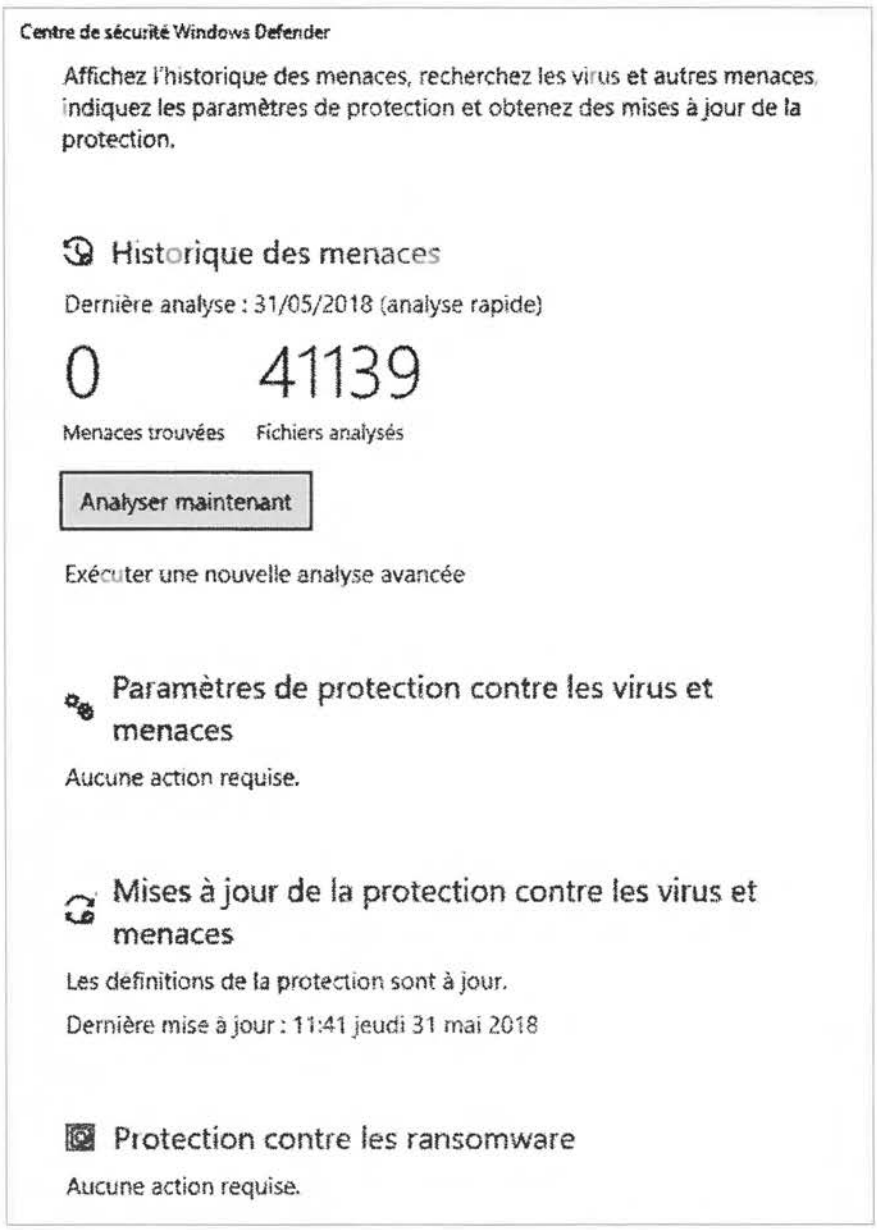
Disons mettre à jour les définitions virales de l'antivirus Microsoft Windows Defender ;

Mentionnons que les caractéristiques du poste informatique utilisé, propriété de la CNIL, sont les suivantes :

[redacted]

[redacted]

Disons effectuer une analyse virale à l'aide de l'antivirus Windows Defender et constatons que le résultat de l'analyse est le suivant :

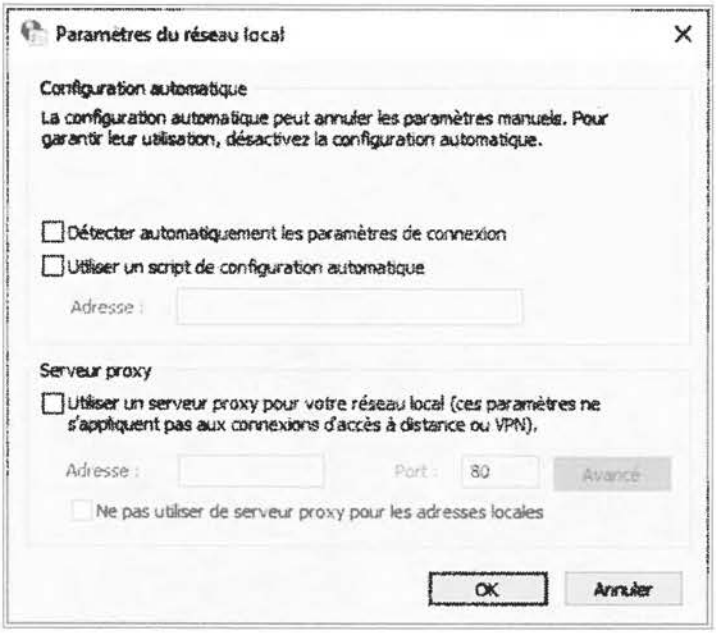


Paraphes

[redacted]

Description de l'architecture du réseau local sous la maîtrise de la Commission :

Mentionnons qu'aucun serveur mandataire (*proxy*) n'est présent dans le réseau local informatique :



Mentionnons que Windows Defender est le seul pare-feu (*firewall*) installé sur le système hôte ;

Mentionnons accéder au réseau Internet au moyen d'une Livebox ADSL dont le modèle est Livebox Pro v3, [redacted]

Mentionnons que [redacted]

[redacted]

Description des éléments relatifs au fournisseur d'accès à Internet :

[redacted]

En ce qui concerne les applicatifs utilisés :

Mentionnons créer un dossier dénommé « PiecesNumeriques » à la racine du disque C:\ ;

Disons utiliser le logiciel ORACLE VM VIRTUALBOX, version 5.2.12 r122591 (Qt5.6.2) ;

Mentionnons que le logiciel est configuré pour se connecter sans utilisation de serveur mandataire (*proxy*) :

Mentionnons avoir téléchargé, à partir du site web https://www.debian.org, l'image ISO d'installation de la distribution GNU/Linux Debian version 9.4.0, dénommée « debian-9.4.0-amd64-DVD-1 », ainsi que le fichier « SHA256SUMS » contenant les empreintes correspondant à cette image ;

Disons calculer l'empreinte numérique du fichier ISO précité à l'aide de l'algorithme SHA256 ; constatons que l'empreinte obtenue est 8ff2f9091204b897b3acad5411a90524dc4ad9e2c4b2d1a70f1c95167061f69a ;

Constatons que cette empreinte est identique à l'empreinte SHA256 contenue dans le fichier « SHA256SUMS » précédemment téléchargé ;

Description des éléments relatifs à la création de la machine virtuelle de référence :

Mentionnons commencer la création de la machine virtuelle de référence à 11 heures 46 ;

Mentionnons créer une nouvelle machine virtuelle de type GNU/Linux version Debian (64 bits) dans le logiciel ORACLE VM VIRTUALBOX, nommée « Contrôle référence » (ci-après, « la machine virtuelle »), puis sélectionner le type de machine virtuelle « Linux », « Debian (64 bits) » ;

Mentionnons allouer 8192 Mio mémoire vive à la machine virtuelle ;

Mentionnons créer un disque dur virtuel de 20 Gio, de type VDI (image disque virtualbox) dont la taille est dynamiquement allouée, puis ajoutons ce disque à la machine virtuelle ;

Mentionnons activer la fonction PAE/NX dans la configuration système de la machine virtuelle « Contrôle référence » ;

Mentionnons configurer la machine virtuelle afin d'utiliser deux processeurs ;

Mentionnons sélectionner l'image ISO précédemment téléchargée afin que celle-ci soit chargée dans le lecteur CD/DVD de la machine virtuelle ;

Mentionnons sélectionner l'« accès par pont » dans la configuration réseau de la carte réseau n°1 de la machine virtuelle ;

Mentionnons créer un dossier partagé, nommé « PiecesNumeriques » entre la machine virtuelle et la machine hôte Windows ;

Mentionnons configurer le montage du dossier « C:\PiecesNumeriques » de la machine hôte en mode automatique au démarrage de la machine virtuelle ;

Mentionnons démarrer la machine virtuelle à 11 heures 52 ;

Mentionnons sélectionner le mode « Graphical Install » dans le menu d'installation ;

Mentionnons choisir la langue « Français » et le pays « France » pour le processus d'installation ;

Mentionnons choisir la disposition de clavier de type « Français » ;

Mentionnons renseigner « controle » en tant que nom de machine ;

Mentionnons renseigner « home » en tant que nom de domaine ;

Mentionnons renseigner [redacted] en tant que mot de passe root ;

[redacted]

Mentionnons sélectionner la méthode de partitionnement « Assisté – Utiliser un disque entier » ;

Mentionnons sélectionner le disque dur de 20 Gio attaché à la machine virtuelle ;

Mentionnons utiliser le schéma de partitionnement « Tout dans une seule partition » ;

Mentionnons valider le partitionnement et le formatage proposés par le système ;

Mentionnons ne pas analyser un autre CD ou DVD relatif au support d'installation ;

Mentionnons utiliser un miroir permettant le téléchargement de paquets d'installation sur le réseau ; choisissons le miroir ftp.fr.debian.org ;

Mentionnons laisser vide le champ relatif au serveur mandataire HTTP (*proxy*) ;

Mentionnons désactiver l'étude statistique sur l'utilisation des paquets Debian (*popularity-contest*) ;

Mentionnons sélectionner les groupes de paquets « environnement de bureau Debian », « KDE » et « utilitaires usuels du système » ; constatons le téléchargement de 1567 fichiers ;

Mentionnons activer l'installation de « GRUB » sur le chargeur de démarrage ;

Constatons le redémarrage de la machine virtuelle à 12 heures 14 ;

Mentionnons nous connecter à la machine virtuelle avec l'identifiant « controle » ;

Mentionnons effectuer les configurations suivantes en mode super-utilisateur depuis la session de l'utilisateur « controle » :

- ajout des dépôts « non-free » et « contrib » dans la liste des dépôts (fichier /etc/apt/source.list),
- suppression du disque Debian dans la liste des dépôts (fichier /etc/apt/source.list),
- suppression des dépôts de type « deb-src »,
- mise à jour de la liste des dépôts[1],

Mentionnons installer ou réinstaller les paquets suivants avec la commande « apt install » :

- ntp et ntpdate
- vim
- wireshark ; lors de l'installation, choisissons d'autoriser les utilisateurs non privilégiés à capturer des paquets réseau ;
- wipe
- rkhunter, clamav et chkrootkit
- gtk2-engines-qtcurve, gtk-theme-switch
- zenity

Mentionnons installer les « linux-headers [2]» ;

Mentionnons installer les « additions invité » de Virtualbox dans la machine virtuelle à partir de l'image intégrée au logiciel ORACLE VM VIRTUALBOX[3] ;

Mentionnons redémarrer la machine virtuelle ;

Mentionnons effectuer les configurations suivantes en mode super-utilisateur depuis la session de l'utilisateur « controle » :

Mentionnons effectuer les mises à jour de sécurité[4] ;

Mentionnons supprimer les anciens paquets téléchargés[5] ;

Mentionnons effectuer les configurations suivantes :

- désactivation des services « ntp »[6] ;
- désactivation du service « clamav-freshclam[7] » ;
- activation de la complétion de la ligne de commande[8] ;
- ajout de l'utilisateur « controle » aux groupes sudo, wireshark, vboxsf[9] ;
- ajout d'un raccourci « Wireshark » sur le bureau et dans les favoris ;

1 À l'aide de la commande « apt update »
2 À l'aide de la commande « apt install make linux-headers-amd64 »
3 Exécutons « sh VBoxLinuxAdditions.run » dans le répertoire /media/cdrom0
4 À l'aide de la commande « apt dist-upgrade »
5 À l'aide de la commande « apt clean »
6 À l'aide des commandes « systemctl disable ntp »
7 À l'aide de la commande « systemctl disable clamav-freshclam »
8 « Enable bash completion in interactive shell » dans le fichier /etc/bash.bashrc
9 A l'aide des commandes « gpasswd -a controle sudo », « gpasswd -a controle wireshark » et « gpasswd –a controle vboxsf »

- ajout d'un raccourci Mozilla Firefox sur le bureau et dans les favoris ;
- ajout dans le fichier /etc/fstab[10] d'une entrée relative au montage du dossier partagé « PiecesNumeriques » et création sur le bureau d'un dossier dénommé« PartagePiecesNumeriques » ;
- ajout d'un raccourci vers l'outil « Spectacle » ;

Mentionnons redémarrer la machine virtuelle ;

Mentionnons effectuer les configurations suivantes en mode super-utilisateur depuis la session de l'utilisateur « controle » :

- installation de l'outil « CyCLENum » permettant le calcul d'empreintes numériques et création d'un raccourci « CyCLENum » sur le bureau ;
- ajout sur le bureau d'un raccourci « Konsole » ;
- ajout sur le bureau d'un raccourci « Konsole administrateur »[11] ;
- ajout des applications précitées dans le menu « Favoris » ;

Mentionnons effectuer les configurations suivantes sur le navigateur Mozilla Firefox :

- ajout de la barre de menus sur l'écran général ;
- affichage d'une page vide au démarrage du navigateur ;
- suppression des moteurs de recherche de la barre de moteurs à l'exception de « Wikipédia ») ;
- désactivation de l'option « Afficher les suggestions de recherche » ;
- suppression dans l'écran général de la barre de moteurs de recherche et de l'icône « Pocket » ;
- dans le menu « about:config », renseignement du champ « keyword.enabled » à « false » ;
- dans le menu « about:config », renseignement du champ « extensions.pocket.enabled » à « false » ;
- téléchargement et installation de l'extension, dénommée « Cookies List », à partir de l'URL https://github.com/LINCnil/CNIL-Cookies-List/tree/master/release ;
- désactivons la mise à jour automatique du module précité ;
- l'option « Conserver l'historique » est sélectionnée ;
- les options « Utiliser la protection contre le pistage dans les fenêtres de navigation privée » et « Ne pas me pister » ne sont pas sélectionnées ;
- l'option « Blocage des fenêtres popup » est désactivée ;
- les options « Bloquer les contenus dangereux ou trompeurs » sont désactivées ;
- l'option « Autoriser Firefox à envoyer pour vous les rapports de plantage en attente » est désactivée ;
- la configuration du serveur proxy pour accéder à Internet est : « Pas de proxy » ;
- l'option « Mettre à jour automatiquement les moteurs de recherche » est désactivée ;

Mentionnons vider tout l'historique de navigation (navigation, téléchargements, formulaires, recherches), les cookies, le cache, les connexions actives, les données de site web hors connexion et les préférences de site présents dans le navigateur ;

Mentionnons effectuer une analyse anti-malware et anti-rootkit avec les outils « Rkhunter » (commande « rkhunter -c » exécutée avec les droits administrateur) et « Chkrootkit » (commande « chkrootkit » exécutée avec les droits administrateur) ;

10Ajout de la ligne « PiecesNumeriques /home/controle/Bureau/PartagePiecesNumeriques vboxsf defaults,_netdev 0 0 »

11A l'aide de la commande : kdesudo /usr/bin/konsole

[redacted]

Mentionnons mettre à jour les définitions de virus de Clamav (commande « freshclam ») ; exécutons la commande « touch /etc/clamav/clamd.conf » ; puis exécutons une analyse virale (commande « clamscan -r ») ;

Mentionnons que le résultat obtenu n'appelle pas de commentaire au regard de la sécurité de l'environnement virtuel ;

Mentionnons arrêter la machine virtuelle ;

Mentionnons exporter la machine virtuelle, nommée « Contrôle référence » ;

Mentionnons obtenir un fichier que nous nommons « Contrôle référence v0.6-1.ova » et dont l'empreinte SHA256 est ccdec75b761392f8b100d11d27c472ef404aa612f540213e547c600235d488bc ;

Terminons nos opérations de recette de l'environnement technique, ce jour, à 18 heures 19 ;

Signature des agents en charge de l'installation de l'environnement technique de référence
[redacted]

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

ANNEXE N° 3 :

VÉRIFICATIONS PRÉALABLES AU CONTRÔLE SUR L'ENVIRONNEMENT TECHNIQUE

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

Nous soussignés, [redacted] juriste au service des contrôles, [redacted] auditeur des systèmes d'information au service des contrôles, agents de la CNIL, dûment habilités dans les conditions prévues à l'article 19 de la loi précitée ;

Conformément à la décision de la présidente de la CNIL **n°2020-091C** en date du **22 mai 2020**, la mission de contrôle a pour objet de procéder à la vérification de la conformité de tout traitement accessible à partir du domaine **conformité du traitement de données à caractère personnel "CONTACT COVID", résultant de l'adaptation du système d'information "amelipro" 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 la Caisse nationale de l'assurance maladie et de tout traitement lié**, aux disposition du règlement (UE) 2016/679 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 ;

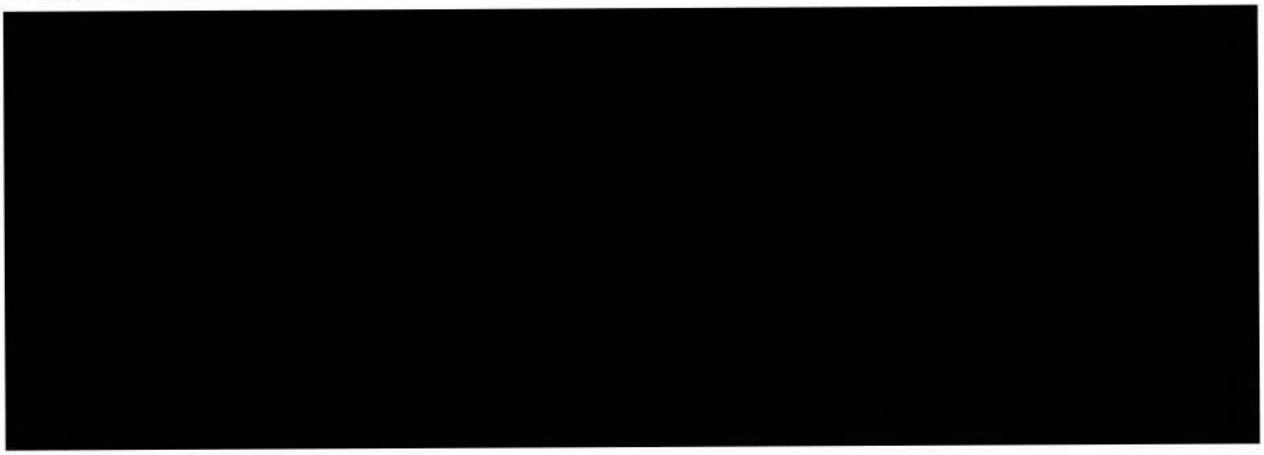
Disons nous assurer des caractéristiques de l'environnement informatique utilisé par les opérations suivantes, débutées ce jour, le 12 novembre 2020, à 09h15 ;

Description de la configuration du poste utilisé pour les constatations :

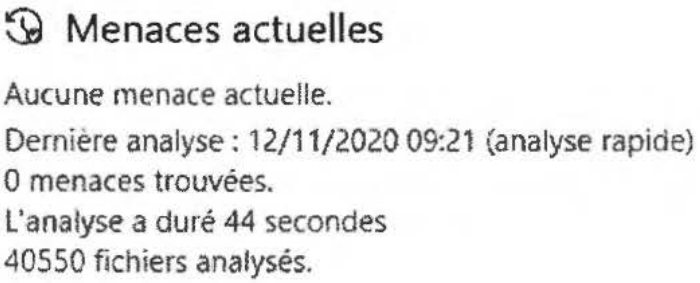
Constatons que la fenêtre « Informations système générales » délivre les informations suivantes :

Disons mettre à jour les définitions virales de l'antivirus Microsoft Windows Defender ;

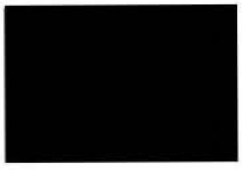
Mentionnons que les caractéristiques du poste informatique utilisé, propriété de la CNIL, sont les suivantes :



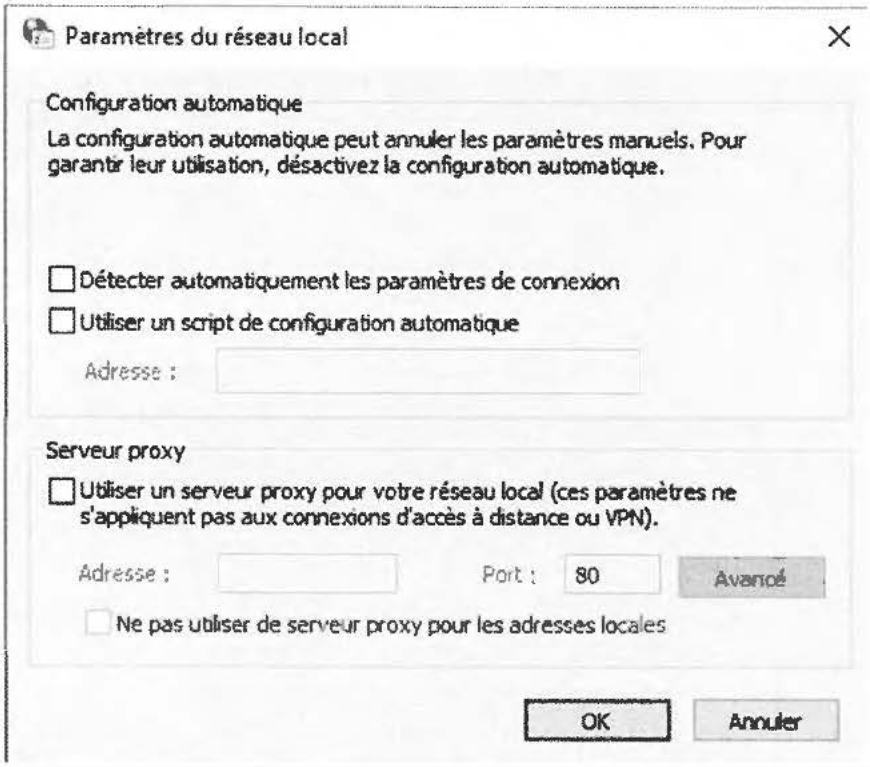
Disons effectuer une analyse virale à l'aide de l'antivirus Windows Defender et constatons que le résultat de l'analyse est le suivant :



Description de l'architecture du réseau local sous la maîtrise de la Commission :



Mentionnons qu'aucun serveur mandataire (*proxy*) n'est présent dans le réseau local informatique :



[redacted]

Description des éléments relatifs au fournisseur d'accès à Internet :

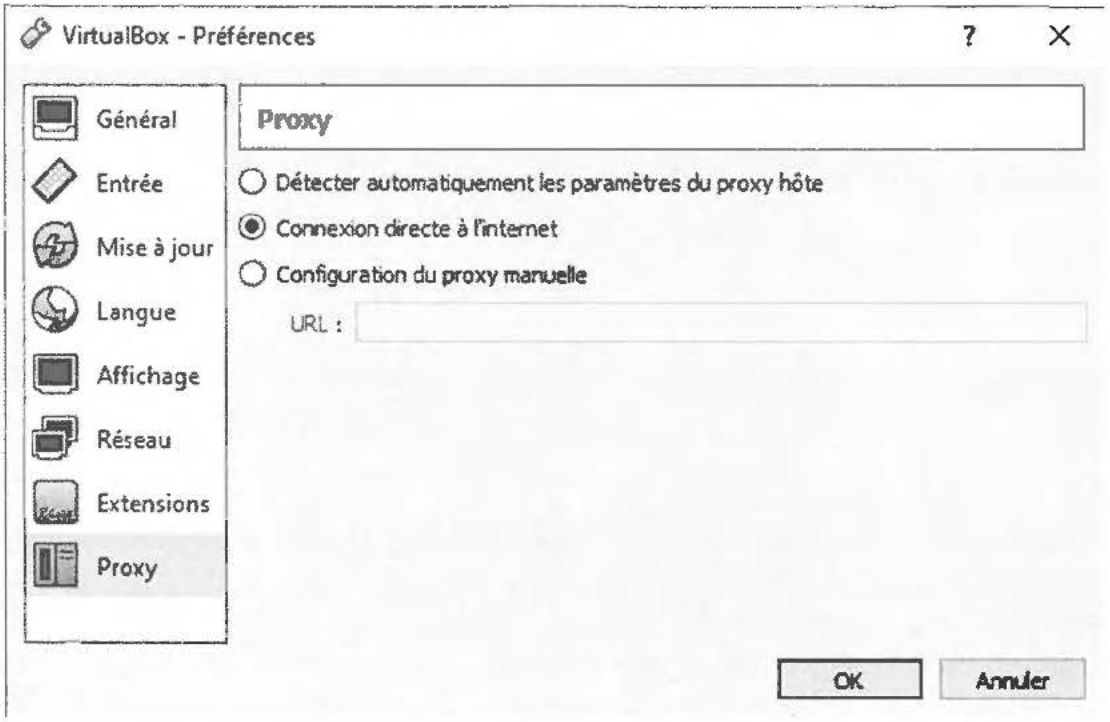
[redacted]

En ce qui concerne les applicatifs utilisés :

Disons utiliser le logiciel ORACLE VIRTUALBOX, version 6.1.12;

Mentionnons que le logiciel est configuré pour se connecter sans utilisation de serveur mandataire (*proxy*) :

[redacted]



Disons utiliser la machine virtuelle « Contrôle Référence », version 0.6-3, dont l'empreinte, calculée avec l'algorithme SHA256 est 0e872fdb6d73663a54b1fb892c9092e56b3cee562f5498a10c0e9c1698e09fa6 et dont les caractéristiques sont placées en annexes n° 1 et n°2 du procès-verbal n° 2020-091/7 sous les références 2018-001R et 2019-002M ;

Importons la machine virtuelle dans le logiciel VIRTUALBOX en choisissant l'option « Politique d'adresse MAC : générer de nouvelles adresses MAC pour toutes les interfaces réseau » et en décochant l'option « Importer les disques durs comme VDI » ;

Mentionnons que la machine virtuelle est configurée pour utiliser une connexion par pont ;

Démarrons la machine virtuelle à 9h30 ;

Précisons exécuter les commandes suivantes en tant que super-utilisateur (root) ;

Mentionnons ouvrir un terminal et exécuter la commande « ntpdate ntp.obspm.fr » afin de nous synchroniser au serveur de temps ntp.obspm.fr (protocole NTP) ;

Mentionnons nous assurer que le système est à jour (commande « apt update » suivie de la commande « apt dist-upgrade -y ») ;

Mentionnons exécuter la commande « lsb_release -a » afin d'afficher la version du système installée :

```
No LSB modules are available.

Distributor ID: Debian

Description:    Debian GNU/Linux 9.13 (stretch)
```


[redacted]

Release: 9.13 Codename: stretch

Mentionnons exécuter les commandes « chkrootkit » et « rkhunter -c » (analyse anti-rootkits) ;

Mentionnons exécuter la commande « freshclam » (mise à jour antivirus) ;

Mentionnons exécuter la commande « clamscan -r » (analyse antivirus) ;

Mentionnons exécuter la commande « ifconfig enp0s3 » afin d'afficher les propriétés de la connexion réseau :

[redacted]

Mentionnons exécuter la commande « cat /etc/resolv.conf » ;

Constatons que le résultat affiché dans le terminal est le suivant :

Generated by NetworkManager search home nameserver [redacted]

Mentionnons exécuter la commande « cat /etc/hosts » permettant d'afficher le contenu du fichier « hosts » contenant les correspondances adresse IP / noms de domaine ;

[redacted]

Constatons que la corbeille est vide ;

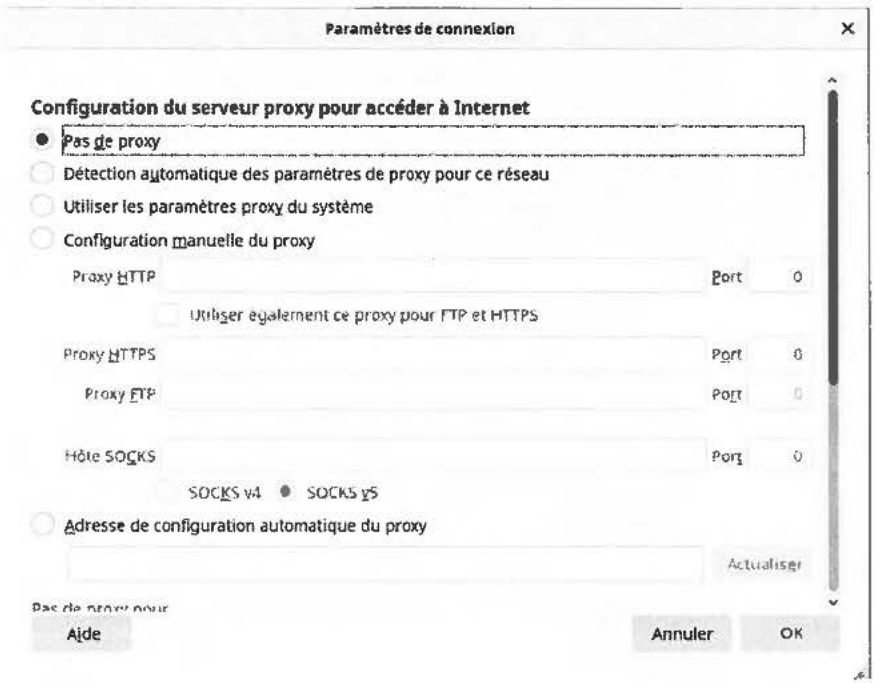
Mentionnons télécharger le programme Mozilla Firefox version 82.0.3 à partir du site internet www.mozilla.org et installer celui-ci dans le répertoire /home/controle/Programmes/ (commande « tar xjf firefox-82.0.3.tar.bz2 ») ;

Précisons utiliser la version 82.0.3 de Firefox :

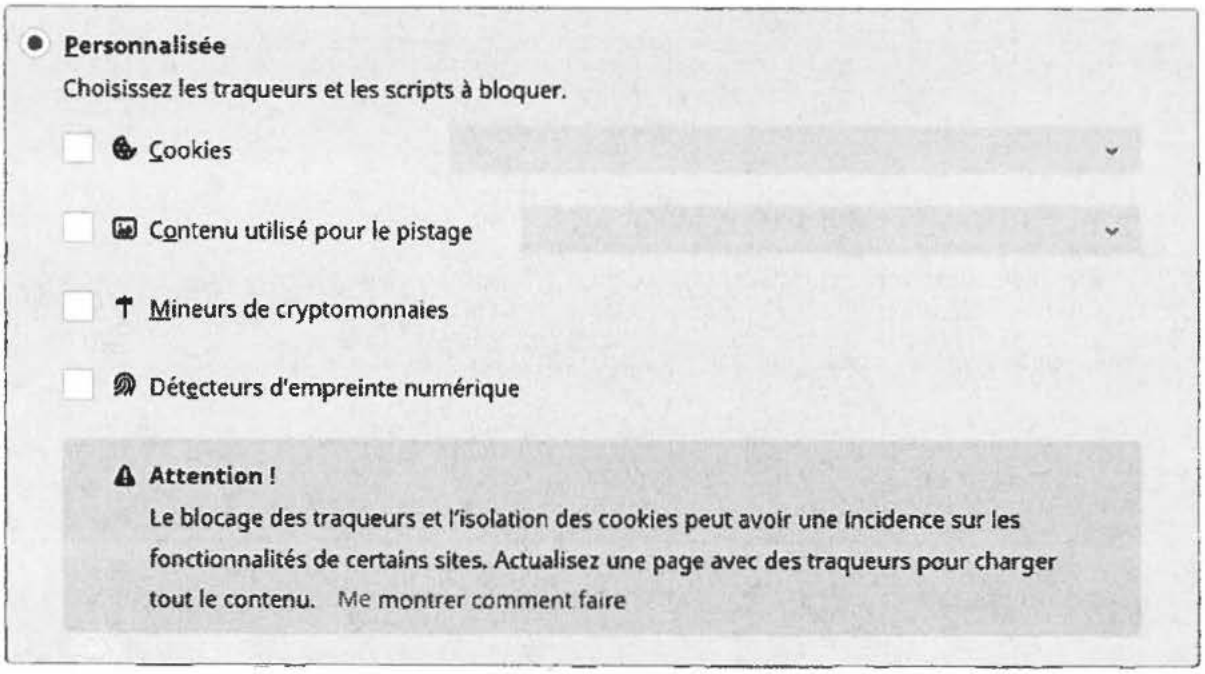
Mentionnons que le programme « CNIL-Cookies-List » est la seule extension installée dans le navigateur ;

Précisons que le navigateur est configuré afin de démarrer sur une page vide ;

Précisons que le navigateur est configuré afin de se connecter sans utilisation de serveur mandataire (*proxy*) ; que le navigateur s'ouvre systématiquement sur une page vide ; que le navigateur est configuré afin de ne pas bloquer les cookies et les traqueurs :



[redacted]



Précisons qu'aucun moteur de recherche n'est installé dans le navigateur à l'exception de « Wikipédia » ;

Accédons au site Internet http://www.mon-ip.com et constatons que l'adresse IP publique avec laquelle nous nous présentons est la suivante : [redacted]

[redacted]

Exécutons la commande « ping -c5 declare.ameli.fr » dont le résultat est le suivant :

[redacted]

Constatons que l'adresse IP renvoyée par la commande ping es[redacted]

Exécutons la commande « nslookup declare.ameli.fr » dont le résultat est le suivant :

[redacted]

[redacted]

[redacted]

Exécutons la commande « whois ameli.fr » dont le résultat est le suivant :

```
%%
%% This is the AFNIC Whois server.
%%
%% complete date format : YYYY-MM-DDThh:mm:ssZ
%% short date format    : DD/MM
%% version              : FRNIC-2.5
%%
%% Rights restricted by copyright.
%% See https://www.afnic.fr/en/products-and-services/services/whois/whois-special-notice/
%%
%% Use '-h' option to obtain more information about this service.
%%
%% [92.169.103.209 REQUEST] >> -V Md5.2 ameli.fr
%%
%% RL Net [##########] - RL IP [#########.]
%%

domain:     ameli.fr
status:     ACTIVE
hold:       NO
holder-c:   CNDL496-FRNIC
admin-c:    AN9464-FRNIC
tech-c:     IDN552-FRNIC
zone-c:     NFC1-FRNIC
nsl-id:     NSL19570-FRNIC
registrar:  CSC CORPORATE DOMAINS INC.
Expiry Date: 2021-07-05T07:26:05Z
created:    2002-08-21T22:00:00Z
last-update: 2020-07-01T05:10:56Z
source:     FRNIC

ns-list:    NSL19570-FRNIC
nserver:    dns1.cscdns.net
nserver:    dns2.cscdns.net
source:     FRNIC

registrar:  CSC CORPORATE DOMAINS INC.
type:       Isp Option 1
address:    251 Little Falls Drive
address:    DE 19808 WILMINGTON
country:    US
phone:      +1 302 636 5400
fax-no:     +1 302 636 5454
```


[redacted]

e-mail: tldsupport@cscglobal.com
website: https://www.cscdigitalbrand.services
anonymous: NO
registered: 2006-10-17T12:00:00Z
source: FRNIC

nic-hdl: CNDL496-FRNIC
type: ORGANIZATION
contact: caisse nationale de l'assurance maladie des travailleurs salaries
address: 26-50, avenue du Professeur Andre Lemierre
address: 75986 Paris
country: FR
phone: +33 1 72 60 10 00
e-mail: domaines.ameli@cnamts.fr
registrar: CSC CORPORATE DOMAINS INC.
changed: 2018-12-18T12:12:40Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: ok
eligsource: REGISTRY
eligdate: 2018-12-18T12:12:40Z
reachmedia: email
reachstatus: ok
reachsource: REGISTRY
reachdate: 2018-12-18T12:12:40Z
source: FRNIC

nic-hdl: AN9464-FRNIC
type: PERSON
contact: Administrateur Ndd
address: 5-7, rue Georges Berger
address: 75017 Paris
country: FR
phone: +33 1 40 06 92 00
fax-no: +33 1 40 06 92 01
e-mail: juaye@france-lex.com
registrar: CSC CORPORATE DOMAINS INC.
changed: 2018-12-18T12:12:35Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: not identified
reachstatus: not identified
source: FRNIC

nic-hdl: IDN552-FRNIC
type: ORGANIZATION
contact: Indom.com Domain Names
address: 124-126, rue de Provence
address: 75008 Paris
country: FR
phone: +33 1 76 70 05 67
fax-no: +33 1 48 01 67 73
e-mail: indom@indom.com

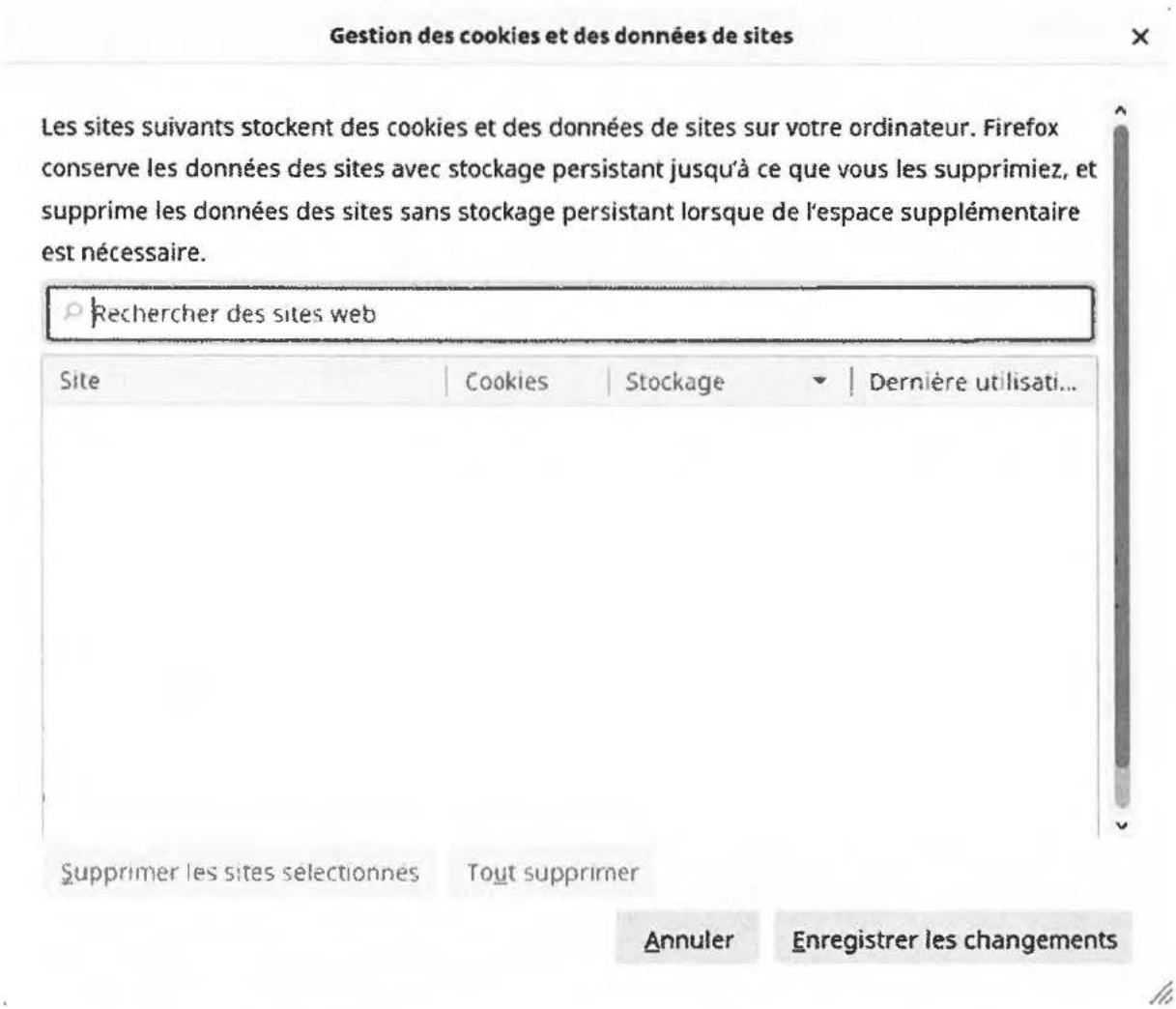
[redacted]

registrar: CSC CORPORATE DOMAINS INC.
changed: 2018-12-18T10:43:53Z nic@nic.fr
anonymous: NO
obsoleted: NO
eligstatus: not identified
reachstatus: not identified
source: FRNIC

Effaçons les éléments suivants du navigateur :

- Historique de navigation et des téléchargements ;
- cookies ;
- cache ;
- connexions actives ;
- historique des formulaires et des recherches ;
- données de sites web hors connexion ;
- préférences de sites.

Constatons l'absence de cookies enregistrés dans le navigateur :



Terminons nos opérations de contrôle de l'environnement technique, préalable aux constatations en ligne, le 12 novembre 2020, à 10h18.

[redacted]

Signature des agents chargés de la mission de contrôle
[redacted]

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS 3, place de Fontenoy – TSA 80715 75334 PARIS Cedex 07 www.cnil.fr	**ANNEXE N°2 :** **MISE A JOUR DE L'ENVIRONNEMENT TECHNIQUE**

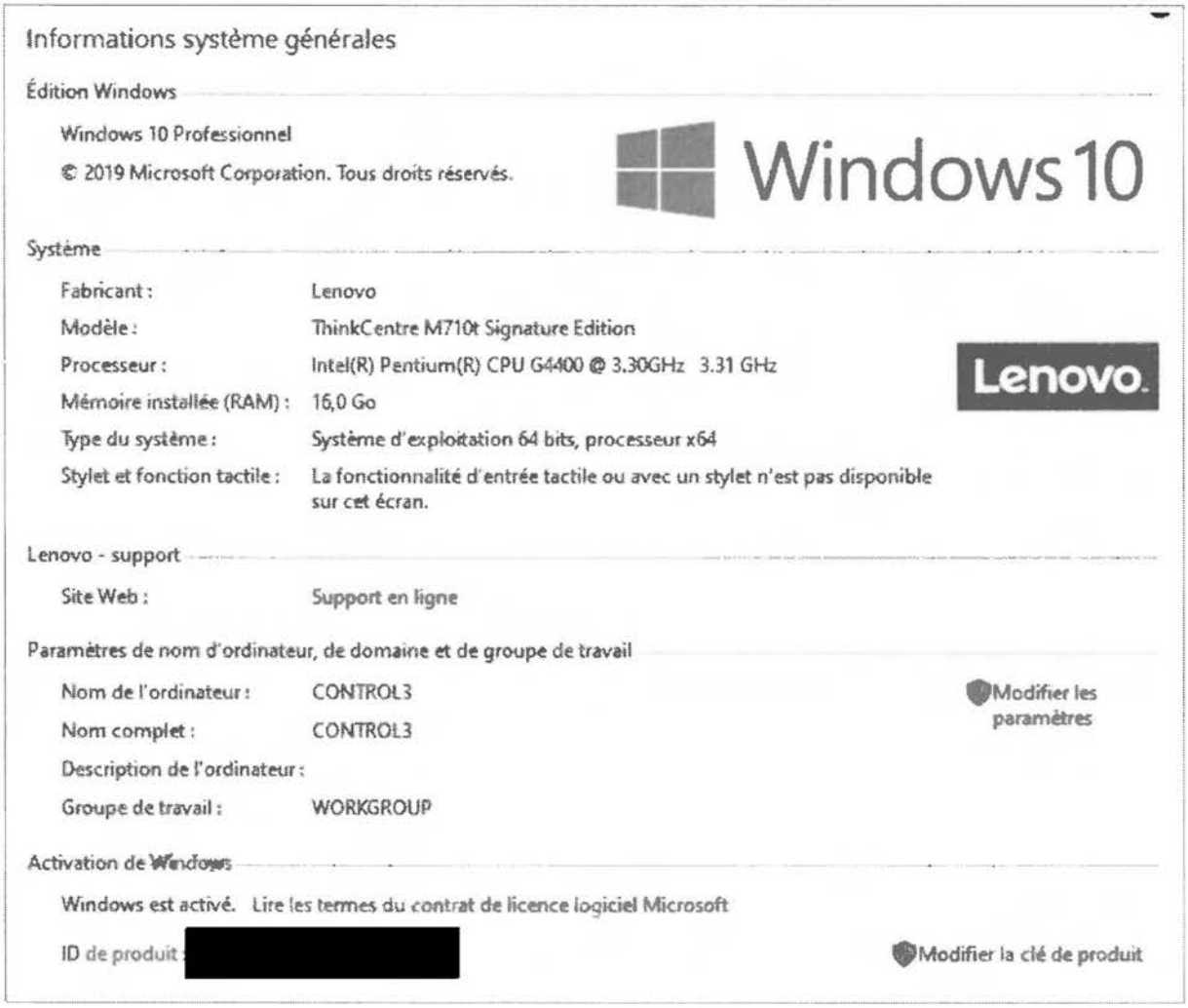
En application des dispositions prévues par les articles 55 à 62 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, les articles 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 ;

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

Procédons à la mise à jour de la machine virtuelle, dite « de référence », par les opérations suivantes, débutées le 14 juin 2019, à 10h10 ;

Description de la configuration du poste utilisé :

Constatons que la fenêtre « Informations systèmes générales » délivre l'information suivante :



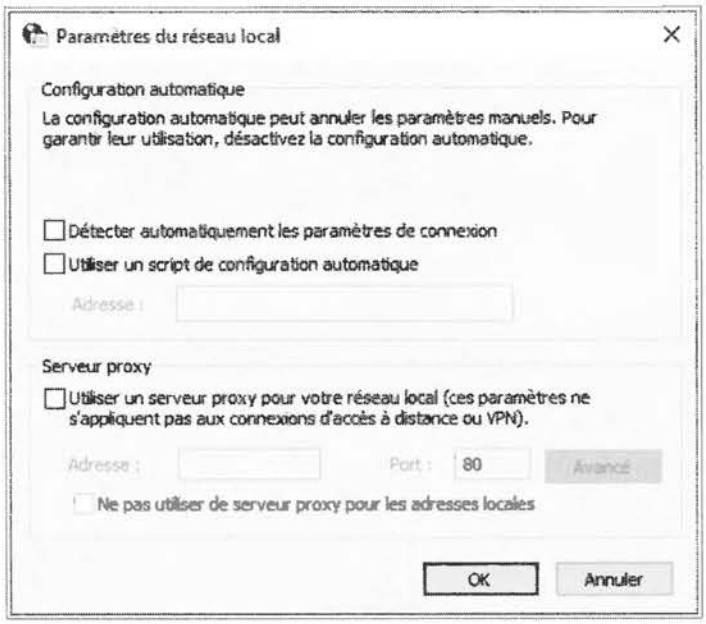
Disons mettre à jour les définitions virales de l'antivirus Microsoft Windows Defender ;

Mentionnons que les caractéristiques du poste informatique utilisé, propriété de la CNIL, sont les suivantes :

Disons effectuer une analyse virale à l'aide de l'antivirus Windows Defender et constatons que le résultat de l'analyse est le suivant :

Description de l'architecture du réseau local sous la maîtrise de la Commission :

Mentionnons qu'aucun serveur mandataire (*proxy*) n'est présent dans le réseau local informatique :



[redacted]

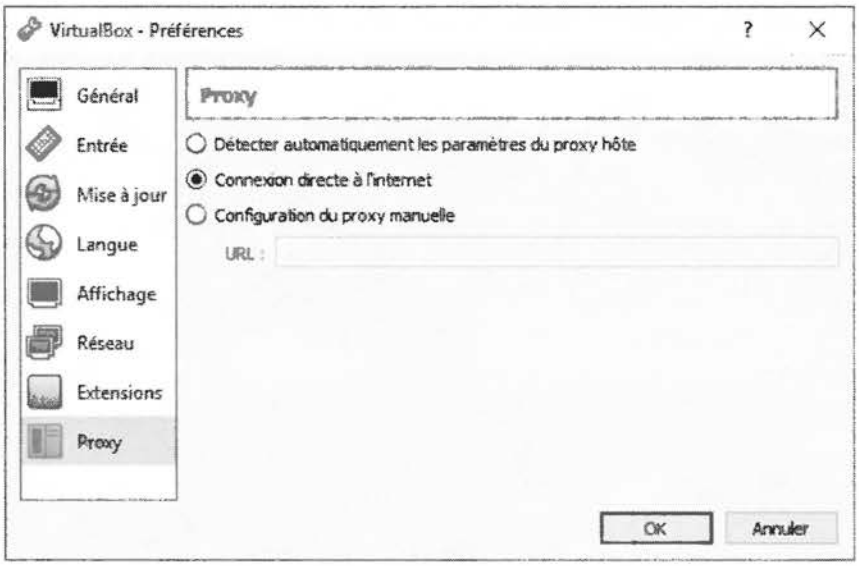
Description des éléments relatifs au fournisseur d'accès à Internet :

[redacted]

En ce qui concerne les applicatifs utilisés :

Disons utiliser le logiciel ORACLE VIRTUALBOX version 6.0.8 r130520 (Qt5.6.2) ;

Mentionnons que le logiciel est configuré pour se connecter sans utilisation de serveur mandataire (*proxy*) :



Disons utiliser la machine virtuelle « Contrôle Référence », version 0.6-1, dont l'empreinte, calculée avec l'algorithme SHA256 est *ccdec75b761392f8b100d11d27c472ef404aa612f540213e547c600235d488bc* et dont les caractéristiques sont placées dans l'annexe n° 1 sous la référence 2018-001R ;

Importons la machine virtuelle dans le logiciel VIRTUALBOX en sélectionnant l'option « Politique d'adresse MAC : Générer de nouvelles adresses MAC pour toutes les interfaces réseau » et en décochant l'option « Importer les disques durs comme VDI » ;

Mentionnons que la machine virtuelle est configurée pour utiliser une connexion par pont ;

Démarrons la machine virtuelle à 10 heures 29 ;

Mentionnons ouvrir l'application Apper et configurer l'option « vérifier s'il existe de nouvelles mises à jour : » à « jamais » dans les paramètres généraux ;

Précisons exécuter les commandes suivantes en tant que super-utilisateur (root) ;

Mentionnons ouvrir un terminal et exécuter la commande « ntpdate ntp.inria.fr » afin de nous synchroniser au serveur de temps ntp.inria.fr (protocole NTP) ;

Mentionnons désinstaller les paquets unattended-upgrades et firefox-esr (commande « apt autoremove ») ;

Mentionnons nous assurer que le système est à jour (commande « apt update » suivie de la commande « apt dist-upgrade -y») ;

Mentionnons installer les paquets suivants (commande « apt install ») : aptitude, dnsutils, whois, multitail, firmware-linux, firmware-realtek, firmware-linux-nonfree, firmware-linux-free, firmware-misc-nonfree, firmware-ralink, firmware-atheros, firmware-iwlwifi, hostapd, dnsmasq, wireless-tools, iw, wvdial, rfkill ;

Mentionnons supprimer le raccourci « Firefox-esr » du bureau ;

Mentionnons télécharger le programme Mozilla Firefox version 67.0.2 à partir du site internet www.mozilla.org et installer celui-ci dans le répertoire /home/controle/Programmes/ (commande « tar xjf firefox-67.0.2.tar.bz2 »).

Mentionnons ajouter un raccourci Firefox sur le bureau ;

Mentionnons démarrer Firefox et choisir l'option « Faire de Firefox mon navigateur par défaut » ;

Constatons que le navigateur Firefox est à jour :

Précisons que le navigateur est configuré afin de démarrer sur une page vide (page d'accueil, nouvelles fenêtres, nouveaux onglets) ;

Précisons que le navigateur est configuré afin de se connecter sans utilisation de serveur mandataire (*proxy*) ; que le navigateur s'ouvre systématiquement sur une page vide ; que le navigateur est configuré afin d'accepter les cookies et traqueurs ;

Mentionnons choisir « Wikipédia » en tant que moteur de recherche par défaut et supprimer les autres moteurs de recherche disponibles ;

Précisons décocher l'option « Afficher les suggestions de recherche » ;

Précisons décocher l'option « Bloquer les fenêtres popup » ;

Mentionnons installer l'extension Cookies List téléchargée à partir de l'URL https://github.com/LINCnil/CNIL-Cookies-List ;

Mentionnons vider tout l'historique de navigation (navigation, téléchargements, formulaires, recherches), les cookies, le cache, les connexions actives, les données de site web hors connexion et les préférences de site présents dans le navigateur ;

Mentionnons exécuter les commandes « chkrootkit » et « rkhunter -c » (analyse anti-rootkits) ; Mentionnons que les résultats observés n'appellent pas de commentaire au regard de la sécurité de l'environnement virtuel ;

Mentionnons exécuter la commande « freshclam » (mise à jour antivirus) ;

Mentionnons exécuter la commande « clamscan -r » (analyse antivirus) ; Mentionnons que les résultats observés n'appellent pas de commentaire au regard de la sécurité de l'environnement virtuel ;

Mentionnons exécuter la commande « ifconfig enp0s3 » afin d'afficher les propriétés de la connexion réseau :

[redacted]

Mentionnons exécuter la commande « cat /etc/resolv.conf » ;

Constatons que le résultat affiché dans le terminal est le suivant :

[redacted]

Mentionnons exécuter la commande « cat /etc/hosts » permettant d'afficher le contenu du fichier « hosts » contenant les correspondances adresse IP / noms de domaine ;

[redacted]

Constatons que la corbeille est vide ;

Arrêtons la machine virtuelle ;

Exportons la machine virtuelle, nommée « Contrôle référence v0.6-3 » ;

Mentionnons obtenir un fichier « Contrôle référence v0.6-3.ova » dont l'empreinte SHA256 est *0e872fdb6d73663a54b1fb892c9092e56b3cee562f5498a10c0e9c1698e09fa6* ;

[redacted]

Terminons nos opérations de mise à jour de l'environnement technique, ce jour, à 11 heures 30 ;

Signature des agents en charge de l'installation de l'environnement technique de référence
[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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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 ;

[redacted] dûment habilités à procéder à des missions de vérification sur place ;

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

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le mardi 17 novembre 2020, à 9 heures 30, dans les locaux de Caisse primaire d'assurance maladie de la Côte d'Or, situés au 1D Boulevard de Champagne à DIJON (21000) 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] ont été préalablement informés du contrôle par courriel en date du 13 novembre 2020 ;

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert près la cour d'Appel de Dijon.

[redacted] *nous informent des éléments suivants :*

En ce qui la CPAM de la Côte d'Or

La CPAM de la Côte d'Or a été créée en 1946. Elle comprend 423 salariés.

Son budget de fonctionnement pour l'année 2019 est de 23 millions d'euros.

La CPAM de la Côte d'Or dispose de plusieurs activités :

- le remboursement des frais de santé auprès notamment des assurés et des établissements de santé ;
- l'indemnisation des arrêts de travail et arrêts de congés maternité ;
- l'accompagnement des assurés.

Pour la mission de « *contact traçing* », 110 personnes de la CPAM de la Côte d'Or sont mobilisées dont 25 personnes en CDD.

Une plateforme d'appui au « contact tracing » par la MSA (mutualité sociale agricole) Bourgogne-Franche-Comté a été créée au mois de novembre 2020 comprenant 15 CDD.

La CPAM de la Côte d'Or a créé au niveau départemental, trois comptes superadministrateurs et a créé au niveau régional, trois comptes superadministrateurs au niveau de la cellule de coordination régionale rattachée aux médecins du service médical de la direction générale du risque en région.

[redacted] sont titulaires d'un compte superadministrateur.

La CPAM de la Côte d'Or a notamment créé des comptes administrateurs locaux pour la CARSAT Bourgogne-Franche-Comté (Caisse d'assurance retraite et de la santé au travail), la MSA Bourgogne-Franche-Comté et l'ARS Bourgogne-Franche-Comté et des établissements de santé (privés comme publics)

En ce qui concerne l'accès au dispositif CONTACT COVID de la CPAM de la Côte d'Or

[redacted] *se connecte à l'interface d'administration des accès partenaires de l'application Contact Covid et illustre sa navigation à l'aide de copies d'écran (voir pièces en annexe).*

[redacted]

Sommes informés que la connexion à l'interface d'administration pour les superadministrateurs s'effectue au moyen de la carte agent, ce qui constitue un système d'authentification forte. Constatons que [redacted] e connecte au moyen de sa carte agent.

Les superadministrateurs accèdent à la liste des administrateurs locaux et de leurs utilisateurs (créés par ces derniers) pour l'ensemble du territoire national.

Au niveau de la CPAM de la Côte d'Or, il n'est pas mis en œuvre de supervision active des journaux aux fins d'identification de tentatives frauduleuses de connexion à un compte utilisateur sur le portail partenaire, la CPAM de la Côte d'Or n'ayant pas accès à ces journaux. La CPAM peut faire la demande de ces journaux en cas de suspicion d'accès frauduleux.

Lors de la création de comptes utilisateurs, la CPAM de la Côte d'Or considère qu'il appartient à l'administrateur local de délivrer à l'utilisateur des informations quant à l'usage de l'outil CONTACT COVID en lui faisant notamment signer un engagement unilatéral de confidentialité. Lors de l'entretien, qui dure en moyenne 30 min, des rappels sont faits sur la sécurité des données, la nécessité d'un engagement de confidentialité.

Constatons, pour les comptes rattachés à la MSA Bourgogne-Franche-Comté, la présence de 2 comptes administrateurs locaux et 18 comptes utilisateurs.

Constatons, pour les comptes rattachés à la CARSAT Bourgogne-Franche-Comté, la présence de 2 comptes administrateurs locaux et 11 comptes utilisateurs.

Constatons, pour les comptes rattachés à l'ARS Bourgogne-Franche-Comté, la présence de 150 comptes administrateurs et utilisateurs.

La CPAM de la Côte d'Or précise que, pour les ARS et les établissements de santé, le nom de domaine attaché à l'adresse de courriel de l'administrateur local et de ses utilisateurs doit être identique.

Effectuons les requêtes suivantes au moyen du champ de recherche des comptes utilisateurs et administrateurs de l'accès partenaire à la plateforme CONTACT COVID :

- CARSAT BOURGOGNE
- ARS BOURGOGNE
- MSA BOURGOGNE
- des comptes utilisateurs dont l'adresse électronique est rattachée au domaine :
    - wanadoo.fr,
    - yahoo.fr,
    - gmail.com,
    - orange.fr,
    - hotmail.com / hotmail.fr,
- des comptes utilisateurs dont l'adresse électronique contient
    - « prestataire »,
    - « partenaire »,
    - « secrétariat »,
    - « direction »,
    - « pharmacie ».

Constatons la présence d'adresse électronique de comptes administrateurs locaux ou utilisateurs se terminant par « *@orange.fr* », « *gmail.fr* », « *wanadoo.fr* » (voir pièces en annexe).

Constatons notamment la présence de comptes utilisateurs dont l'adresse de courriel commence par « secrétariat », « direction », « qualite », « infirmierhygieniste », « cadrebloc » (voir pièces en annexe).

Constatons notamment la création de comptes utilisateurs dont l'adresse de courriel commence par « pharmacie ». La CPAM de la Côte d'Or précise qu'il s'agit probablement de pharmacies à usage intérieur (voir pièces en annexe).

Mentionnons prendre copie des formulaires signés par les administrateurs locaux lors de la création de leur compte. Ces formulaires sont accompagnés, lors de leur signature, d'une copie de la pièce d'identité du demandeur, immédiatement supprimée à compter de la vérification de leur identité.

En ce qui concerne la suppression des données contenues dans le dispositif CONTACT COVID

[redacted] *se connecte à l'application Contact Covid et illustre sa navigation à l'aide de copies d'écran* [redacted]

Constatons la présence de 1 667 fiches dans le dispositif CONTACT COVID dont la date de modification est comprise entre le 14 mai 2020 et le 14 août 2020.

Constatons la présence de 1 667 fiches dans le dispositif CONTACT COVID dont la date de modification est comprise entre le 14 mai 2020 et le 14 août 2020 et la date de création est comprise entre le 14 mai 2020 et le 14 août 2020.

À notre demande, [redacted] ouvre plusieurs fiches issues des deux requêtes précédentes. Constatons que ces fiches sont liées à des cas contacts dont les données ont été actualisées dans les trois mois suivant la création des fiches et depuis moins de trois mois. En l'espèce, les patients zéros consultés sont liés à des cas contacts dont les données ont été actualisées depuis le 17 août 2020.

Lorsqu'une personne est testée positive au covid-19, l'agent de la CPAM en charge de créer la fiche P0 effectue une recherche dans l'outil CONTACT COVID à partir du NIR de la personne concernée. Lorsqu'il existe une ou plusieurs fiches « cas contact » associée à ce NIR dans l'outil CONTACT COVID, une de ces fiches est transformée en fiche « P0 ». La CPAM de la Côte d'Or nous indique qu'il semblerait que, lorsqu'il existe plusieurs fiches cas contact, la modification soit effectuée à partir de la fiche cas contact la plus récente afin de tracer les chaînes de contamination.

Constatons la présence d'une fiche patient zéro « P0-confirmé-contacté » créée le 22 mai 2020, le patient a été contacté le 23 mai 2020. La CPAM de la Côte d'Or précise que cette fiche apparait toujours dans le dispositif CONTACT COVID, car la fiche d'une des personnes identifiées comme un des cas contacts de ce patient zéro a été modifiée le 19 août 2020. [redacted]

Constatons la présence de 5 fiches dans le dispositif CONTACT COVID dont la date de création est comprise entre le 14 mai 2020 et le 28 mai 2020.

Constatons la présence d'une fiche « P0 – en attente de diagnostic », dans le dispositif CONTACT COVID, dont la date de modification est comprise entre le 14 mai 2020 et le 1er novembre 2020.

Ne constatons pas la présence de fiche « P0 – à contacter » dont la date de modification est comprise entre le 14 mai 2020 et le 1er novembre 2020 dans le dispositif CONTACT COVID.

Ne constatons pas la présence de fiche « P0 – clôturé » dont la date de modification est comprise entre le 14 mai 2020 et le 14 août 2020 dans le dispositif CONTACT COVID.

Ne constatons pas la présence de fiche « P0 – à rappeler » dont la date de modification est comprise entre le 14 mai 2020 et le 14 août 2020 dans le dispositif CONTACT COVID.

Ne constatons pas la présence de fiche « P0 – non avéré » dont la date de modification est comprise entre le 14 mai 2020 et le 15 novembre 2020 dans le dispositif CONTACT COVID.

En ce qui concerne le traçage des cas contacts dans les établissements scolaires et les universités :

Établissements scolaires :

En milieu scolaire, le traçage des cas contacts d'un patient zéro est d'abord réalisé par l'établissement scolaire puis par l'ARS Bourgogne-Franche-Comté en cas de suspicion de foyer de contamination au sein de l'établissement scolaire.

Le traçage des cas contacts d'un patient zéro en dehors de l'établissement scolaire est réalisé par la CPAM de la Côte d'Or.

L'information à destination des patients zéros et des cas contacts est désormais réalisée par l'établissement scolaire lui-même conformément au protocole mis en place par l'Éducation nationale. Une fiche d'information à destination des représentants légaux délivrée par les établissements scolaires a été formalisée par la CNAM et diffusée sur le territoire national à l'ensemble des établissements scolaires.

Lorsque les cas contacts ont été identifiés par la médecine préventive de l'établissement scolaire, la liste de ces cas est adressée par l'établissement scolaire à l'ARS qui le transmet à la CPAM de la Côte d'Or par l'intermédiaire d'un lien PÉTRA adressé par cette dernière. La CPAM crée ensuite les fiches des cas contacts identifiés dans l'outil CONTACT COVID. Le statut des fiches est passé en « Pc– appel réalisé ».

[redacted] accède à l'outil PETRA au moyen d'un identifiant qu'elle nous indique comme étant partagé avec une autre personne afin d'assurer la continuité opérationnelle.

Constatons qu'un tableur (fichier « Excel ») est adressé par le lien PETRA mis à disposition de l'ARS par la CPAM de la Côte d'Or contenant les données d'identification du patient zéro et de ses cas contacts.

Ces fichiers récupérés via la plateforme PETRA sont déposés par Mme MONTANDON ou son collègue sur un serveur de fichier réseau de la CPAM de la Côte d'Or et immédiatement supprimés de la plateforme PETRA. Ces fichiers sont ensuite supprimés du réseau dès leur intégration dans l'outil CONTACT COVID.

[redacted] nous présente le répertoire réseau destiné à recevoir les fichiers précédemment mentionnés. Constatons que ce répertoire ne contient pas de tableur.

Le fichier utilisé par l'établissement scolaire pour transmettre les informations relatives à un patient P0 et ses cas contacts est un fichier type transmis par la CNAM. Constatons que les

fichiers ouverts sur la plateforme PETRA et déposés le 17 novembre 2020 matin respectent ce modèle.

Une case « Contact hors brigade » a été ajoutée dans le dispositif CONTACT COVID pour les cas contacts identifiés dans les établissements scolaires.

Universités :

Pour les universités, le traçage des cas contacts d'un patient zéro est réalisé par l'ARS Bourgogne-Franche-Comté. La médecine préventive de l'université est en charge de l'enquête des cas avérés dans l'établissement puis contacte l'ARS Bourgogne-Franche-Comté qui prend attache avec les personnes ayant été en contact avec le patient zéro dans l'enceinte de l'université.

Lorsque les contacts avec le patient zéro ont eu lieu en dehors de l'enceinte de l'université, l'ARS Bourgogne-Franche-Comté prend attache avec la CPAM de la Côte d'Or afin qu'elle procède elle-même à des appels téléphoniques auprès de ces cas contacts.

Mentionnons que le [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie au moyen d'un lien PETRA ; que les pièces numériques ainsi communiquées ont été stockées, [redacted]

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 ;

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

[redacted]

La mission de contrôle s'est terminée, ce jour, à 15 heures 30 ;

En foi de quoi, il a été dressé procès-verbal contradictoire des diligences effectuées, signé par nous et [redacted] de la CPAM de la Côte d'Or.

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]

Paraphes [redacted]

[redacted]

PIECE N°7 : [redacted]

PIECE 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 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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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 ;

[redacted] dûment habilités à procéder à des missions de vérification sur place ;

En présence du [redacted] médecin expert près la Cour d'Appel de Dijon, en qualité de médecin expert ;

Le procureur de la République territorialement compétent préalablement informé ;

Le délégué à la protection des données de l'Agence Régionale de Santé Bourgogne-Franche-Comté (ci-après ARS BFC), [redacted] a été préalablement informé du contrôle par courriel et par appel téléphonique en date du 13 novembre 2020 ;

Nous sommes présentés le mercredi 18 novembre 2020, à 9 heures 30, dans les locaux de l'Agence Régionale de Santé Bourgogne-Franche-Comté, situés 2 Place des Savoirs à DIJON (21000) 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 :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted], médecin expert près la cour d'Appel de Dijon.

[redacted]

nous informent des éléments suivants :

En ce qui concerne l'ARS BOURGOGNE-FRANCHE-COMTÉ

L'ARS BOURGOGNE-FRANCHE-COMTÉ (« BFC »), est principalement répartie entre deux antennes situées à Dijon et Besançon qui pilotent à distance les équipes départementales et locales. Localement, les délégations départementales sont essentiellement composées d'animateurs territoriaux et de personnels santé-environnement.

L'ARS BFC emploie 420 ETP et a complété ses équipes d'environ 80 personnes supplémentaires depuis le début de la crise. Le budget global de l'ARS BFC est d'environ 37 millions d'euros.

L'ARS BFC a avancé des dépenses sur le fonds d'intervention régional (FIR) a hauteur de 10 millions d'euros (achat de matériel, masques, recrutement intérimaires, accompagnement des médecins, etc.) dans le cadre de la lutte contre le covid-19.

L'ARS BFC a fait le choix de garder, en interne, la maitrise pleine et entière du processus et de la supervision de l'ensemble des collaborateurs amenés à participer à l'activité de « contact tracing ». L'ARS BFC emploie en propre les personnes qui traitent les données en lien avec le COVID-19.

L'ARS BFC a mis en œuvre sa cellule régionale d'appui et de pilotage sanitaire qui pilote notamment l'activité de « contact tracing » en charge de freiner la propagation de l'épidémie de COVID-19. Au sein de la CRAPS, des équipes spécialisées ont été créées dans le cadre du « contact tracing » (CRAPS-COVID19) en charge de freiner l'épidémie de covid-19 et sont notamment chargées :

- des signaux entrants (appels publics, signaux sanitaires) ;
- des analyses et synthèses (stats, clusters, synthèses) ;
- des investigations et interventions (appuis et investigations, intervention) ;
- du suivi isolement (cellules de suivi).

[redacted]

L'ARS BFC applique les recommandations de Santé Publique France (SPF) en matière de définition de cluster. L'ARS BFC prend désormais en compte le seuil de 10 cas contact ainsi que les risques de propagation de la maladie en lien avec la CPAM locale (voir pièce en annexe).

Le suivi de l'isolement est assuré par l'ARS BFC. Dans ce cadre, les coordonnées des personnes nécessitant une aide particulière sont transmises aux cellules territoriales d'appui à l'isolement (CTAI), gérées par les préfectures.

En ce qui concerne l'application SORMAS :

L'outil SORMAS est un outil *open source*, développé par une université allemande sur financement de l'OMS. Il a été identifié par l'ARS BFC comme solution permettant d'assurer sa mission de contact tracing.

Une instance de SORMAS est déployée par l'ARS BFC. Un projet de déploiement de SORMAS à plus grande échelle est piloté au niveau interrégional. L'ARS BFC, compte tenu de son utilisation précoce de SORMAS poursuit l'utilisation de son instance, gérée localement.

L'ARS BFC participe aux développements de l'outil SORMAS.

L'ARS BFC a exprimé auprès de la direction du numérique (DNUM) du ministère des Solidarités et de la Santé la nécessité de bénéficier d'outils fiables permettant d'assurer ses missions dans le contexte de crise sanitaire actuel.

L'ARS BFC a construit ses processus de contact tracing autour de l'outil SORMAS.

Dès la réception d'un signal (niveau 3), l'outil SORMAS est utilisé, pour toutes les phases : investigation, retranscription des informations de contact tracing de l'assurance maladie, suivi et analyse des clusters, suivi des signaux, suivi des cas et des contacts. L'objectif de l'ARS BFC est de n'utiliser que l'outil SORMAS dans l'intégralité de son processus de gestion de l'épidémie. Le modèle de données de l'outil SORMAS doit permettre la gestion complète des signaux, des cas, des contacts et des clusters.

L'ARS-BFC sous-traite l'hébergement de l'application SORMAS au groupement régional d'appuis à la e-santé (« GRADeS »). Le GRADeS est un groupement d'intérêt public « GIP » qui reprend les prérogatives du groupement de coopération sanitaire « GCS » EMOSIST et le « GCS » e-santé Bourgogne. Le « GRADeS » BFC est agréé « hébergeur de données de santé » (HDS). SORMAS est hébergée au sein de l'espace numérique régional de santé (« ENRS »).

L'ARS BFC a tenu à ce que les données à caractère personnel qu'elle traite soient conservées par un HDS.

La CNAM a mis en place une transmission complète des données issues du traitement CONTACT COVID à destination des ARS utilisatrices de SORMAS. Cette extraction a lieu une à deux fois par jour.

L'ARS BFC récupère les données nationales issues de CONTACT COVID. Celle-ci filtre les données en ne retenant que les données des personnes vivant en BFC puis les injecte dans SORMAS.

Il n'y a aucune alimentation de l'outil SORMAS à partir de SI-DEP, mais une réflexion nationale est en cours pour rapprocher les données positives de SI-DEP avec celles de CONTACT COVID pour ensuite alimenter les différentes instances SORMAS.

[redacted]

L'ARS BFC est responsable du traitement SORMAS. L'ARS n'a conclu aucun contrat avec la DNUM en lien avec ce traitement.

Une analyse d'impact relative à la protection des données (AIPD) est en cours de rédaction, avec l'appui du logiciel PIA (*privacy impact assesment)* de la CNIL, concernant l'outil SORMAS. Celle-ci doit être finalisée au cours du mois de décembre.

La gestion de suivi de cas positifs et de cas contacts se fait essentiellement par l'outil SORMAS. L'ARS BFC considère que les outils de télésuivi n'ont pas vocation à servir d'outil de gestion de l'épidémie de COVID-19.

Les catégories de données traitées dans l'outil SORMAS sont les suivantes :

- identité,
- contact,
- statut (cas positif, contact)
- suivi,
- évènements et signaux identifiés,
- traitement de ces signaux et évènements.

Au sein de l'outil SORMAS sont présents des champs de commentaires libres. L'ARS BFC a donné l'instruction à l'ensemble de ses agents de ne faire figurer aucune donnée médicale dans l'outil SORMAS (à l'exception du statut – cas contact ou cas avéré – de la personne concernée).

Les agents (téléopérateurs du suivi isolement) saisissent, dans le champ de texte libre de l'onglet de suivi, les besoins exprimés par les personnes testées positives ou cas contacts dans le cadre du suivi par la cellule d'appui à l'isolement.

En ce qui concerne l'information des personnes des traitements réalisés des données collectées par l'ARS BOURGOGNE-FRANCHE-COMTÉ à partir de « Contact-covid »

L'ARS BFC informe les personnes concernées du traitement de leurs données dans l'outil SORMAS par l'intermédiaire de son site web.

L'ARS BFC a formalisé une procédure d'information des personnes concernées à destination de ses téléopérateurs.

En ce qui concerne l'exercice des droits des patients zéros et des cas contacts

L'ARS BFC recueille, par l'intermédiaire de ses téléopérateurs (du suivi isolement), le consentement des personnes concernées à être suivies par l'ARS.

L'ARS BFC n'a reçu aucune demande relative à l'exercice des droits des personnes concernées (droit d'accès, opposition) en lien avec l'épidémie de COVID-19.

L'ARS BFC considère que l'information, relative au traitement des données des personnes concernées dans le cadre du contact tracing, a déjà été délivrée par la CPAM locale lors de la saisie des données dans l'outil CONTACT COVID.

[redacted] [redacted]

En ce qui concerne les durées de conservation des données contenues dans l'outil SORMAS :

La fiche correspondant à un signalement est maintenue dans l'outil SORMAS, mais les données sont anonymisées et supprimées de l'affichage (IHM). Le script d'anonymisation/suppression des données est présenté et remis à la délégation (voir pièces en annexe).

Lorsque la date de signalement est supérieure à 90 jours, les noms et prénoms contenus dans une fiche correspondant à un signalement sont anonymisés (remplacés par FIRST et LAST suivi par l'identifiant SORMAS). Les données contenues dans les autres champs d'une fiche (cas ou contact), dont le champ commentaire, sont supprimés 90 jours après la date de signalement.

Lors de l'anonymisation/suppression des données, celles-ci voient leur statut passé à « Archivé » et ne sont plus visibles dans l'application.

Demandons à rechercher l'ensemble des cas dans l'outil SORMAS (via l'application). Effectuons un tri par date de signalement. Constatons la présence de deux fiches dont les dates de signalement sont antérieures à 90 jours. L'ARS BFC nous indique qu'il semblerait que le changement de statut d'un cas contact à un patient zéro soit réalisé à partir de la fiche cas contact déjà créée afin de tracer les chaînes de contamination.

En ce qui concerne le traitement de données à caractère personnel réalisé à partir de « CONTACT COVID »

Les données contenues dans l'outil SORMAS correspondent en majorité aux données saisies par les agents des CPAM locales dans l'outil CONTACT COVID. Une synchronisation étant effectuée environ 2 fois par jour.

L'ARS BFC dispose d'accès partenaires à l'application CONTACT COVID, les agents des cellules départementales d'investigation (CDI) peuvent être amenés, à la marge, à consulter des données dans l'outil CONTACT COVID. La consultation étant principalement à des fins de vérification en cas de données non synchronisées dans SORMAS.

Dans le cadre d'un signalement d'un éventuel cluster, le médecin (de la médecine préventive ou du service de la médecine au travail) adresse la liste des personnes identifiées comme cas positifs et cas contacts à l'adresse de contact unique mis en place par l'ARS BFC. L'ARS BFC adresse ensuite cette liste à la CPAM locale par l'intermédiaire d'un lien PETRA fourni par cette dernière.

Demandons [redacted] de nous présenter les signaux issus des médecines préventives et médecines du travail reçus par l'ARS BFC. Constatons que les messages (format .msg) sont stockés au sein de l'outil infonuagique (*cloud*) dont il nous est indiqué qu'il est hébergé par le GRADeS.

Constatons que lorsque le signalement d'un cas positif émane de l'assurance maladie, le courriel ne contient que le numéro associé à la fiche créée dans l'outil CONTACT COVID.

Constatons que certains courriels ont été adressés par des responsables des ressources humaines de sociétés ou le représentant d'un établissement scolaire.

Constatons, pour l'un des envois présentés à la délégation que le courriel contient un document PDF protégé par mot de passe.

L'ARS BFC ne traite que les cas positifs de personnes résidant dans la région BFC.

[redacted] *présente l'outil SORMAS à la délégation et documente sa navigation à l'aide de captures d'écran.*

Précisons que les copies d'écran de l'application SORMAS qui contiennent des données individuelles de santé sont placées dans un document distinct [redacted]

Constatons que [redacted] se connecte au portail applicatif (ENRS) au moyen d'un identifiant et d'un mot de passe suivi d'un code reçu par courriel ou par SMS. Ce portail applicatif contient un lien vers l'application SORMAS.

Constatons que la connexion à l'application SORMAS s'effectue au moyen d'un couple identifiant / mot de passe.

Constatons le dénombrement de 66 654 cas positifs enregistrés dans l'application SORMAS dans l'onglet « cas ».

Constatons le dénombrement de 171 379 cas contacts enregistrés dans l'application SORMAS dans l'onglet « contacts ».

Constatons la présence d'un champ de texte libre (« description ») dans le menu « Signal » / « Evènement ». Constatons la présence d'un champ de texte libre dans l'onglet de suivi des « cas » et des « contacts ».

Depuis le 10 novembre 2020, les éléments contenus dans les signalements opérés par l'intermédiaire d'un échange de courriel entre l'organisme et l'ARS BFC sont retranscrits dans l'outil SORMAS dans l'onglet « actions de l'évènement ».

À compter de la mi-novembre 2020, l'ARS BFC a prévu une gestion des pièces jointes directement dans l'application SORMAS.

Dans le cadre du contact tracing, l'ARS BFC a également recours à l'utilisation de tableurs (fichiers « Excel ») dans le cadre de la recherche de clusters (autour d'un signal pour identifier des liens entre des cas positifs) et d'un outil statistique « R », hébergé par le GRADeS en qualité de HDS.

L'ARS BFC souhaite intégrer, à terme, la recherche de clusters dans l'outil SORMAS à partir de 2021.

Les données inscrites par les agents de l'ARS dans l'outil SORMAS ne sont pas transmises aux CPAM locales ou à la CNAM et ne font pas l'objet d'une intégration dans CONTACT COVID.

L'ARS BFC précise que plusieurs onglets et menus de l'outil SORMAS ne sont pas utilisés. Les agents ont pour instruction de ne pas compléter certains champs présents dans l'outil (voir supports de formation et d'utilisation de l'outil en annexe).

En ce qui concerne l'envoi de SMS aux cas contacts et patients zéros de la région BFC

Un SMS ou, à défaut, un courriel, est envoyé par l'ARS BFC, aux cas contacts et aux patients zéros de la région BFC, à partir des données contenues dans le logiciel SORMAS. Ce message

[redacted] [redacted]

contient une URL unique (contenant l'identifiant SORMAS de la personne concernée) à partir duquel la personne peut exprimer son choix d'être suivie plus particulièrement par l'ARS BFC (voir pièces en annexe).

Le SMS est envoyé par un générateur de SMS hébergé chez le GRADeS, à partir de numéros de téléphones issus de SORMAS.

L'outil de télésuivi est une des options proposées dans le SMS : solution [redacted] (éditée par la société [redacted]

L'ARS BFC n'utilise pas les outils COVIDOM et COVISAN.

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 :

- Extraction de l'ensemble des champs de texte libre (« description ») de l'onglet évènement
- Extraction de l'ensemble des champs de texte libre des onglets de suivi (« cas » et « contact »)

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

[redacted]

[redacted]

La mission de contrôle s'est terminée, ce jour, à 18 heures 30

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]

[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.

Mentionnons que [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.

PIECE N°1 : [redacted]

- [redacted]

PIECE N°2 : [redacted]

- [redacted]

[redacted]

[redacted]

- [redacted]

PIECE N°3 : [redacted]

- [redacted]

[redacted]

- [redacted]

PIECE N°4 : [redacted]

- [redacted]

PIECE N°5 : [redacted]

- [redacted]

[redacted]

- [redacted]

PIECE N°6 : [redacted]

- [redacted]

PIECE N°7 : [redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]

PIECE N°8 : [redacted]

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

PIECE N°9 : [redacted]

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

[redacted]

- [redacted]

[redacted]

- [redacted]

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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, en particulier, il s'est agi de donner suite à la saisine n° 20008478.

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

En présence du docteur [redacted] médecin expert près la Cour de d'Appel de Bordeaux, en qualité de médecin expert ;

Le procureur de la République territorialement compétent préalablement informé ;

Nous sommes présentés le 04 février 2021, à 09h00, dans les locaux de Agence régionale de santé Nouvelle Aquitaine, situés 103 bis rue Belleville à Bordeaux (33000) 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 ;

 Paraphes [redacted]

Nous sommes entretenus avec :

[redacted]

Avons procédé aux diligences et constatations suivantes :

En ce qui concerne l'AGENCE REGIONALE NOUVELLE AQUITAINE

Sommes informés des éléments suivants :

L'ARS NOUVELLE AQUITAINE (ci-après désignée « ARS NA ») est issue de la fusion des régions Limousin, Aquitaine et Poitou-Charentes au 1er janvier 2016. Elle est répartie sur 13 sites. Elle regroupe 12 délégations départementales (ci-après désignées « DD »).

L'ARS NA a un effectif d'environ 845 équivalents temps plein dont 54% dans les délégations départementales.

L'activité de « *contact tracing* » de niveau 3 réalisée par l'ARS NA consiste principalement :

- au suivi de l'isolement des patients zéro et des cas contacts (à partir d'une extraction du système d'information CONTACT COVID réalisée par la Direction du numérique (ci-après désignée « DNUM ») du ministère des Solidarités et de la Santé (ci-après désignée « MSS») ;
- au suivi, au sein des délégations départementales, des foyers de contamination complexes (ci-après désignés « clusters »).

Demandons copie de la convention d'objectif, de la présentation de l'ARS NA, de l'organigramme de l'ARS NA, du schéma d'organisation du « contact tracing » de niveau 3.

En ce qui concerne le responsable des traitements mis en œuvre par l'ARS NA dans le cadre des traitements de « contact tracing » de niveau 3 et la base légale des traitements de « contact tracing » de niveau 3

Sommes informés des éléments suivants :

L'ARS NA a réalisé quatre « déclarations de traitements » correspondant à des fiches annexées à son registre des traitements.

Elles sont relatives :

- aux habilitations ;
- au suivi de l'isolement avant la mise en œuvre de [redacted]
- au suivi de l'isolement après la mise en œuvre de [redacted]
- au traitement des données extraites à partir du dispositif CONTACT COVID.

L'ARS NA a réalisé deux analyses d'impact (ci-après désignée « AIPD » sur les traitements liés à la mise en œuvre du « contact tracing » de niveau 3, relatives à :

- la gestion relative au suivi de l'isolement avant la mise en œuvre de [redacted] validée par le délégué à la protection des données) ;
- la gestion relative au suivi de l'isolement après la mise en œuvre de [redacted]

Demandons copie d'une extraction du registre des activités de traitement liées à la mise en œuvre de « CONTACT COVID » et du tracing de niveau 3 ainsi que des AIPD.

En ce qui concerne l'activité de « tracing » de l'ARS NA :

Sommes informés des éléments suivants :

En ce qui concerne l'activité de suivi de l'isolement

Dans le cadre de son activité de suivi de l'isolement et d'appels téléphoniques des personnes testées positives ou cas contacts, l'ARS NA a eu pour mission de procéder au suivi et au rappel des mesures d'isolement aux patients zéro et des cas contacts concernés par cette procédure.

A ce titre, l'ARS NA a procédé à des « campagnes de rappel » qui s'étendaient sur une période maximale de trois mois correspondant aux périodes d'évolution importantes des modalités de prise en charge des patients zéro et des cas contacts.

Pour ce faire, la DNUM met quotidiennement à disposition de l'ARS NA une extraction complète de données issues de la base de données CONTACT COVID.

L'ARS NA a eu recours aux services proposés par la société [redacted] en qualité de sous-traitant, afin de bénéficier d'un service adapté aux besoins de son activité de « *contact tracing* ».

La société [redacted] édite un outil de gestion des appels à destination des centres d'appels téléphoniques.

L'outil [redacted] contient notamment les noms et prénoms des personnes désignées comme patients zéro ou cas contacts.

L'ARS NA a eu recours à des étudiants en médecine de troisième année, recrutés par l'ARS NA en qualité de vacataires.

Les données sont conservées trois mois à compter de leur transmission par la CNAM. Une purge est manuelle dans ce délai. Les données sont écrasées à chaque nouvelle campagne de rappel qui durent en moyenne trois mois.

Cet outil a été mis en œuvre entre fin juin 2020 et le 20 janvier 2021.

Puis depuis le 21 janvier 2021, l'ARS NA ne gère plus l'activité de suivi de l'isolement, la CNAM a repris cette activité à compter du 27 janvier 2021.

En ce qui concerne l'activité de recherche des cas contacts et des patients zéro dans le cadre des foyers de contamination

Dès le 24 janvier 2020, le premier cas de Covid a été signalé à l'ARS NA par un établissement de santé de Bordeaux.

Au début de l'épidémie, et avant l'habilitation des agents de l'ARS NA à accéder à CONTACT COVID, une cellule départementale d'appui ad'hoc au sein de chaque direction départementale a été créée aux fins de gestion et de suivi de l'épidémie.

Au sein de l'ARS NA, l'échange des données relatives aux patients zéro ou cas contacts était réalisé :

- par l'intermédiaire de tableurs (Excel), par l'intermédiaire de messageries sécurisées de santé, conformément aux recommandations de la Caisse nationale de l'assurance maladie (ci-après désignée « CNAM ») ;
- puis, dans un second temps, par l'intermédiaire d'ordinateurs portables sécurisés mis à disposition par la CNAM permettant, à l'ARS NA, l'accès CONTACT COVID .

Depuis l'habilitation des agents de l'ARS NA à accéder à CONTACT COVID à partir de l'interface, dans le cadre des signalements complexes, les signalements transmis à l'ARS NA sont reçus par trois canaux :

- par la CPAM (notamment, dans le cadre d'un squat, de « gens du voyage »...) (voir pièces) ;
- par les établissements sanitaires, sociaux et médico-sociaux.
- par des entreprises et collectivités

La CNAM réalise désormais le suivi individuel des personnes dans le cadre des clusters lorsque les personnes sont facilement identifiables.

Dans le cadre de ces signalements complexes, d'une part, la CNAM, par l'intermédiaire des Caisse primaires d'assurance maladies locales (ci-après désignées « CPAM »), adresse un courriel à l'ARS NA contenant le numéro de la fiche CONTACT COVID ou les initiales des personnes, leur numéro de téléphone et la situation ayant conduit au signalement, de la personne concernée, à l'ARS NA.

D'autre part, les signalements émanent établissements sanitaires, sociaux et médico-sociaux par l'intermédiaire d'un courriel.

Chaque signalement entrant est reporté dans un tableur de suivi (Excel). Ils sont hébergés des réseaux sécurisés de l'ARS NA.

Les signalements sont notamment reçus sur une boîte aux lettres électronique dédiée, par exemple [redacted] pour la Gironde, ou sur la boîte aux lettres personnelles des médecins des DD.

La suppression des données contenues dans les boîtes aux lettres électroniques des personnes destinataires de signalements est réalisée manuellement par chacune de ces personnes.

En ce qui concerne le recours au sous-traitant

Sommes informés des éléments suivants :

L'ARS NA fait appel à 3 sous-traitants dans le cadre du contact tracing de niveau 3 :

- la société [redacted] éditrice d'un logiciel de gestion de campagnes de rappel téléphonique. La société fait appel à un hébergeur de données de santé dans le cadre de sa prestation avec l'ARS NA.

- Le GIP ESEA opère les messageries sécurisées de santé utilisées par les médecins de l'ARS NA.

- la DNUM du MSS fournie la messagerie électronique ainsi que le serveur d'identité « ACTIVE DIRECTORY » de l'ARS NA.

En ce qui concerne le recueil du consentement à la divulgation de l'identité du patient zéro au cas contact

Sommes informés des éléments suivants :

L'ARS NA ne recueille pas le consentement du patient zéro à la divulgation de son identité au cas contact car elle considère que ce consentement a déjà été recueilli par la CPAM locale lors du premier échange téléphonique.

L'ARS NA ne délivre pas l'identité du patient zéro au cas contact ou à l'organisme à l'origine du signalement.

Si l'ARS NA a besoin de divulguer l'identité du patient zéro à l'organisme à l'origine du signalement, elle recueille systématiquement le consentement auprès du patient zéro.

En ce qui concerne l'information des personnes sur le traitement de leurs données dans le cadre du « contact tracing » de niveau 3 et l'exercice de leurs droits « Informatique et Libertés »

Sommes informés des éléments suivants :

Les catégories de données traitées ainsi que l'exercice du droit des droits des personnes, dans le cadre du traitement CONTACT COVID, sont contenus sur le site web de l'ARS NA.

A la suite d'un appel téléphonique et depuis sa mise en place, un SMS, contenant un lien renvoyant vers le site web de l'ARS NA est systématiquement adressé à la personne isolée (cas contacts et patients zéros de la région NA), par l'intermédiaire de l'outil [redacted]

L'ARS NA n'a formalisé aucune procédure relative à l'exercice des droits des personnes.

En ce qui concerne la sécurité des données

Sommes informés des éléments suivants :

Depuis l'été 2020, la CNAM a fourni un accès à l'application « CONTACT COVID » accessible à partir d'une URL dédiée permettant l'accès à distance. Avant la mise en œuvre de cet accès, l'accès à l'application « CONTACT COVID » nécessitait un poste dédié.

L'authentification à l'application « CONTACT COVID » repose sur un mot de passe et un nom d'utilisateur.

Les tableaux de suivis des « clusters » ainsi que les exports de données de CONTACT COVID sont stockés dans un lecteur réseau hébergé par l'ARS NA. L'accès à ces fichiers est limité par la gestion des droits de fichiers WINDOWS.

L'authentification des utilisateurs par l'ACTIVE DIRECTORY repose sur un mot de passe et un nom d'utilisateur. Les mots de passe doivent être d'une longueur minimale de 8 caractères dont au moins une lettre et un chiffre, sans contrainte supplémentaire.

L'ACTIVE DIRECTORY est hébergé et administré par le MSS.

L'ARS NA ne fait pas appel à des sous-traitant pour réaliser le rappel des cas contact et des patients zéro.

En ce qui concerne la plainte n°20008478

Sommes informés des éléments suivants :

Une saisine a été déposée auprès de la CNIL à l'encontre de l'ARS NA le 22 juillet 2020 et enregistrée le 7 mai 2020.

D'une part, cette saisine fait état d'une demande, formulée par l'ARS NA auprès des laboratoires d'analyses de biologie de lui adresser, chaque jour, en clair et dans un tableur (Excel), les résultats des tests PCR Covid 19 comportant les noms, prénoms, date de naissance, adresse et numéro de téléphone des personnes testées

D'autre part, la saisine mentionne que les directeurs d'EHPAD, dans le cadre de la crise de la Covid 19 doivent adresser à l'ARS NA, en clair, des tableurs décrivant les symptômes de la personne testée positive au sein de ces établissements, comprenant également les données des salariés de ces établissements.

En réponse, l'ARS NA précise qu'il s'agissait du début de la mise en œuvre de l'activité de contact tracing par l'ARS NA et que les consignes données n'étaient pas celles décrites dans la saisine. L'ARS NA précise qu'il a s'agit d'une incompréhension, entre les acteurs, des modalités de transmission des données de personnes testées positives à la Covid.

L'ARS NA précise qu'elle n'a demandé que le nombre des personnes testées, le nombre des personnes positives dans les EHPAD, patients et salariés, ainsi que le nombre de personnes symptomatiques.

L'ARS NA précise que l'absence d'accès aux différents systèmes d'information dès le début de la crise, en janvier 2020, l'a contrainte à réaliser des traitements relatifs au « contact tracing » avant l'adoption d'un cadre juridique spécifique.

L'ARS NA indique les traitements qu'elle réalise dans le cadre de l'activité de contact tracing s'inscrivent dans les missions de l'ARS NA et en particulier, les traitements en lien avec la crise sanitaire.

Depuis la date de la saisine, l'ARS NA a modifié ses pratiques d'échanges afin de les sécuriser et notamment, par l'intermédiaire des messageries sécurisées de santé, utilisées depuis avril 2020.

Avons procédé aux constatations suivantes :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert.

A notre demande, [redacted] accède au lecteur réseau hébergé par l'ARS NA qui héberge les fichiers CSV issues de l'extraction de CONTACT COVID et documente sa progression à l'aide de captures d'écran.

Sommes informés que ce lecteur n'est accessible qu'à un groupe d'utilisateur limité (voir pièces).

A notre demande, [redacted] accède au lecteur réseau hébergé par l'ARS NA qui héberge les fichiers CSV issues de l'extraction de CONTACT COVID.

A notre demande, [redacted] accède au serveur ACTIVE DIRECTORY afin d'afficher la liste des membres du groupe ayant accès aux extractions de CONTACT COVID et documente sa progression à l'aide de captures d'écran.

A notre demande, [redacted] accède au dernier export de la base de données de l'application [redacted] Constatons que la base de données contient uniquement des signalements ayant été transmis par l'Assurance maladie entre le 07 novembre 2020 et le 20 janvier 2020.

A notre demande [redacted] accède aux tableaux de suivi des « clusters » et documente sa progression à l'aide de captures d'écran (voir pièces). Sommes informés que ces tableaux ne doivent pas contenir de données nominatives.

Constatons que l'ARS NA a traité 3011 signalements depuis le mois de mai 2020.

Prenons copie de deux tableaux de suivi départementaux ainsi que du tableau régional (voir pièces).

Sommes informés que la dernière campagne mise en œuvre a été supprimée de l'application [redacted] le 04 février 2020.

Sommes informés que le fichier transmis par la DNUM du MSS contient l'ensemble des données de CONTACT COVID pour l'ensemble cas contact et patients zéro de France. L'ARS NA réalise alors une extraction à partir de ce fichier afin d'alimenter les campagnes de rappel gérés dans le logiciel [redacted]

A notre demande [redacted] accède à sa boîte aux lettres personnelle et recherche les courriels relatifs aux signalements de « clusters » par l'assurance maladie ou par l'organisme à l'origine d'un signalement.

Ces courriels émanent soit de la boîte aux lettres électroniques dédiée [redacted], soit sont adressés directement par l'organisme signalant un éventuel cluster.

[redacted] nous précise que les CPAM n'adressent pas les signalements de foyers de contamination par l'intermédiaire d'une messagerie sécurisée de santé.

Constatons que les courriels de signalement peuvent contenir les données suivantes :

- Numéro de fiche CONTACT COVID
- Initiales
- Numéro de téléphone
- Département
- Élément justifiant le traitement par le niveau 3

[redacted] prend copie de deux signalements transmis par courriel.

A notre demande [redacted] accède à la boîte aux lettres commune [redacted] et recherche les courriels relatifs aux signalements de « clusters » par l'assurance maladie ou par l'organisme à l'origine d'un signalement. Sommes informés qu'il s'agit d'une messagerie sécurisée de santé.

Constatons que le signalement le plus ancien présent dans la boîte aux lettres date du 05 janvier 2021. Sommes informés, que les messages sont supprimés chaque mois. Constatons que le dossier « messages supprimés » de la boite aux lettres est vide.

[redacted] nous informe qu'il adresse les fichiers contenant les données nominatives des patients aux directions régionales du service médical par l'intermédiaire d'une messagerie sécurisée de santé.

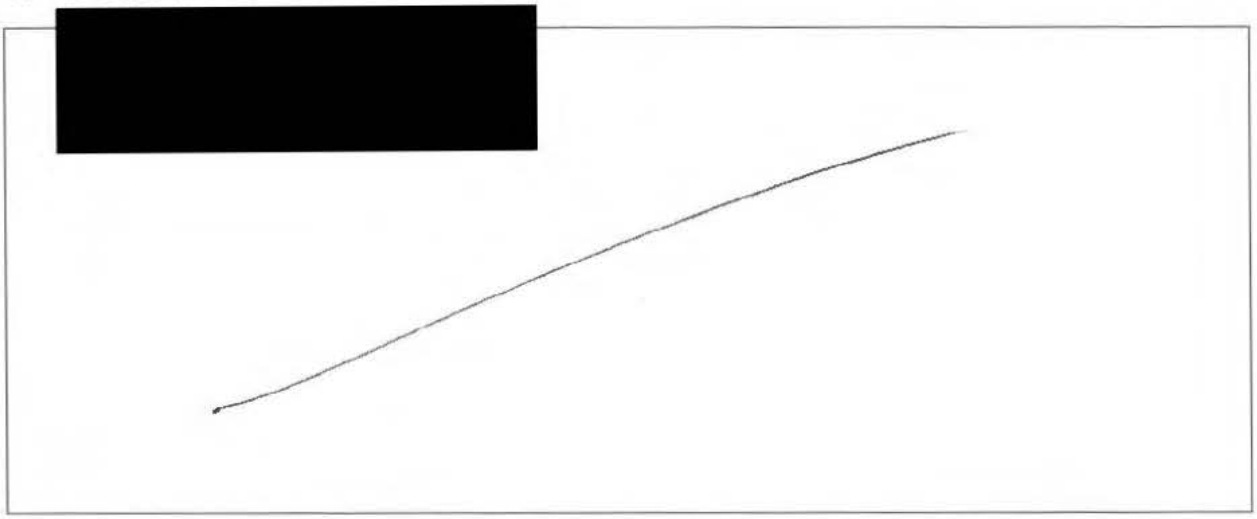
Avons demandé communication des documents nécessaires à l'accomplissement de notre mission et en avons pris des copies figurant dans l'inventaire joint en annexe du présent procès-verbal ;

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) le schéma d'organisation du « contact tracing » de niveau 3 ;
2) les dix dernières demandes d'exercice des droits des personnes relatives aux traitements liés au contact tracing de niveau 3;
3) Convention avec la DNUM relative à l'extraction des informations issues de CONTACT COVID ;
4) Certification HDS de l'hébergeur utilisé par l'outi[redacted]
5) Algorithme de stockage de mot de passe utilisé par l'ACTIVE DIRECTORY ;
6) Les modalités d'authentification à l'application [redacted] longueur minimale et complexité des mots de passe et algorithme utilisé pour le stockage des mot de passe.

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 18h00 ;

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.

Mentionnons que [redacted] *médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées,* [redacted] *sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.*

PIECE N°1 : [redacted]

- [redacted]

PIECE N°2 : [redacted]

[redacted]

PIECE N°3 : [redacted]

Paraphes [redacted]

- [redacted]
- [redacted]

PIECE N°4 : [redacted]

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

PIECE N°5 : [redacted]

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

- [redacted]

PIECE N°6 : [redacted]

- [redacted]

PIECE N°7 : [redacted]

- [redacted]

PIECE N°8 : [redacted]

- [redacted]

Paraphes [redacted]

- [redacted]

PIECE N°9 : [redacted]

- [redacted]

PIECE N°10 : [redacted]

- [redacted]

PIECE N°11 : [redacted]

Paraphes [redacted]

- [redacted]

PIECE N°12 : [redacted]

- [redacted]

PIECE N°13 : [redacted]

- [redacted]

PIECE N°14 : [redacted]

- [redacted]

PIECE N°15 : [redacted]

- [redacted]

PIECE N°16 : [redacted]

Paraphes [redacted]

PIECE N°17 : [redacted]

PIECE N°18 : [redacted]

PIECE N°19 : [redacted]

PIECE N°20 : [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°2020-091C en date du 22 mai 2020, la mission a eu pour objet à la vérification sur place de la conformité du traitement de données à caractère personnel dénommé « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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.

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

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

Le procureur de la République territorialement compétent préalablement informé ;

[redacted] a été préalablement informé du contrôle par courriel le 08 mars 2020.

Nous sommes présentés le 17 mars 2021, à 9h00, dans les locaux de l'Agence régionale de santé, situés Cité Coligny - 131 rue du faubourg Bannie à Orléans (45044) 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 :

L'Agence régionale de santé Centre-Val de Loire

Sommes informés des éléments suivants :

L'ARS Centre-Val de Loire a été créée le 1er avril 2010.

Elle comprend six délégations départementales correspondant à chaque préfecture de la région Centre-Val de Loire.

Au début de l'épidémie, sa gestion était assurée par une équipe régionale située au siège de l'ARS CVL. Du fait de l'augmentation des cas, la gestion de l'épidémie a été réalisée par une équipe régionale répartie entre les délégations départementales et le siège de l'ARS CVL.

L'ARS CVL a un effectif de 310 équivalents temps plein.

Environ 20 agents appartenant à l'ARS CVL sont dédiés à l'activité de contact tracing de l'ARS CVL.

50 à 70 personnes, en plus des agents appartenant à l'ARS CVL, ont participé à l'activité de contact tracing de l'ARS CVL. Ces effectifs supplémentaires sont principalement composés des professionnels et de personnels de santé.

Le budget d'intervention pour l'année 2020 de l'ARS CVL est de 149 millions d'euros.

Depuis mai 2020, l'ARS CVL a reçu environ entre 40 (a minima) et 300 signaux par jour (en novembre 2020) de la part des caisses primaires d'assurance maladie (CPAM) et des partenaires listés ci-dessous.

A ce jour, l'ARS CVL reçoit environ 100 signaux par jour qui nécessitent une investigation de niveau 3.

La responsabilité des traitements mis en œuvre par l'ARS CVL dans le cadre des traitements de « contact tracing » de niveau 3 et la base légale de ces traitements

Sommes informés des éléments suivants :

L'ARS CVL se considère responsable de traitement du serveur de fichiers utilisé pour le stockage des documents d'investigation hébergés en interne.

L'ARS CVL se considère responsable conjointe de traitement des données contenues dans l'application SORMAS avec l'ensemble des ARS utilisatrices de l'application SORMAS.

[redacted] [redacted]

L'ARS CVL n'a pas de registre de traitement global mais a formalisé une fiche de traitement relative aux traitements mis en œuvre dans le cadre du « contact tracing » de niveau 3.

La base légale des traitements liés à la mise en œuvre du « contact tracing » de niveau 3 est la mission d'intérêt public.

L'ARS CVL n'a pas, à ce jour, réalisé d'analyse d'impact sur les traitements liés à la mise en œuvre du « contact tracing » de niveau 3, mais a identifié la nécessité de réaliser une analyse d'impact.

L'activité de « contact tracing » réalisée par l'ARS CVL

Sommes informés des éléments suivants :

L'ARS CVL reçoit les signalements de patients zéro ou de cas contacts nécessitant une investigation de niveau 3 par le biais de deux canaux :

- Une boîte aux lettres dédiée dans le cadre de signalements ne contenant aucune donnée identifiante,
- des applications dédiés éditées par Santé Publique France lorsqu'il s'agit de personnes testées positives au sein d'établissement de santé, d'EHPAD, etc.

L'ARS CVL reçoit notamment les signalements de patients zéro ou de cas contacts nécessitant une investigation de niveau 3 sur une boite aux lettres électronique « alerte » dédiée.

Ces signalements sont ensuite envoyés sur une boite aux lettres électronique « régulation » dédiée à la gestion de la crise sanitaire.

La boîte aux lettres « régulation » est purgée une fois par semaine.

Ces boîtes aux lettres électroniques ne sont pas des messageries sécurisées de santé (MSS).

Les signalements ne contiennent pas de données directement identifiantes concernant les patients. Ils contiennent notamment le numéro d'identification CONTACT COVID ainsi que la typologie d'établissement (EHPAD, crèches…).

Les équipes responsables de la régulation sont chargées de récupérer les données nominatives relatives aux patients signalés dans le téléservice CONTACT COVID à partir du numéro d'identification CONTACT COVID.

A partir des signalements reçus par ce biais, l'ARS CVL assure le suivi et la gestion des signalements :

- émanant des établissements de santé MCO et des établissements publics de santé mentaux,
- émanant des EHPAD,
- émanant des établissements médicaux sociaux pour les personnes en situation de handicap,
- émanant d'une structure de soin résidentielle pour les personnes sans domiciles fixes,
- dans le cadre de l'identification de personnes infectées par les variants V2 et V3 (sud-africains et brésiliens),

[redacted] [redacted]

- lorsque les signalements attribués au prestataire sont trop complexes et qu'ils ne peuvent pas être traités par ce dernier (voir ci-dessous).

L'ARS CVL ne procède pas systématiquement à l'appel téléphonique des patients zéro ou des cas contacts identifiés dans le cadre des signalements transmis par les CPAM locales.

S'il apparait qu'un patient zéro est infecté par le variant V2 ou V3, l'ARS CVL procède à l'appel téléphonique du patient zéro, et plus exceptionnellement, aux cas contacts de ce patient dans le cadre de rassemblements ou lorsque le patient n'est pas en mesure de retracer l'origine de la transmission.

Dans le cadre du suivi de ces signalements, l'ARS CVL répertorie les informations relatives au suivi des personnes inscrites dans CONTACT COVID sur un espace de travail situé sur un serveur de fichiers.

Lorsque les signalements adressés par une CPAM locale à l'ARS CVL contiennent des données nominatives telle que la liste des patients zéro ou des cas contacts, leurs envois sont réalisés par l'intermédiaire d'une MSS.

Enfin, lorsque qu'une administration dispose d'un service de gestion en interne du contact tracing de niveau 3, l'ARS CVL délègue le suivi des patients zéro et des cas contacts à ces administrations.

L'ARS CVL travaille ainsi en collaboration avec le rectorat de la région Centre-Val de Loire (hors vacances scolaires), le service de santé universitaire de Tours avec une équipe dédiée (Indre et Loire et Loir et Cher), le service de santé des armées, la direction régionale de l'alimentation agriculture et forêt (lycées agricoles…) et les services de santé au travail de la région Centre-Val de Loire.

Pour ce faire, ces administrations n'ayant pas accès au téléservice CONTACT COVID, l'ARS CVL procède, à partir de l'identifiant CONTACT COVID, à la ré-identification des personnes désignées dans un signalement d'une CPAM locale. Les données nominatives des personnes désignées dans un signalement sont ensuite transmises aux administrations listées ci-dessus par l'intermédiaire d'une MSS.

L'ARS CVL n'adresse pas de courriel ou de SMS aux personnes après un entretien téléphonique.

En accord avec le niveau régionale de l'Assurance Maladie, l'ARS CVL n'alimente pas le téléservice CONTACT COVID.

L'activité de « contact tracing » réalisée par le sous-traitant de l'ARS CVL

Sommes informés des éléments suivants :

L'ARS CVL a délégué une partie de la gestion du suivi des patients zéro et cas contacts à la société [redacted]

La société [redacted] est ainsi chargée de l'activité de « contact tracing » de niveau 3 :

- des structures d'accueil du jeune enfant, périscolaire,
- des structures de l'aide à l'enfance,

[redacted]

- des signalements émanant de l'Université d'Orléans (Cher, Eure et Loire, Loiret et l'Indre) ;
- des entreprises du bâtiment de l'Indre et Loire et du Loir et Cher,
- des structures d'hébergement collectif,
- voyages à l'étranger,
- des établissement sociaux d'hébergement et d'insertion,
- des rassemblements et les cas positifs ayant eu plus de 11 contacts à risque,
- du sport,
- de la culture,
- de l'enseignement et formation hors du système universitaire pendant les périodes de vacances scolaires,
- de l'administration et collectivités territoriales,
- des établissements pour personnes âgées non médicalisés et soins à domiciles non médicalisées,
- de tous les professionnels de santé.

La société [redacted] est chargée, à partir des fiches de signalement émises par une CPAM, et transmises par l'ARS CVL, de prendre contact, par courriel ou appel téléphonique, avec la structure désignée dans le signalement.

Lors de cet échange, des instructions sont données à la structure afin qu'elle assure elle-même la gestion et le suivi des personnes testées positives ou ayant pu être en contact avec ces personnes.

La société [redacted] ne gère l'activité de contact tracing qu'à partir de l'application SORMAS.

La société [redacted] a accès à l'application CONTACT COVID mais ne l'alimente pas.

L'application SORMAS

Sommes informés des éléments suivants :

Avant décembre 2020, l'activité de contact tracing de niveau 3 et le suivi des cas positifs ou de leurs cas contacts était réalisé par l'intermédiaire de fichiers textes (Word). L'ARS CVL a ensuite eu recours à l'application One Note pour assurer ce suivi.

Depuis décembre 2020, la société [redacted] utilise une instance de l'application SORMAS dans le cadre de l'activité de contact tracing de niveau 3 de l'ARS CVL.

Depuis janvier 2021, l'ARS CVL utilise une instance de l'application SORMAS dans le cadre de son activité de contact tracing de niveau 3.

L'application SORMAS est alimentée par le téléservice CONTACT COVID et l'application SI-DEP.

Tous les signalements nécessitant une investigation de niveau 3 donnent lieu à la création :
- par l'ARS CVL, d'un « évènement » dans l'application SORMAS attribuée à l'origine d'un éventuel foyer de contamination ;
- par import automatisé depuis CONTACT COVID, d'une fiche « identité » attribuée à un cas « confirmé » (testé positif) ou à un cas contact.

Les fiches liées à un évènement et les fiches liées à un patient zéro ou à un cas contact ne sont pas systématiquement reliées entre elles.

Parallèlement, la personne désignée pour traiter l'évènement dans l'application SORMAS vérifie que l'identité de la personne testée positive ou d'un cas contact renseignée dans la téléservice CONTACT COVID correspond effectivement à celle inscrite dans l'application SORMAS.

Le recours des sous-traitants

Sommes informés des éléments suivants :

L'ARS CVL a conclu une convention avec la société [redacted] en qualité de sous-traitant, pour le traitement des données issues du téléservice CONTACT COVID et enregistrées dans l'application SORMAS, dans le cadre des traitements de « contact tracing » de niveau 3.

L'ARS CVL a conclu une convention avec la direction du numérique (DNUM) du ministère des Solidarités et de la Santé, en qualité de sous-traitant, pour l'administration et l'hébergement de l'instance de l'application SORMAS.

L'ARS CVL a conclu avec la société [redacted] en qualité de sous-traitant, pour la mise à disposition d'une MSS.

Le recours à hébergeur de données dans le cadre des traitements de « contact tracing » de niveau 3

Sommes informés des éléments suivants :

Les sociétés [redacted] et [redacted] fournissent des services certifiés hébergeurs de données de santé.

L'information des personnes sur le traitement de leurs données dans le cadre du « contact tracing » de niveau 3 et l'exercice de leurs droits « Informatique et Libertés »

Sommes informés des éléments suivants :

Une charte utilisateur est délivrée aux personnes amenées à accéder aux applications CONTACT COVID et SORMAS.

L'ARS CVL n'a pas formalisé de document d'information destiné aux personnes dont les données issues de CONTACT COVID sont traitées dans le cadre de l'activité de « contact tracing » de niveau 3.

Au jour du contrôle, aucun information relatives aux traitements dans le cadre de l'activité de « contact tracing » de niveau 3 n'est présente sur le site web institutionnel de l'ARS CVL. Une information est en cours de rédaction.

L'ARS CVL considère ainsi que la CPAM, les administrations ou les établissements à l'origine du signalement ont d'ores et déjà informé des personnes dont les données issues de CONTACT COVID.

L'ARS CVL a formalisé une procédure d'exercice des droits des personnes globale comprenant les droits des personnes dont les données issues de CONTACT COVID.

[redacted]

Le site web de l'ARS CVL contient une page dédiée à l'exercice des droits des personnes sur laquelle figure une adresse de courriel dédiée. Le service DPO est chargé de répondre aux demandes d'exercice de droits des personnes concernées.

Le recueil du consentement à la divulgation de l'identité du patient zéro au cas contact

Sommes informés des éléments suivants :

L'ARS CVL ne communique l'identité d'un patient zéro à un cas contact seulement lorsque le consentement du patient zéro à la divulgation de son identité au cas contact est indiqué dans l'encart de la fiche du téléservice « CONTACT COVID » prévu à cet effet.

En ce qui concerne les durées de conservation

Sommes informés des éléments suivants :

L'ARS CVL n'a pas formalisé une procédure de conservation des données relatives aux traitements mis en œuvre par l'ARS CVL dans le cadre des traitements de « contact tracing » de niveau 3.

L'ARS CVL a défini une durée de conservation de trois mois pour les données des patients zéro, cas contacts ou cas co-exposés à compter de leur collecte. Il s'agit de la durée prévue par les textes applicables.

L'ARS CVL considère qu'il revient à la DNUM du ministère des Solidarités et de la Santé de mettre en œuvre une purge automatique des données issues de CONTACT COVID et importées dans l'application SORMAS à l'issue du délai de conservation de trois mois.

Les données contenues dans le serveur de fichiers ne sont pas systématiquement supprimées. Une réflexion sur la suppression automatique de ces données est en cours. L'ARS CVL est dans l'attente d'un espace sécurisé fourni par la DNUM pouvant héberger des données de santé.

Dans un but statistique, l'ARS CVL conserve une synthèse anonymisée des signalements reçus contenant le trigramme des signalements enregistrés ou traités.

Aucune consigne d'archivage intermédiaire ou de suppression n'a été reçue par l'ARS CVL pour leurs fichiers hébergés en interne. Ces fichiers sont supprimés manuellement.

Violation de données subie par l'ARS CVL

Sommes informés des éléments suivants :

L'ARS CVL n'a eu pas eu connaissance d'une violation des données issues de CONTACT COVID traitées dans le cadre de l'activité de « contact tracing » de niveau 3 depuis mai 2020.

L'ARS CVL a formalisé une procédure relative à la gestion des violations de données.

L'ARS CVL tient un registre de violations des données. L'ARS CVL n'a pas subi de violations des données.

La sécurité des données

[redacted]

Sommes informés des éléments suivants :

Depuis le mois d'août 2020, la CNAM a fourni un accès à l'application « CONTACT COVID » accessible à partir d'une URL dédiée permettant l'accès à distance. Avant la mise en œuvre de cet accès, l'accès à l'application « CONTACT COVID » nécessitait un poste dédié.

Au jour du contrôle, l'ARS dispose de 57 comptes utilisateurs nominatifs et de 7 comptes administrateurs.

L'authentification à l'application « CONTACT COVID » repose sur un mot de passe et un nom d'utilisateur (adresse de messagerie). [redacted]

Chaque création de compte utilisateur au sein de l'application « CONTACT COVID » est validée par le directeur par intérim de la direction santé publique environnementale de l'ARS CVL.

Toutes les 2 semaines environ, une revue des comptes est réalisée au sein de l'ARS CVL. [redacted]

Les comptes « WINDOWS » permettant l'accès au dossier contenant les signalements sont nominatifs.

L'authentification à l'application SORMAS repose sur un mot de passe et un nom d'utilisateur ainsi que la déclaration d'un liste blanche d'adresse IP autorisées à l'application. La mise en œuvre d'une double authentification est prévue dans les prochaines semaines avec un code à usage unique envoyé par SMS ou par courriel.

Avons procédé aux constatations suivantes :

Précisons que l'accès à des données médicales individuelles a été effectué sous l'autorité et le contrôle du [redacted] médecin expert.

A notre demande, [redacted] se connecte au serveur de fichiers contenant les signalements issus de CONTACT COVID et documente sa progression à l'aide de captures d'écran.

Sommes informés que les données issues de CONTACT COVID sont enregistrées dans le dossier « contact covid ».

Sommes informés que la date contenue dans le nom de fichier correspond à la date de traitement du signalement.

Constatons que les dossiers relatifs aux signalements au sein d'établissements relevant de l'éducation nationale sont vides. Constatons que la date de modification de ces dossiers est le 15 mars 2021.

Sommes informés qu'une purge des données a été réalisée à cette date.

[redacted]

Prenons copie des fichiers des « points de situations » retraçant l'historique des signalements au sein des établissements relevant de l'éducation nationale.

Sommes informés que ces fichiers ne contiennent pas de données nominatives.

Constatons qu'un fichier nominatif de signalement issue de la médecine du travail datant du 07 juillet 2020 est toujours présent sur le serveur de fichiers.

Sommes informés que la purge des données antérieure à 3 mois n'est pas encore finalisée.

Constatons la présence de 62 signalements nominatifs en août 2020, 174 signalements nominatifs en octobre 2020, 19 signalements nominatifs en novembre 2020 présents sur le serveur de fichiers. Ces signalements ont été transmis par les services de santé au travail du Loiret.

Sommes informés que depuis novembre 2020, les services de santé au travail disposent d'une MSS afin de transmettre directement aux CPAM la liste de leurs cas contact et patient positifs.

A notre demande, [redacted] se connecte à l'application SORMAS et documente sa progression à l'aide de captures d'écran.

Constatons [redacted] n'a accès qu'aux signalement concernant la région Centre Val de Loire.

Sommes informés que dans l'application SORMAS, chaque ARS n'a accès qu'aux signalements concernant sa région.

Constatons qu'un message indique qu'une fiche non mise à jour est automatiquement archivée.

Constatons que la fiche archivée la plus ancienne dans SORMAS date du 28 août 2020.

Constatons que la fiche active la plus ancienne dans SORMAS date du 28 octobre 2020.

Sommes informés que ces fiches, étant antérieures à la date d'utilisation de SORMAS par l'ARS VDL, ont dû être importées automatiquement depuis CONTACT COVID par la DNUM.

Constatons la présence de 50 617 fiches dont 26 890 actives dans l'application SORMAS.

A notre demande, [redacted] connecte l'application CONTACT COVID et documente sa progression à l'aide de captures d'écran.

Constatons la présence de 45 fiches dont la dernière modification a été réalisée entre le 15 mai 2020 et le 16 décembre 2020.

Mentionnons que [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.

[redacted]

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) la procédure de durées de conservation des données relatives aux traitements mis en œuvre par l'ARS CVL dans le cadre des traitements de « contact tracing » de niveau 3 ;
2) Tout document relatif à la purge automatique ou à l'archivage des données contenues dans SORMAS ;
3) tous les éléments encadrant les relations contractuelles entre l'ARS VDL et ses sous-traitants [redacted] a DNUM et [redacted]
4) la certification hébergeur de données de santé (HDS) des sociétés [redacted] et [redacted]
5) de préciser si, d'une manière ou d'une autre, des données à caractère personnel sont transférées en dehors de l'Union Européenne et, le cas échéant, de quelle manière et quelles sont les garanties associées;
6) Tout document relatif à la politique de complexité des mots de passe ainsi qu'à l'algorithme de stockage des mots de passe pour l'application SORMAS et pour l'Active Directory ;
7) Liste des personnes disposant d'un accès au dossier contenant les signalements dans le serveur de fichier W.

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 18h30 ;

[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]

[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.

Mentionnons que [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, par [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.

PIECE N°1 : [redacted]

- [redacted]

PIECE N°2 : [redacted]

- [redacted]
- [redacted]

PIECE N°3 : [redacted]

- [redacted]
- [redacted]

PIECE N°4 : [redacted]

- [redacted]

[redacted]

PIECE N°5 : [redacted]

- [redacted]

PIECE N°6 : [redacted]

- [redacted]

PIECE N°7 : [redacted]

- [redacted]

[redacted]

PIECE N°8 : [redacted]

- [redacted]

PIECE N°9 : [redacted]

- [redacted]
- [redacted]

PIECE N°10 : [redacted]

[redacted]

[redacted]

[redacted]

PIECE N°11 : [redacted]

- [redacted]
- [redacted]

PIECE N°12 : [redacted]

- [redacted]

PIECE N°13 : [redacted]

- [redacted]

PIECE N°14 : [redacted]

- [redacted]

PIECE N°15 : [redacted]

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

[redacted]

- [redacted]

PIECE N°16 : [redacted]

- [redacted]

PIECE N°17 : [redacted]

- [redacted]

PIECE N°18 : [redacted]

- [redacted]

PIECE N°19 : [redacted]

- [redacted]

[redacted]

- [redacted]
- [redacted]

PIECE N°20 : [redacted]

- [redacted]
- [redacted]

2

Signature des membres de la mission de vérification	Signature du responsable des lieux
[redacted]	[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, les articles L. 251-1 et suivants du code de la sécurité intérieure, les 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°2020-091C 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié, 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.

[redacted]

En présence [redacted], médecin expert près la cour d'Appel, en qualité de médecin expert.

Le procureur de la République territorialement compétent préalablement informé.

Nous sommes présentés le 23 novembre 2021, à 09h30, dans les locaux du Rectorat de l'académie d'Orléans-Tours, situés 21, rue Saint Etienne à Orléans (45000) et avons été reçus par [redacted]

Cette dernière a informé la délégation de contrôle que les équipes en charge de la gestion des élèves testés positifs au COVID et leurs cas contact sont situées, pour le département du Loiret, dans les locaux de la direction des services départementaux de l'éducation nationale (DSDEN) situés 19, rue Eugène Vignat à Orléans (45000). La délégation s'est rendue dans les locaux de la DSDEN.

Nous sommes présentés le 23 novembre 2021, à 10h00, dans les locaux du Rectorat de l'académie d'Orléans-Tours, situés 19, rue Eugène Vignat à Orléans (45000) et avons été reçus immédiatement.

Le responsable des lieux au sens du décret précité, en la personne de [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 du Rectorat de l'académie d'Orléans-Tours

Sommes informés des éléments suivants :

L'académie Orléans-Tours est dirigée par la Rectrice. Cette académie est composée de six départements dont le Loiret. Chaque département est piloté par un adjoint de la Rectrice. Ces adjoints sont également inspecteurs de l'académie, directeur académique des services de l'éducation nationale (IADASEN).

Le Secrétaire général de la DSDEN notamment pour mission de gérer le bon fonctionnement des équipes de Directions des services départementaux de l'éducation nationale (DSDEN).

Pour la DSDEN du Loiret, il est prévu qu'elle soit dotée de dix médecins (équivalent temps plein « ETP ») et d'un médecin conseiller technique (médecin qui coordonne les activités des médecins de la DSDEN). Au jour du contrôle, la DSDEN du Loiret compte un effectif de 3,6 ETP de médecins effectivement en poste et aucun médecin conseiller technique. Ce rôle est de fait assuré par le médecin conseiller technique de la Rectrice.

Ces médecins ont un rôle de médecine préventive. Leurs principales missions sont :
- L'aménagement des épreuves des examens pour les élèves qui en auraient besoin ;
- Les visites nécessaires à la dérogation à l'utilisation de machines dangereuses dans les établissements scolaires à voie professionnelle ;
- Les visites afin de contrôler les obligations médicales dans les établissements scolaires.

Au commencement de l'épidémie, une cellule dédiée au COVID a été créée au niveau du rectorat. Dès 2020, une cellule a été structurée au niveau de la DSDEN du Loiret. Le rôle de cette cellule a évolué et est voué à évoluer selon les instructions du ministère de l'Éducation nationale (MEN) dont le rectorat dépend.

[redacted]

Au jour du contrôle, les missions de la cellule COVID au sein de la DSDEN du Loiret sont notamment la mise en place d'un accueil téléphonique à disposition des chefs d'établissement ou des inspecteurs de l'éducation nationale (IEN) et l'appui du médecin conseil technique dans la décision de fermeture de classe.

La direction de la DSDEN est également informée par les chefs d'établissements et IEN des survenues de cas de COVID au sein d'un établissement.

La mise en œuvre de cette organisation est adossée au protocole sanitaire mis à disposition par le MEN, sur la Foire Aux Questions (FAQ) disponible sur le site web du MEN et respecte les instructions du médecin conseiller technique de la rectrice.

La collecte et le traitement des données des personnes testées positives, des cas à risque et des cas contacts par la DSDEN

Lorsqu'un élève, scolarisé dans un établissement scolaire du département du Loiret, présente des symptômes ou est testé positif, les parents de cet élève ou l'élève lui-même doivent rapporter l'information au directeur d'école ou au chef d'établissement.

Le chef d'établissement ou l'IEN procède ensuite à la collecte d'un certain nombre de données individuelles de santé et notamment les données relatives à la traçabilité du parcours de l'élève durant les jours précédents le test dont le résultat est positif.

Ces données sont retranscrites dans une fiche dédiée dénommée « note d'information COVID 19 positif ou situation complexe ». Cette fiche est déclarative et repose sur les données transmises par les parents de l'élève testé positif.

La fiche est mise en œuvre par la DSDEN et conçue avec l'aide du médecin conseiller technique appartenant au Rectorat d'Orléans-Tours.

La fiche contient notamment l'identité de l'élève testé positif, la date à laquelle il a été testé positif, s'il présente des symptômes, s'il a déjeuné avec d'autres élèves au sein de la cantine de l'établissement scolaire, s'il a participé à des activités sportives dans le cadre scolaire, etc.

Après avoir complété cette fiche ou collecté les informations nécessaires à la complétion de cette fiche à l'aide des informations transmises par les parents de l'élève, le chef de l'établissement ou l'IEN peut (i) soit, appeler la cellule COVID afin de lui transmettre, par téléphone, les données collectées auprès des parents de l'élève (ii) soit transmettre directement cette fiche par courrier électronique à une adresse dédiée cellulecovid45@ac-orleans-tours.fr mise en place par la DSDEN.

Lorsque la fiche est reçue par courrier électronique, le courrier est stocké dans la boite aux lettres électronique cellulecovid45@ac-orleans-tours.fr. Cette fiche est ensuite imprimée en format papier.

Cette fiche imprimée en format papier ainsi que la fiche qui est remplie directement par les services de la cellule COVID de la DSDEN, dans le cadre de la retransmission des informations par le chef d'établissement ou l'IEN par téléphone, sont conservées au sein des bureaux de la cellule COVID de la DSDEN.

Les fiches ainsi remplies sont ensuite analysées par les médecins ou infirmiers de la cellule COVID qui détermine, au regard des informations contenues dans ces fiches, s'il y a un ou plusieurs cas contact à risque élevé.

[redacted]

Lorsque la cellule a identifié un cas contact à risque élevé, elle informe le chef d'établissement ou l'IEN qu'une fiche complémentaire, dénommée FT19, doit être remplie par ces derniers puis transmise à la cellule COVID de la DSDEN sur l'adresse dédiée [redacted]

Cette cellule transmet ensuite la fiche FT19, par l'intermédiaire d'une messagerie sécurisée de santé (MSS) d'un médecin, à la caisse primaire d'assurance maladie locale (CPAM).

[redacted]

Après réception de la fiche FT19, la CPAM la complète en indiquant si les cas contact à risque élevé nécessitent un isolement ou non. Pour tous les élèves de moins de 12 ans, cet isolement est immédiat et pour tous les élèves de plus de 12 ans, la nécessité d'un isolement immédiat est déterminée en fonction du statut vaccinal du cas contact à risque élevé.

Le nombre de cas positifs et cas contact à risque élevé identifiés dans le cadre des fiches « note d'information COVID 19 positif ou situation complexe » ainsi que l'établissement scolaire correspondant et la date de création de la fiche sont notamment retranscrits dans l'outil dédié « CONFLUENCE ».

Cet outil, proposé par le rectorat d'Orléans-Tours au vu des besoins sur le territoire, se présente comme un espace collaboratif nécessaire à la remontée du nombre de cas positifs et cas contact dans plusieurs départements appartenant à l'académie d'Orléans-Tours et assurer un suivi des situations sanitaires.
Cet outil a été proposé à l'ensemble des départements de l'académie. Au jour du contrôle, seuls certains départements ont choisi d'utiliser cette solution.

Le rectorat d'Orléans-Tours est chargé d'assurer le remplacement des agents des établissements du second degré testés positif au COVID.

La DSDEN du Loiret est chargée d'assurer le remplacement des agents des établissements du premier degré testés positifs au COVID. La procédure de prise en charge est similaire à la procédure de gestion habituelle d'un arrêt maladie.

Constatations

[redacted]

A notre demande, [redacted] se connecte à la boite aux lettres électronique dédiée à la réception des signalements [redacted] et documente sa progression à l'aide de captures d'écrans. Sommes informés qu'il ne s'agit pas d'une MSS. Constatons que cette boite aux lettres électronique contient des messages comportant en pièce jointe [redacted]

[redacted]

[redacted] ainsi que des fiches FT19 contenant l'identité d'un élève positif au COVID et la liste de ses cas contact. Sommes informés que ces fiches sont transmises par les chefs d'établissement [redacted] prend copie de messages électroniques contenant [redacted] ainsi que des fiches FT19.

Constatons qu'un courriel contenant une fiche d'identification d'élève positif au COVID ou une fiche FT19 date du 05 octobre 2020. Constatons qu'un dossier de la boite aux lettres électronique contient 65 courriels contenant une fiche d'identification d'élève positif au COVID ou une fiche FT19 reçus entre le 21 septembre 2020 et le 16 octobre 2020.

Sommes informés, qu'aucune durée de conservation de ces courriels n'a été définie. Aucune procédure de suppression n'a été mise en œuvre.

Sommes informés que les fiches d'identification d'élèves positifs au COVID ainsi que les fiches FT19 sont systématiquement imprimées et conservées dans une armoire au sein de la DSDEN. Aucune durée de conservation de ces fiches n'a été définie. Aucune procédure de suppression n'a été mise en œuvre.

Sommes informés par le médecin conseiller technique de la Rectrice que le MEN n'a pas communiqué au rectorat de l'académie d'Orléans-Tours de consignes relatives à la durée de conservation de ces fiches ni à une éventuelle procédure de suppression de celles-ci.

Sommes informés que l'ensemble des fiches créées depuis le début de la crise sanitaire a été conservé. Constatons la présence d'une fiche d'identification au format papier d'un élève positif en date du 20 novembre 2020.

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) l'organigramme du rectorat de l'académie d'Orléans Tours,
2) tout document relatif à la gestion des élèves testés positifs au COVID ;
3) les fiches du registre des activités de traitement liées à la gestion des élèves testés positifs au COVID et leurs cas contact ;
4) l'éventuelle analyse d'impact à la protection des données (AIPD) ou, le cas échéant, les raisons ayant conduit à ne pas en faire ;
5) le registre des violations de données à caractère personnel et, le cas échéant, la procédure de gestion associée ;
6) tous les éléments d'information à destination des personnes dont les données sont traitées dans le cadre de la gestion des élèves testés positifs au COVID et leurs cas contact (notice d'information, affiche, information présente sur le site web);
7) le cas échéant, la procédure d'exercice des droits des personnes dont les données sont traitées dans le cadre de la gestion des élèves testés positifs au COVID et leurs cas contact ;
8) le cas échéant, les des dix dernières demandes d'exercice des droits des personnes dont les données sont traitées dans le cadre de la gestion des élèves testés positifs au COVID et leurs cas contact et les réponses qui leur ont apportées par le rectorat de l'académie d'Orléans Tours ;

[redacted] [redacted]

[redacted]

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 18h30.

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

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

Mentionnons que [redacted] médecin expert, a pris copie des éléments nécessaires à l'élaboration de son rapport ; que ces documents lui ont été communiqués sans que les membres de la délégation en aient pris copie ; que les pièces numériques ainsi communiquées ont été stockées, par [redacted] sur un support chiffré dont il est le seul à avoir connaissance du mot de passe.

[redacted]

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

[redacted]

Contrôle effectué le 23 Novembre 2021 à la DASEN 45000 ORLEANS, numéro de décision 2020-091C en date du 22 mai 2020.

Par une convention conclue en date du 15 Mars 2021, j'ai été désignée par la Présidente de la Commission Nationale de l'informatique et des libertés afin d'accompagner une délégation afin de participer à la mission d'expertise auprès de la DASEN qui s'est déroulée le 23 Novembre 2021.

Cette mission de contrôle a été effectuée en application de la décision de contrôle de la CNIL n° 2020-091C en date du 22 mai 2020 et pour lequel j'ai été désignée par un ordre de mission en date du 15 mars 2021.

1.Constats effectués sur place :

[redacted]

- ✓ La copie d'écran d'un mail électronique de [redacted] provenant de l'ARS/CPAM, en date du 28 septembre 2020, transféré à la cellule COVID45@ac-orleans-tours.fr comprend dans le corps du message 5 résumés de situation d'établissements scolaires ne comportant pas d'identification des élèves mais les initiales des noms et prénoms des élèves COVID positifs. Les 5 dossiers joints sont les fiches PATIENT extraites du logiciel CONTACT COVID comprenant l'intégralité des données des élèves COVID.

- [redacted]

[redacted]

[redacted]

Contrôle effectué le 17 mars à l'ARS Centre Val de Loire 45000 ORLEANS, numéro de décision 2020-091 C en date du 22 mai 2020

Par une convention conclue en date du 15 mars 2021, j'ai été désignée par la Présidente de la Commission nationale de l'informatique et des libertés afin d'accompagner une délégation de la CNIL afin de participer à la mission d'expertise auprès de L'ARS Centre Val de Loire qui s'est déroulée le 17 Mars 2021. Cette mission de contrôle a été effectuée en application de la décision de contrôle de la CNIL n° 2020-091C en date du 22 mai 2020 et pour lequel j'ai été désignée par un ordre de mission en date du 15 Mars 2021.

1. **Constats effectués sur place**

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

2. **Conclusion**

Il n'a pas été constaté de manquement sur les différents documents analysés concernant les données nominatives.

Des données nominatives ont été transmises d'une adresse non sécurisée, « Direction de la prévention de la santé et de l'environnement du travail du conseil régional du centre val de Loire » à l'ARS.

L'archivage des données ne correspond pas au 45 jours affichés du Logiciel SORMAS.

4 fiches issues de CONTACT COVID comprises entre le 4 novembre et le 14 novembre 2020 ne sont pas archivées.

[redacted]

[redacted]
EXPERT PRES LA COUR D'APPEL DE BORDEAUX
ATTESTATION D'ÉTUDE RÉPARATION JURIDIQUE DU DOMMAGE CORPOREL
D.I.U. APTITUDE À L'EXPERTISE MÉDICALE
D.I.U. NATIONAL D'EXPERTISES EN ACCIDENTS MÉDICAUX

[redacted]

Bordeaux, le 04 janvier 2021

Mandant : Mme Marie-Laure DENIS Présidente de la Commission Nationale de l'Informatique et des Libertés

Références Affaire :

- **Décision n° 2020-091C**
- **CNIL/ARS Aquitaine**
- **Le 4 février 2021 ARS Aquitaine 103 bis rue Belleville - CS 91704 - 33063 Bordeaux Cedex**

Rapport d'expertise dans le cadre de sa mission de contrôle portant sur le dispositif dénommé « Contact-covid » auprès de l'Agence régionale de santé Nouvelle aquitaine le jeudi 4 février 2021

Étaient présents :

Pour la CNIL :

[redacted]ntrôles

Pour l'ARS AQUITAINE :

[redacted]Gironde
[redacted]nitaire

MISSION

En application de l'article 68 de la loi informatique et libertés, un rapport d'expertise doit être établi. L'objectif de ce rapport est de dresser une synthèse des opérations d'expertise effectuées et d'apporter, tout élément de nature à éclairer la CNIL, sur les suites à donner à la mission de vérification. Dans le cas de la désignation d'un médecin, ce rapport ne doit pas faire état de données médicales individuelles.

Par une convention conclue en date du 15 janvier 2020, j'ai été désignée par la Présidente de la Commission nationale de l'informatique et des libertés afin d'accompagner une délégation de la CNIL afin de participer en date du 4 février 2021 auprès de l'ARS d'Aquitaine. Cette mission de contrôle a été effectuée en application de la décision de contrôle de la CNIL n° 2020-091C en date du 22 mai 2020 et pour lequel j'ai été désigné par un ordre de mission en date du 21 janvier 2020.

Il conviendra de relater de manière factuelle les vérifications ainsi que les opérations d'expertise menées, en se fondant si nécessaire sur les pièces obtenues à l'occasion de la procédure.

Cette conclusion a pour objet de donner une impression générale de la mission de contrôle et de mentionner, le cas échéant, les points concernant des manquements à la loi « Informatique et Libertés » et/ou à tout autre règlementation et si nécessaire, suggérer les mesures correctives pouvant être mis en place.

Il s'agit pour l'expert, s'il estime utile, de faire état de toute appréciation sur les faits constatés, en précisant que la CNIL n'est pas liée par celle-ci.

Certifie avoir rempli en Honneur et Conscience ma mission et présenter ci-dessous le résultat de mes constatations médico-légales.

CONTEXTE

Dans le cadre de la lutte contre l'épidémie de covid-19, le Gouvernement a mis en place 2 fichiers : SI-DEP (création du système d'information national de dépistage) et Contact Covid (l'adaptation du système d'information « amelipro » pour tracer les contacts), auxquels s'ajoute le déploiement de l'application mobile StopCovid.

La mise en œuvre du traitement « Contact-covid » a été autorisée par décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions. Ce décret prévoit la création de « SI-DEP » et « Contact Covid ». (Lien du décret : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000041869923).

Le 8 mai 2020, la CNIL s'était prononcée en urgence sur le projet de décret encadrant les conditions de mise en œuvre des fichiers SI-DEP et Contact Covid.

Enfin, le décret n° 2020-650 du 29 mai 2020 autorisant l'application Stop Covid prévoit en son article 6 que l'article 9 du décret du 12 mai 2020 (concernant la liste des catégories contenues dans le traitement SI-DEP) soit complété par un QR-code.

TRAITEMENT ET RESPONSABLE DE TRAITEMENT

Le traitement « Contact-Covid » a pour finalité l'identification, des personnes infectées, des personnes présentant un risque d'infection, l'orientation des personnes infectées, et des personnes susceptibles de l'être, et enfin la surveillance épidémiologique et la recherche sur le virus et les moyens de lutter contre sa propagation.

La multitude des catégories de données comprises dans ce traitement, visées à l'article 2 du décret du 12 mai 2020, sont collectées :
auprès d'un « patient zéro » ou de la personne évaluée comme contact à risque de contamination, lorsque ces derniers les ont communiquées,
par l'intermédiaire du traitement autorisé « SI-DEP »
par l'intermédiaire des agents habilités de l'assurance maladie « AM ».

Le responsable de ce traitement est la caisse nationale de l'assurance maladie (« CNAM »).

Elle a le statut juridique d'établissement public national à caractère administratif et agit sous la double tutelle du ministère des Solidarités et de la santé (« MSS ») et du ministère de l'Économie et des finances.

Le réseau de la CNAM se compose notamment des caisses primaires d'assurance maladie (« CPAM »).

LES DONNÉES COLLECTÉES

1. Les données d'identification (noms, prénoms, date de naissance, sexe) de la personne et de ses éventuels représentants légaux et NIR ;
2. Les coordonnées de contact (adresse de résidence, le numéro de téléphone et l'adresse électronique) ;
3. La désignation de l'organisme d'affiliation assurant la prise en charge des frais de santé ;
4. Les coordonnées et la spécialité du médecin à l'origine de l'inscription dans le traitement de données ;
5. Les données permettant de déterminer que la personne est infectée (caractère positif du test, date de prélèvement ou, pour patient hospitalisé, l'existence de symptômes associés à un scanner) ;
6. Le cas échéant, l'existence de symptômes et la date de leur apparition ;
7. Les données relatives à la situation de la personne au moment du dépistage (hospitalisé, à domicile ou déjà à l'isolement) ;
8. La déclaration d'un besoin d'accompagnement social et d'appui à l'isolement et le consentement de la personne à la communication de son identité et de ses coordonnées à l'organisme compétent en vue d'organiser cet accompagnement ;
9. La mention de la profession et du lieu d'exercice professionnel ;
10. Le cas échéant, les départements, collectivités autres que ceux de résidence, dans lesquels la personne s'est rendue dans les quatorze derniers jours ainsi que la date de son retour en France lorsqu'elle a séjourné à l'étranger ;
11. Le cas échéant, la fréquentation dans les quatorze derniers jours des structures suivantes, ainsi que leurs coordonnées : structures ou lieux d'hébergement collectif (foyer, pensionnat, établissement d'hébergement pour personnes âgées dépendantes, établissement médico-social accompagnant des personnes handicapées, établissements pénitentiaires, structure d'hébergement touristique) ; structures d'accueil du jeune enfant ; milieu scolaire ; milieu

universitaire ; établissements de santé ; autres établissements recevant du public dans lesquels les gestes barrières ne peuvent être pleinement respectés ;
12. Le cas échéant, la participation, dans les quatorze derniers jours, à un rassemblement de plus de dix personnes (localisation, date et objet du rassemblement : événement sportif ; événement culturel ; réunion familiale, rassemblement festif ; rassemblement pour raison professionnelle ; autre type de rassemblement) ;
13. La mention d'une identification dans le traitement comme ancien cas contact ;
14. Les données d'identification et les coordonnées des personnes évaluées comme contacts à risque de contamination (nom, prénom, sexe, date de naissance, numéro de téléphone, adresse électronique) ;
15. Le cas échéant, le consentement du patient zéro à la divulgation de son identité à chaque personne évaluée comme étant un contact à risque de contamination ;
16. Les dates et heures de création, modification, traitement de la fiche et des contacts ;
17. Le cas échéant, la mention que la personne était en quarantaine au cours des quatorze derniers jours et les raisons de cette quarantaine (personne identifiée comme cas contact à risque de contamination à la covid-19 ; personne ayant dans son entourage une personne dépistée positive à la covid-19 ; personne présentant des symptômes de contamination à la covid-19 ; personne ayant dans son entourage une personne présentant des symptômes de contamination à la covid-19) ;
18. Le cas échéant, l'information selon laquelle la personne a eu un contact avec une personne infectée ou présentant les symptômes d'infection à la covid-19 au cours des quatorze derniers jours ;
19. Le cas échéant, la mention que la personne a été dépistée dans le cadre d'une campagne de dépistage organisée par une agence régionale de santé ;

PERSONNES HABILITÉES À ACCÉDER AUX DONNÉES SUR « CONTACT-COVID »

1. Au sein de la plateforme « Contact-Covid », peuvent enregistrer et consulter les données susmentionnées dans la limite de leurs besoins respectifs d'en connaître :

- les agents spécialement habilités de l'AM, de la caisse nationale militaire de sécurité sociale ainsi des autres organismes de protection sociale ;
- les agents spécialement habilités des agences régionales de santé (« ARS ») ainsi que de leurs sous-traitants mentionnés ;
- Les professionnels de santé et personnels spécialement habilités du service de santé des armées ;
- Les personnels spécialement habilités des communautés professionnelles territoriales de santé, des maisons de santé, des centres de santé ou structures créées pour lutter contre le covid-19, des organismes de protection sociale à qui l'assurance maladie, par convention, délègue, les missions dévolues aux agents des organismes locaux d'assurance maladie ;
- Les professionnels de santé et personnels spécialement habilités des établissements de santé ;
- Les médecins libéraux ou les personnes placées sous leur autorité.

2. Enfin, sont seulement destinataires des données relatives aux personnes infectées et aux personnes ayant été en contact avec ces personnes, ayant fait l'objet de mesures adéquates de pseudonymisation, et dans la limite des finalités décrites à l'article 3 du décret du 12 mai 2020 :

- L'Agence nationale de santé publique (« ANSP ») ;
- La direction de la recherche, des études, de l'évaluation et des statistiques du MSS ;
- La Plateforme des données de santé[3] (anciennement dénommée INDS) ;
- La CNAM ;
- Le service de santé des armées.

CONSTATATIONS

Quatre documents comprenant des données médicales m'ont été confiés pour analyse et conservation via une clé USB chiffrée :

[redacted]

1- [redacted] :

[redacted]

Il n'a pas été constaté dans ce document de manquement aux règles de collecte des données précédemment énoncées.

2- [redacted] :

[redacted].

[redacted]

Il n'a pas été constaté dans ce document de manquement aux règles de collecte des données précédemment énoncées.

3- [redacted] :

[redacted]

Il n'a pas été constaté dans ce document de manquement aux règles de collecte des données précédemment énoncées.

4- [redacted] :

[redacted]

Il n'a pas été constaté dans ce document de manquement aux règles de collecte des données précédemment énoncées.

CONCLUSION

Aucun manquement aux règles de collecte des données médicales n'a été constaté dans l'ensemble des documents portés à ma connaissance à ce jour.

LISTE DES ANNEXES

Annexe 1 : Décision n°2020-091C 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
Annexe 2 : Ordre de mission
Annexe 3 : Convention d'exercice d'une activité d'expert auprès de la Commission Nationale de l'Informatique et des Libertés

Annexe 1 : Décision n°2020-091C 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

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

La Présidente

Le 22 mai 2020

Décision n° 2020-091C 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 « Contact Covid », résultant de l'adaptation du système d'information « amelipro » 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 la caisse nationale de l'assurance maladie 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

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 – 75334 PARIS CEDEX 07 – 01 53 73 22 22 – www.cnil.fr

Annexe 2 : Ordre de mission

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Le 21/01/2021

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 6 novembre 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-2020-003 du 10 novembre 2020 habilitant des agents de la CNIL à procéder à des missions de vérification ;

[redacted]

Le secrétaire général

[redacted]

RÉPUBLIQUE FRANÇAISE

3 Place de Fontenoy, TSA 80715 - 75334 PARIS CEDEX 07 - 01 53 73 22 22 - www.cnil.fr

Les données personnelles nécessaires à l'accomplissement des missions de la CNIL sont traitées dans des fichiers destinés à son usage exclusif.
Les personnes concernées peuvent exercer leurs droits Informatique et Libertés en s'adressant au délégué à la protection des données (DPO) de la CNIL via un formulaire en ligne ou par courrier postal. Pour en savoir plus : www.cnil.fr/donnees-personnelles

Annexe 3 : Convention d'exercice d'une activité d'expert auprès de la Commission Nationale de l'Informatique et des Libertés

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Convention d'exercice d'une activité d'expert auprès de la Commission Nationale de l'Informatique et des Libertés

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

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 l'attestation sur l'honneur [redacted] en date du 15 janvier 2021,

Il est convenu ce qui suit entre les soussignés :

La Présidente de la Commission Nationale de l'Informatique et des Libertés,

Et :

[redacted]

Dénommée ci-après l'expert

Article 1er – Conformément à l'article 35 du décret n° 2019-536 du 29 mai 2019 susvisé, l'expert est désigné par la CNIL pour les vérifications décidées par la Présidente dans ses décisions n°2020-091C, 2020-092C et 2020-097C des 22 et 28 mai 2020.

L'expert participe aux missions de la Commission pour lesquelles il est mandaté. Les opérations d'expertises sont menées contradictoirement et un rapport d'expertise est remis à la présidente de la Commission.

Article 2 – L'expert consigne dans son rapport les vérifications qu'il a faites, sans faire état, en aucune manière, des données médicales individuelles auxquelles il a eu accès.

Article 3 – L'expert perçoit une indemnité forfaitaire de 800 € bruts par journée d'exercice de son activité auprès de la CNIL. Cette somme inclut la participation à la mission de contrôle ainsi que la rédaction du rapport d'expertise. Cette somme n'inclut pas les frais de déplacement et de restauration. Les conditions et frais occasionnés par les déplacements de l'expert sont déterminés selon l'arrêté du 8 avril 2016 pris en application du décret 2006-781 du 3 juillet 2006.

Fait à Paris, le 15 janvier 2021

en double exemplaire

L'expert,

[redacted]

La Présidente,

[redacted]

Marie-Laure DENIS

Par délégation de la Présidente

[redacted]

RAPPORT DU [redacted]

1. Rappel du contexte de la mission

Par une convention conclue en date du 23 septembre 2020, j'ai été désignée par la Présidente de la Commission Nationale de l'Informatique et des Libertés pour accompagner une délégation de la CNIL auprès de l'Agence Régionale de Santé Grand-Est qui s'est déroulée le 14 octobre 2020, 3 boulevard Joffre à Nancy – 54000. Cette mission de contrôle a été effectuée en application de la décision de contrôle de la CNIL n° 2020-091C en date du 22 mai 2020 et pour laquelle il m'est demandée de consigner les vérifications que j'ai faites sans faire état de données médicales individuelles.

2. Constats effectués dans les locaux de l'ARS Grand Est (GE)

La matinée a été consacrée à une présentation du fonctionnement général de l'ARS GE par [redacted], puis à des échanges d'information sur les modalités d'organisation et de recueil du dispositif « Contact-Covid » entre les 4 représentants de la mission CNIL et ceux de l'ARS sous la [redacted]

L'après-midi, les membres de la mission CNIL, [redacted] assisté à la fin d'un échange téléphonique mené par [redacted] collaboratrice du [redacted] de la cellule veille sanitaire en charge de recueillir les informations de niveau 3 des cas index Covid et de leur contact.

A la demande de [redacted] Y nous a ensuite présenté les différents fichiers d'exploitation du recueil des informations concernant les cas zéro et les contacts Covid et a procédé à différentes copies d'écran qui m'ont été transmises sur une clé USB verrouillée avec un mot de passe strictement personnel préalablement configuré avec l'assistance de [redacted]

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

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

3. Conclusions

Au terme de ma participation à cette journée de présentation, d'échanges et de transmission d'informations puis à la lecture des différents documents qui m'ont été communiqués, j'ai pu constater que les conditions de recueil et de communication des données personnelles (nom, prénom, date de naissance, sexe, NIR) et des données de santé concernant les cas index et les contacts COVID étaient globalement respectées par l'assurance maladie l'ARS GE ainsi que l'exercice du droit d'opposition de communication de données nominatives du cas zéro auprès de ses contacts de même que l'identification d'au moins un représentant légal lors de cas survenu en lycée. Lors de la transmission de données entre les représentants de l'ARS et l'Assurance Maladie figurait bien l'identification des personnes habilitées à saisir les données, néanmoins lorsqu'il s'agissait de représentants de la société BIOSERENETY, société avec laquelle l'ARS a sous-traité suite à un contrat une partie du recueil des informations concernant le tracing des cas contact, l'identité nominative du « pilote » recueillant les données n'était pas saisie.

Nous n'avons pas recueilli de fichiers concernant des cas survenus en EHPAD et à posteriori je m'interroge sur le fait de savoir si comme dans les lycées dans le fichier de recueil le nom d'un représentant légal figure bien lors de contact Covid chez des personnes âgées placées en tutelle ou curatelle suite à des troubles mnésiques type maladie d'Alzheimer.

Nancy, le 21 octobre 2020

[redacted]

Rapport du [redacted]

1. Rappel du contexte

Par une convention conclue en date du 17.11.2020, j'ai été désignée par la Présidente de la Commission nationale de l'informatique et des libertés afin d'accompagner une délégation de la CNIL composée de [redacted] service des contrôles. Cette mission s'est déroulée en date du 17.11.2020 auprès de Caisse Primaire d'Assurance Maladie de Côte d'Or dans le cadre de l'application «CONTACT-COVID ». De plus, cette mission de contrôle a été effectuée en application de la décision de contrôle de la CNIL n° 2020-091C en date du 22 mai 2020 et pour lequel j'ai été désigné par un ordre de mission en date du 17.11.2020.

2. Constats effectués sur place

Dans le cadre de la mission trois observations peuvent être faites :
1. Dans le cadre des comptes utilisateur et administrateur il a été mis en évidence un certain nombre de comptes personnelles de type #orange.fr#. Ce point devra être investigué pour mieux appréhender l'utilisation de messagerie personnelle plutôt que professionnelle.
2. Une attention toute particulière a été portée par la délégation de la CNIL sur la destruction des données au-delà du 3ème mois. Nous avons pu mettre en évidence la persistance de certains dossiers mais l'analyse soigneuse de ces derniers nous a permis d'établir des modifications de statuts qui expliquent ces persistances ; Pour exemple certains patients étaient classés P0 durant la première vague de COVID et deviennent des patients contacts sur une seconde période. Il nous a été clairement expliqué que si le patient était déjà créé il existait une continuité dans le cadre du suivi informatique de l'application. En conséquence le chainage devrait être un point de vigilance.
3. Concernant les données à caractère personnel il faut souligner que dans tous les exemples qui nous ont été présentés il existait une stricte application du protocole. Ce protocole de saisie informatique a une caractéristique tout à fait particulière de ne permettre aucun champ libre ni de fichiers associés.

4. Conclusion

Dns le cadre de cette mission on peut souligner l'excellente coopération des acteurs de la CPAM de Côte d'Or et que d'un point de vue médical aucun manquement à la loi « Informatique et Libertés » n'a été observé.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
La Présidente

CAISSE NATIONALE DE L'ASSURANCE MALADIE
Monsieur le Directeur Général
26 avenue du professeur André Lemierre
75020 PARIS

Paris, le 11 SEP. 2020

N/Réf. : [redacted]CS201028
LRAR n° 2C 1410021596 7
À rappeler dans toute correspondance

Monsieur le directeur général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué plusieurs contrôles auprès de la Caisse nationale d'assurance maladie (ci-après « CNAM ») qui se sont déroulés entre le 25 mai et le 16 juin 2020.

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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 le 22 juin 2020 dans les locaux de la Caisse primaire d'assurance maladie de Seine Saint-Denis situés 2 avenue de la Convention à Bobigny (93000), le 3 juillet 2020, dans les locaux de la fondation hôpital Saint-Joseph, situés 185 rue Raymond Losserand à PARIS (75014) et le 22 juillet 2020, dans les locaux de l'agence régionale de santé (« ARS ») Île-de-France situés Millénaire 2, 35 rue de la gare à Paris (75019).

A ce stade, les constatations effectuées lors des investigations menées me conduisent à vous faire part des observations suivantes.

En premier lieu, la délégation a constaté que les médecins de la fondation hôpital Saint-Joseph, ne disposant pas d'accès à l'application « CONTACT COVID », ont reçu de la part de la CNAM la consigne de transmettre l'identité des « patients zéros » à la CPAM de Paris par l'intermédiaire de fichiers Excel envoyés par la messagerie sécurisée de santé (fiche de transmission FT 19. A cet égard, l'absence de mécanisme de gestion du cycle de vie des données au sein des fichiers Excel (notamment de purge) et la dispersion de ces fichiers dans les messageries ne permet pas de garantir l'effectivité des durées de conservation.

Or, je vous rappelle les dispositions de l'article 5, §1, e) du règlement précité qui prévoient que les données à caractère personnel doivent être conservées pendant une durée « *n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ». À cet égard, le décret n° 2020- 551 du 12 mai 2020 dispose que « *les données à caractère personnel contenues dans le traitement "Contact Covid" ne peuvent être conservées à l'issue d'une durée de trois mois après leur collecte* ».

Par conséquent, je vous prie de bien vouloir mettre en œuvre un mécanisme d'échange des données à caractère personnel entre les utilisateurs de l'application « CONTACT COVID » garantissant une durée de conservation des données relatives aux personnes concernées qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées. Le mécanisme devant être privilégié consiste à créer pour ces structures un accès à l'application CONTACT-COVID. D'après les informations dont je dispose, cette solution est en cours de déploiement.

En deuxième lieu, la délégation a été informée qu'aucun support d'information à destination des « patients zéros » n'a été transmis par la CNAM à [redacted] De plus, la délégation a constaté que ces patients ne sont pas informés par [redacted] du traitement qui est opéré sur leurs données et des droits qu'ils détiennent à cet égard.

Or, en application des articles 12, 13 et 14 du règlement précité, il vous appartient, en tant que responsable du traitement, de vous assurer, dans toute la mesure du possible, que, dans les lieux où le traitement est opéré, une information concise, transparente, compréhensible et aisément accessible est délivrée aux personnes concernées. La CNIL recommande que certaines informations essentielles soient délivrées aux personnes au moment de la collecte et notamment, l'identité et les coordonnées du responsable de traitement, la finalité poursuivie par le traitement, la base légale du traitement de données, le caractère obligatoire ou facultatif du recueil des données, les destinataires ou catégories de destinataires des données, la durée de conservation des données et les droits des personnes concernées.

Dès lors, je vous prie de bien vouloir prendre des mesures afin d'assurer que cette information soit effectivement délivrée aux personnes dont les données sont traitées, conformément aux exigences des articles 12, 13 et 14 du RGPD.

En troisième lieu, la délégation a été informée que les données des « cas contacts » ayant refusé de participer au traitement sont immédiatement supprimées. Cependant, ce mécanisme de suppression a été développé après la mise en production du traitement. Or, les données collectées entre le début du traitement et la mise en œuvre de la fonctionnalité de suppression n'ont pas été purgées.

Je tiens à vous rappeler qu'en application des dispositions de l'article 17, a) du règlement précité, « *la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque [...] les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière* ».

Dès lors, je vous prie de bien vouloir procéder à la suppression des données des « cas contacts » ayant refusé de participer au traitement, encore présentes en base de données.

En quatrième lieu, la délégation a constaté que la CPAM de Seine-Saint-Denis transmet à l'ARS Île-de-France par courriel non chiffré la liste des noms et dates de naissance des « patients zéros »

relevant du niveau 3 du traitement. De plus, afin d'accéder à l'application « CONTACT COVID », les agents de l'ARS Île-de-France disposent de comptes non nominatifs fournis par la CNAM. Ces comptes non nominatifs sont partagés par plusieurs agents de l'ARS. Enfin, la délégation a été informée que le portail de connexion à destination des utilisateurs ne disposant pas d'un compte « AMELI PRO » ne met pas en œuvre une authentification forte.

Or, 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, pour satisfaire aux exigences de l'article 32 précité, il conviendra de mettre en œuvre un mécanisme d'authentification forte pour l'accès au portail de connexion à destination des utilisateurs ne disposant pas d'un compte « AMELI PRO ». Il conviendra également de fournir un compte nominatif à chaque utilisateur de l'application « CONTACT COVID ». Enfin, je vous prie de bien vouloir mettre en œuvre un mécanisme d'échange des données à caractère personnel entre les utilisateurs de l'application « CONTACT COVID » garantissant la confidentialité des données.

Par ailleurs, je relève que la délégation a constaté que le champ « adresse » présent dans les fiches des « patients zéros » et des « cas contact » au sein du téléservice « CONTACT COVID » est parfois utilisé afin d'y inscrire différentes informations tels que le suivi de l'envoi de SMS, un numéro de téléphone secondaire ou encore l'opposition d'un « patient zéro » à la divulgation de son identité aux « cas contact ».

Je vous alerte sur le fait qu'une telle pratique des risques en matière de sécurité des données. En effet, si dans le futur l'application concernée était utilisée dans le but d'effectuer un publipostage, l'ensemble des informations se retrouvant dans la « zone adresse » se retrouveraient dans le pavé adresse du courrier et seraient potentiellement accessibles à toute personne par lequel le courrier transiterait.

Là encore, une telle modalité de traitement ne satisfait pas aux exigences de l'article 32 du RGPD précité.

Je vous invite dès lors à mettre en place des menus déroulants afin de renseigner les informations nécessaires au traitement en question, dans le respect des catégories de données listées par le décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions.

Enfin, nous avons constaté que vous avez mis en place une procédure spécifique pour les enquêtes menées lorsque le « patient zéro » est un mineur, ce qui est tout à fait pertinent. J'attire votre attention sur la spécificité de la situation des majeurs protégés et vous invite à sensibiliser les personnes réalisant les enquêtes sur ce point.

En conclusion, il ressort de l'ensemble des éléments précités que les investigations menées par la CNIL font état de plusieurs manquements aux obligations issues du RGPD. L'avis rendu par le collège de la Commission jeudi 10 septembre, en application de l'article 11 de la loi n° 2020-546 du 11 mai 2020, en fait état.

Je tiens à vous assurer que je suis consciente des contraintes opérationnelles rencontrées par vos services lors de la mise en place de ce traitement, notamment en raison du grand nombre d'acteurs concernés et de la crise sanitaire, et du fait que les différents contrôles réalisés ont permis d'établir l'existence d'un processus d'amélioration continu du système

Au demeurant, je tiens à souligner l'entière coopération et l'effort de transparence des personnes rencontrées au sein de vos services, lesquels ont permis la réalisation de ces contrôles dans de bonnes conditions, malgré la crise sanitaire.

Je vous demande de prendre des mesures pour mettre fin aux irrégularités constatées et d'en informer la CNIL. A défaut, ainsi que le rappelle l'avis du 10 septembre dernier, la CNIL pourrait adopter une mesure correctrice contraignante prévue par le RGPD et la loi « Informatique et libertés ».

[redacted]

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

M.-L. D.

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS
La Présidente

AGENCE RÉGIONALE DE SANTÉ ÎLE-DE-FRANCE
Monsieur le Directeur Général
Millénaire 2, 35 rue de la Gare
75019 PARIS

Paris, le 11 SEP. 2020

N/Réf. : MLD/[redacted]/CS201029
LRAR n° 2C 141 002 15 97 4
À rappeler dans toute correspondance

Monsieur le directeur général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, le 22 juillet 2020, un contrôle sur place dans les locaux de l'agence régionale de santé Île-de-France (ci-après « ARS IDF ») situés Millénaire 2, 35 rue de la Gare à Paris (75019).

Ce contrôle avait 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 « CONTACT-COVID », résultant de l'adaptation du système d'information « amelipro » 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 la Caisse nationale de l'assurance maladie et de tout traitement lié.

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 par l'ARS IDF le 28 juillet 2020 et par le ministère des Solidarités et de la Santé le 28 août 2020, me conduisent d'ores et déjà à vous faire part des observations suivantes.

À titre liminaire, il résulte des vérifications opérées que conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et à l'article 1er du décret n°2020-551 du 12 mai 2020 pris pour son application, la Caisse nationale de l'assurance maladie est responsable du traitement de données à caractère personnel dénommé « CONTACT-COVID ».

Pour autant, ainsi qu'il nous a été précisé lors du contrôle du 22 juillet 2020 par l'ARS IDF, chaque agence régionale de santé (ci-après « ARS ») est responsable des traitements des données qu'elle collecte, traite, gère et met en œuvre dans le cadre du « *tracing* » de niveau 3 du traitement « CONTACT COVID » et de tous traitements liés.

A cet égard, les constatations effectuées lors des contrôles de la CNIL appellent de ma part les observations suivantes.

En premier lieu, la délégation a été informée que l'ARS IDF n'a formalisé aucune procédure d'exercice des droits des personnes concernant les traitements mis en œuvre dans le cadre du « tracing » de niveau 3.

Or, l'article 12 du règlement précité dispose que « *le responsable du traitement prend des mesures appropriées (...) pour procéder à toute communication au titre des articles 15 à 22 (...) en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ». De même, en application des dispositions de l'article 24 du RGPD, « *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ». À cet égard,

Par conséquent, je vous prie de bien vouloir définir et mettre en œuvre une procédure d'exercice des droits des personnes dont vous traitez les données dans le cadre du « tracing » de niveau 3 du traitement « CONTACT COVID » et de tous traitements liés. En particulier, je vous invite à donner à ces personnes les moyens d'exercer effectivement leurs droits (accès, rectification, opposition, effacement, portabilité et limitation du traitement) et prévoir le cas échéant, dans vos systèmes d'information, les outils techniques qui permettront la bonne prise en compte de leurs droits.

En second lieu, la délégation a été informée que le fichier Excel contenant l'identité du patient zéro envoyé par l'ARS IDF au médecin référent de la collectivité est chiffré par l'intermédiaire de la solution « Zed! ». Or, la délégation a constaté que les mots de passe de ces archives chiffrées sont adressés au médecin par le même canal de transmission.

Or, de telles configurations, à savoir l'envoi d'une archive chiffrée et le mot de passe permettant le déchiffrement de celle-ci par le même canal d'envoi, ne permettent 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, pour satisfaire aux exigences de l'article 32 précité, je vous prie de bien vouloir mettre en œuvre un mécanisme d'échange des données à caractère personnel entre les utilisateurs de l'application « CONTACT COVID » garantissant la confidentialité des données. Ainsi, je vous recommande que, dès lors qu'il y a transmission d'éléments relatifs à des patients à un professionnel de santé, cette transmission doit s'effectuer de manière chiffrée et la communication du mot de passe permettant le déchiffrement des données doit s'effectuer par un autre canal (par exemple par téléphone lorsque le fichier est envoyé par courriel).

Enfin, la délégation a été informée que dans le cadre de l'activité de « *tracing* », les agents enquêteurs de l'ARS IDF peuvent contacter le patient zéro, le médecin du travail ou le service de médecine préventive du patient zéro ou des « cas contact ». Cependant, en l'absence de médecin du travail, la délégation a constaté que les agents enquêteurs ont été amenés à contacter directement la

structure qui héberge le patient zéro préalablement identifié. Or, il ressort des constations que, au moins dans un cas, l'identité et le statut médical d'un patient zéro ont été communiqués à un responsable d'une collectivité (en l'espèce un foyer d'hébergement) par l'ARS IDF, sans que le consentement de ce patient n'ait été obtenu.

Or, d'une part, en application de l'article 9 du RGPD, le traitement des données à caractère personnel concernant la santé est interdit à moins que la personne concernée n'ait donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques.

D'autre part, l'article 3 du décret n°2020-551 du 12 mai 2020 encadre strictement les conditions dans lesquelles les données du patient zéro ou d'un « cas contact » peuvent être communiquées et aucune ne répond au cas de figure évoqué ci-dessus.

Dès lors, je vous prie de bien vouloir veiller à ce que les ARS ne transmettent des données de santé d'un patient zéro ou des personnes évaluées comme contact à risque de contamination qu'aux seules personnes autorisées par le décret 2020-551 du 12 mai 2020. À défaut, en l'absence de recueil du consentement exprès de la personne concernée à la divulgation de ses données de santé, un manquement pourra être retenu en application de l'article 9 du RGPD.

[redacted]

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

M-L. De

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La présidente

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

Paris, le 11 SEP. 2020

N/Réf. : [redacted]**CS201030**
LRAR n° 2C 141 002 1595 0
À rappeler dans toute correspondance

Monsieur le Ministre,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, le 22 juillet 2020, un contrôle sur place dans les locaux de l'agence régionale de santé Île-de-France (ci-après « ARS IDF ») situés Millénaire 2, 35 rue de la Gare à Paris (75019).

Ce contrôle avait 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 « **CONTACT-COVID** », résultant de l'adaptation du système d'information « amelipro » 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.

À titre liminaire, il résulte des vérifications opérées que conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et à l'article 1 du décret n° 2020-551 du 12 mai 2020, la Caisse nationale de l'assurance maladie est responsable du traitement de données à caractère personnel dénommé « CONTACT-COVID ».

Pour autant, ainsi qu'il nous a été précisé lors du contrôle du 22 juillet 2020 par l'ARS IDF, chaque agence régionale de santé (ci-après « ARS ») est responsable des traitements des données qu'elle collecte, traite, gère et met en œuvre dans le cadre du « *tracing* » de niveau 3 du traitement « CONTACT COVID » et de tous traitements liés.

En outre, en application du décret n° 2010-336 du 31 mars 2010 portant création des agences régionales de santé et de l'article L.1432-1 du Code de la santé publique, les ARS sont des établissements publics de l'État à caractère administratif, et sont placées sous la tutelle des ministres chargés de la santé, de l'assurance maladie, des personnes âgées et des personnes handicapées.

Ainsi, 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 par l'ARS IDF le 28 juillet 2020 et par le ministère des Solidarités et de la Santé le 28 août 2020, me conduisent d'ores et déjà à vous faire part des observations suivantes.

En premier lieu, la délégation a été informée que l'ARS IDF n'a formalisé aucune procédure d'exercice des droits des personnes concernant les traitements mis en œuvre dans le cadre du « *tracing* » de niveau 3.

Or, l'article 12 du règlement précité dispose que « *le responsable du traitement prend des mesures appropriées (...) pour procéder à toute communication au titre des articles 15 à 22 (...) en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ». De même, en application des dispositions de l'article 24 du RGPD, « *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ». À cet égard,

Par conséquent, je vous prie de bien vouloir rappeler aux ARS de définir et de mettre en œuvre une procédure d'exercice des droits des personnes dont elles traitent les données dans le cadre du « *tracing* » de niveau 3 du traitement « CONTACT COVID » et de tous traitements liés. En particulier, je vous invite à faire en sorte qu'elles donnent à ces personnes les moyens d'exercer effectivement leurs droits (accès, rectification, opposition, effacement, portabilité et limitation du traitement) et qu'elles prévoient, le cas échéant, dans leurs systèmes d'information, les outils techniques qui permettront la bonne prise en compte de leurs droits.

En second lieu, la délégation a été informée que le fichier Excel contenant l'identité du patient zéro envoyé par l'ARS IDF au médecin référent de la collectivité est chiffré par l'intermédiaire de la solution « Zed! ». Or, la délégation a constaté que les mots de passe de ces archives chiffrées sont adressés au médecin par le même canal de transmission.

Or, de telles configurations, à savoir l'envoi d'une archive chiffrée et le mot de passe permettant le déchiffrement de celle-ci par le même canal d'envoi, ne permettent 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, pour satisfaire aux exigences de l'article 32 précité, je vous prie de bien vouloir veiller à la mise en œuvre, par les ARS, d'un mécanisme d'échange des données à caractère personnel entre les utilisateurs de l'application « CONTACT COVID » garantissant la confidentialité des données. Ainsi, je vous recommande de préconiser aux ARS que, dès lors qu'il y a transmission d'éléments relatifs à des patients à un professionnel de santé, cette transmission doit s'effectuer de manière chiffrée et la communication du mot de passe permettant le déchiffrement des données doit s'effectuer par un autre canal (par exemple par téléphone lorsque le fichier est envoyé par courriel).

Enfin, la délégation a été informée que dans le cadre de l'activité de « *tracing* », les agents enquêteurs de l'ARS IDF peuvent contacter le patient zéro, le médecin du travail ou le service de médecine préventive du patient zéro ou des « cas contact ». Cependant, en l'absence de médecin du travail, la délégation a constaté que les agents enquêteurs ont été amenés à contacter directement la structure qui héberge le patient zéro préalablement identifié. Or, il ressort des constations que, au moins dans un cas, l'identité et le statut médical d'un patient zéro ont été communiqués à un

responsable d'une collectivité (en l'espèce un foyer d'hébergement) par l'ARS IDF, sans que le consentement de ce patient n'ait été obtenu.

Or, d'une part, en application de l'article 9 du RGPD, le traitement des données à caractère personnel concernant la santé est interdit à moins que la personne concernée n'ait donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques.

D'autre part, l'article 3 du décret n°2020-551 du 12 mai 2020 encadre strictement les conditions dans lesquelles les données du patient zéro ou d'un « cas contact » peuvent être communiquées et aucune ne répond au cas de figure évoqué ci-dessus.

Dès lors, je vous prie de bien vouloir veiller à ce que les ARS ne transmettent des données de santé d'un patient zéro ou des personnes évaluées comme contact à risque de contamination qu'aux seules personnes autorisées par le décret 2020-551 du 12 mai 2020. À défaut, en l'absence de recueil du consentement exprès de la personne concernée à la divulgation de ses données de santé, un manquement pourra être retenu en application de l'article 9 du RGPD.

Pour votre parfaite information, je vous précise qu'un courrier a été adressé à l'ARS IDF faisant apparaître l'ensemble des observations contenues dans le présent courrier.

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]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

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

Paris, le 180121

N/Réf. : [redacted]/CS201049
Par LRAR n° 2C 156 060 2425 1
À rappeler dans toute correspondance

Monsieur le Ministre,

La CNIL a effectué, le 14 octobre et le 18 novembre 2020 respectivement, un contrôle sur place dans les locaux de l'Agence régionale de santé Grand Est (ARS Grand Est) et dans les locaux de l'Agence régionale de santé Bourgogne-Franche-Comté (ARS BFC), afin de vérifier la conformité à la loi informatique et libertés, et au RGPD, du traitement « **CONTACT-COVID** ».

Bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés. Les ARS étant placées sous la tutelle de votre ministère, je tenais d'ores et déjà, sans préjuger des suites qui seront apportées à cette procédure de contrôle, à vous faire part d'un certain nombre d'observations qui sont jointes en annexe.

Je vous précise aussi qu'ont été adressés [redacted] à l'ARS Grand-Est et un courrier d'observations à l'ARS BFC faisant apparaître l'ensemble des observations contenues dans le présent courrier et son annexe. En outre, la CNIL a adressé un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter et les mauvaises pratiques à éviter.

[redacted]

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

M.-L. De

Marie-Laure DENIS

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

ANNEXE

En premier lieu, la délégation a constaté que l'ARS Grand Est a développé un logiciel dénommé « monitoring cluster ». Chaque fiche du logiciel comprend des informations relatives à un cluster au sein d'une structure. La délégation a été informée que cette application a été mise en œuvre spécifiquement pour la gestion du niveau 3 du dispositif d'identification des patients zéros et de leurs cas contacts.

La délégation a en outre constaté la présence d'une zone « commentaire » au sein de ce logiciel.

Par ailleurs, la délégation a constaté que l'ARS BFC utilise une instance du logiciel dénommé « SORMAS » dans le cadre de sa mission de surveillance épidémiologique, conformément à l'article L. 1431-2, 1°, b) du Code de la santé publique qui dispose que les ARS contribuent notamment à l'organisation de la réponse aux urgences sanitaires et à la gestion des situations de crise sanitaire. La délégation a été informée que cette application a été mise en œuvre pour toutes les phases de gestion de l'épidémie de Covid-19, à savoir, l'investigation, la retranscription des informations de contact tracing de l'assurance maladie, la suivi et l'analyse des clusters, le suivi des signaux ainsi que le suivi des cas et des contacts. Ce logiciel comprend donc notamment des fiches relatives à un « événement » (cluster) au sein d'une structure, à un patient zéro ou à un cas contact.

Là aussi, la délégation a constaté la présence de plusieurs champs de texte libres au sein de ce logiciel et notamment dans le menu « Signal » / « Evènement » et dans les onglets de suivi des « cas » et des « contacts ».

Or, l'article 5-1-c) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données (ci-après « le RGPD ») prévoit que « *les données à caractère personnel doivent être (...) c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ».

Ainsi, si l'utilisation du logiciel SORMAS ou de logiciels ad hoc peut être nécessaire pour la gestion de la surveillance épidémiologique dans le cadre du « contact tracing » de niveau 3 par les ARS, la présence de zones de commentaire au sein de ces logiciels favorise la présence de commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées.

Dès lors, en votre qualité de ministère de tutelle, je vous invite à rappeler à l'ensemble des ARS qu'elles doivent, en tant que responsables de traitement, prendre les mesures utiles afin de limiter le risque que des données non pertinentes soient renseignées, par les agents des ARS ainsi que par leurs éventuels sous-traitants, dans les zones commentaires utilisées.

A toutes fins utiles, une fiche pratique « *Zones de bloc-notes et commentaires* » est disponible sur le site de la CNIL (https://www.cnil.fr/fr/zones-bloc-note-et-commentaires-les-bons-reflexes-pour-ne-pas-deraper).

En deuxième lieu, il ressort tout d'abord du contrôle sur place réalisé le 14 octobre 2020 auprès de l'ARS Grand-Est, que cette dernière conserve sans restriction de durée les données contenues dans le logiciel « monitoring cluster » depuis le 14 mai 2020, date de la mise en œuvre de

l'activité de « contact tracing » de niveau 3.

Ainsi, la délégation a constaté la présence entre le 1er mai 2020 et le 14 octobre 2020 de 4 131 fiches enregistrées dans le logiciel « monitoring cluster ». Dès lors, aucune fiche n'a été supprimée depuis la date de la mise en œuvre de l'activité de « contact tracing » de niveau 3.

Enfin, l'ARS Grand Est a indiqué ne pas procéder à un archivage intermédiaire des données.

Or, l'article 5-1-e) du règlement (UE) 2016/679 dispose notamment que les données *« sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées »*.

Néanmoins, je prends acte que dans le cadre du plan d'actions transmis par courriel le 6 novembre 2020, l'ARS Grand Est s'est engagée à « *organiser la suppression systématique glissante des données personnelles tous les trois mois* » de façon prioritaire.

Ensuite, la délégation a été informée que les informations recueillies par l'un des investigateurs de l'ARS Grand-Est, à la suite de l'appel téléphonique à un patient zéro afin d'identifier ses cas contacts, sont renseignées dans un fichier Excel. Ce fichier est ensuite adressé à la CNAM par une messagerie sécurisée de santé pour qu'elle reporte les données dans le téléservice CONTACT COVID.

Ainsi, la délégation a constaté la présence dans le serveur « SHAREPOINT » de l'ARS Grand Est de dix dossiers relatifs à chacun des départements de la région Grand Est contenant des fichiers Excel recensant les cas contacts associés aux patients zéro.

Dès lors, l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge) et la dispersion de ces fichiers dans les messageries ne permet pas de garantir l'effectivité des durées de conservation conformément aux dispositions de l'article 5-1-e) du RGPD précitées.

Par conséquent, je vous prie de bien vouloir veiller à la mise en œuvre, par **l'ensemble des ARS**, d'un mécanisme d'échange des données à caractère personnel entre les utilisateurs de l'application « CONTACT COVID » permettant de garantir une durée de conservation des données relatives aux personnes concernées qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées.

En troisième lieu, la délégation de contrôle a relevé, pour les ARS BFC et Grand-Est, que l'information sur la réutilisation des données issues de CONTACT COVID, dans des outils nécessaires à la gestion et au suivi épidémiologique, n'était que partiellement ou pas du tout délivrée aux personnes concernées lors des appels téléphoniques. En effet, il semble que les deux ARS se contentent d'un renvoi vers leurs sites web respectifs.

Or, je vous rappelle que conformément à l'article 12 du RGPD « *Le responsable du traitement prend des mesures appropriées pour fournir toute information visée aux articles 13 et 14 d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples (...)* ».

Les lignes directrices du groupe de travail « article 29 » sur la transparence au sens du

règlement (Union européenne) 2016/679 WP206 rev. 01 du 11 avril 2018 précisent que « *le critère "aisément accessible" signifie que la personne concernée ne devrait pas avoir à rechercher les informations mais devrait pouvoir tout de suite y accéder* ».

Or, si l'information disponible sur le site est exhaustive, rien ne permet aux patients zéros et aux cas contacts d'y accéder immédiatement à la suite de l'appel téléphonique. En effet, pour accéder à l'ensemble de l'information disponible sur le site, la personne concernée doit, de son propre chef, noter le chemin pour accéder à l'information avant de se rendre sur le site et de rechercher la rubrique correspondante.

De plus, la délégation a été informée que l'ARS Grand-Est n'a formalisé aucune procédure d'exercice des droits des personnes concernant les traitements mis en œuvre dans le cadre du « *tracing* » de niveau 3.

Or, je vous rappelle qu'en application des dispositions de l'article 24 du RGPD, « *le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au présent règlement* ». À cet égard, l'article 12 du règlement précité dispose que « *le responsable du traitement prend des mesures appropriées (...) pour procéder à toute communication au titre des articles 15 à 22 (...) en ce qui concerne le traitement à la personne concernée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples* ».

Dès lors, je vous invite à rappeler **à l'ensemble des ARS** qu'elles doivent, en tant que de responsables de traitement, délivrer aux personnes concernées une information concise, transparente, compréhensible et aisément accessible, par exemple, au moyen d'un SMS ou d'un courriel adressé aux cas contacts et aux patients zéros d'une région donnée.

Je vous recommande également de veiller à ce que **l'ensemble des ARS** définissent et mettent en œuvre une procédure d'exercice des droits des personnes (accès, rectification, opposition, effacement, portabilité et limitation du traitement) dont les données sont traitées dans le cadre du « *tracing* » de niveau 3 du traitement « CONTACT COVID » et de tous traitements liés et de prévoir, le cas échéant, dans leurs systèmes informatiques, les outils techniques qui permettront la bonne prise en compte des droits des personnes.

En quatrième lieu, la délégation a été informée, lors du contrôle de l'ARS Grand-Est, que l'application « monitoring cluster » est accessible depuis un dossier partagé à accès restreint administré et hébergé par l'ARS Grand Est. A l'occasion de ce contrôle, la délégation a constaté et a été informée par l'ARS Grand Est qu'aucune authentification supplémentaire n'est nécessaire pour accéder à cette application.

Or, l'article 32 du RGPD dispose notamment 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* », dont « *[...] le chiffrement des données à caractère personnel* » ainsi que « *des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* ». Dès lors, de telles configurations ne permettent pas de garantir la sécurité des données de manière optimale en ce qu'elles ne permettent pas d'identifier précisément une personne et de tracer les actions faites sur une fiche.

Par conséquent, je vous invite à préconiser à **l'ensemble des ARS**, de prendre toute mesure de

sécurité, pour l'ensemble des traitements de données à caractère personnel qu'elles mettent en œuvre, permettant de préserver la sécurité de ces données et de garantir la traçabilité des accès aux données en mettant en œuvre une authentification reposant sur des comptes individuels et nominatifs.

Toutefois, je prends note que, dans le cadre du plan d'actions transmis par courriel le 6 novembre 2020, l'ARS Grand Est s'est engagé à sécuriser l'accès à l'application « monitoring cluster » en mettant en place de façon prioritaire un processus d'authentification.

En cinquième lieu, la délégation a été informée lors des contrôles du 14 octobre 2020 et du 18 novembre 2020 que, tant l'ARS BFC que l'ARS Grand-Est, n'avaient pas, au jour du contrôle, réalisé d'AIPD concernant les outils de suivi et de gestion de l'épidémie de Covid-19.

Or, l'article 35-1 du RGPD dispose que « *lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.* »

L'article 35-3-b) du RGPD précise qu'une analyse d'impact relative à la protection des données (ci-après « AIPD ») est requise lorsque le traitement implique une collecte de données sensibles à large échelle, ce qui est le cas des traitements relatifs au « contact tracing » de niveau 3.

De surcroît, en application de l'article 67 de la LIL, les traitements de données à caractère personnel mis en œuvre dans le domaine de la santé par les ARS et ayant pour seule finalité de répondre à une alerte sanitaire et d'en gérer les suites, doivent faire l'objet d'une AIPD.

Dès lors, en votre qualité de ministère de tutelle, je vous invite à rappeler à **l'ensemble des ARS** qu'elles doivent procéder à une analyse d'impact relative à la protection des données, s'agissant des traitements relatifs à la mise en œuvre du « contact tracing » de niveau 3.

Je vous indique toutefois que, les dérogations prévues par l'article 67 de la LIL précité, prennent fin un an après la création des traitements. Si ces derniers continuent à être mis en œuvre au-delà de ce délai par l'ARS BFC, ils seront soumis à une autorisation de la Commission.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

CAISSE NATIONALE DE L'ASSURANCE MALADIE
Monsieur le Directeur Général
26 avenue du professeur André Lemierre
75020 - PARIS

Paris, le 180121

N/Réf. : [redacted]/CS201051
Par LRAR n° 2C 156 060 2426 8
À rappeler dans toute correspondance

Monsieur le directeur général,

Conformément à la décision n° 2021-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué plusieurs contrôles auprès de la Caisse nationale d'assurance maladie (ci-après « CNAM »).

Ces contrôles avaient pour objet de vérifier la conformité à la loi du 6 janvier 1978 modifiée (LIL) et au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, du traitement de données à caractère personnel dénommé « **CONTACT-COVID** », résultant de l'adaptation du système d'information « amelipro » 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 la CNAM.

Une première série de contrôles a ainsi été effectuée de mai à août 2020, puis des contrôles complémentaires ont été effectués dans les locaux de la Caisse primaire d'assurance maladie (ci-après CPAM) de la Côte d'Or, situés au 1D boulevard de Champagne à DIJON (21000), le 17 novembre 2020, ainsi que sur audition, de la CNAM, le 10 novembre 2020. Enfin, un contrôle en ligne du site web « declare.ameli.fr/sms/ » a été réalisé le 12 novembre 2020.

La CNIL a également procédé au contrôle des partenaires ayant accès à CONTACT COVID, notamment auprès de l'agence régionale de santé (« ARS ») Grand Est, et de l'ARS Bourgogne-Franche-Comté.

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 le 7 décembre 2020, me conduisent d'ores et déjà à vous faire part des observations suivantes.

Tout d'abord, je note que la CNAM a mis en œuvre de nombreuses mesures techniques et organisationnelles afin de garantir le respect de la protection des données personnelles des patients zéros et des cas contacts au sein de CONTACT COVID. En particulier, je constate que l'information des cas contact et patients zéro est satisfaisante et la suppression automatique des données contenues dans CONTACT COVID à l'issue d'un délai de trois mois à compter de leur collecte est désormais mise en œuvre.

Toutefois, des corrections doivent être apportées sur plusieurs points listés ci-après.

En premier lieu, la délégation a constaté la présence de la solution visant à prévenir les attaques par déni de service [redacted] sur la page web ayant pour URL « https://declare.ameli.fr/sms/ ». Cette solution, proposée et hébergée par la société [redacted] entraine le traitement de données des internautes *via* leur navigateur.

A cet égard, l'article 82 de la loi du 6 janvier 1978 modifiée dispose notamment que *« tout abonné ou utilisateur d'un service de communications électroniques doit être informé de manière claire et complète »* par le responsable du traitement ou son représentant de *« la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations déjà stockées dans son équipement terminal de communications électroniques »* ainsi que *« des moyens dont il dispose pour s'y opposer »*.

Or, la délégation n'a constaté aucune mention d'information relative à ce traitement ni des moyens de s'y opposer.

Je prends acte de la suppression de la solution [redacted] sur la page web ayant pour URL « https://declare.ameli.fr/sms/ » suite aux échanges avec la CNIL.

Pour autant, je vous alerte sur la nécessité mettre en conformité l'ensemble des pages web éditées par la CNAM qui utiliseraient la même solution.

En second lieu, j'ai bien pris note des projets en cours relatifs à la mise en œuvre de l'e-CPS pour l'authentification des utilisateurs de CONTACT COVID ainsi que de l'étude de faisabilité relative à la mise en œuvre d'une authentification forte pour les comptes partenaires à destination des agents des ARS et des établissements de santé.

Toutefois, la délégation a constaté, lors d'un contrôle au sein de la Caisse primaire d'assurance maladie (ci-après CPAM) de la Côte d'Or le 17 nombre 2020, la présence d'adresses électroniques de comptes partenaires (administrateurs locaux ou utilisateurs), ayant pour domaine « orange.fr », « gmail.fr », « wanadoo.fr » ou commençant par « secrétariat », « direction », « qualite », « cadrebloc ».

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 »*.

Or, l'utilisation d'adresses électroniques non professionnelles ou d'adresses génériques ne permet pas de garantir de façon optimale la traçabilité des accès ni la confidentialité des données traitées par CONTACT COVID.

Dès lors, pour satisfaire aux exigences de l'article 32 précité, il conviendra de mettre en œuvre une vérification des domaines utilisés pour la création de comptes ainsi qu'une revue régulière des comptes créés. Vous pouvez notamment limiter la création des comptes aux seuls utilisateurs dont l'adresse électronique appartient au domaine du partenaire.

En troisième lieu, dans le cadre d'un contrôle sur place opéré auprès de l'ARS Grand Est, la délégation a observé que les informations recueillies par un agent de cette ARS, à la suite de l'appel téléphonique à un patient zéro afin d'identifier ses cas contacts, sont renseignées dans un fichier Excel. Ce fichier est ensuite adressé à la CNAM par une messagerie sécurisée de santé pour qu'elle reporte les données dans le téléservice CONTACT COVID.

Sur ce point, si je prends note que cette pratique est prévue par les circulaires MINSANTE n°99 et n°155, je considère cependant, en application de l'article 32 précité, qu'elle entraîne une dispersion des données dans les messageries car les fichiers sont ensuite, au moins en partie, conservés dans les serveurs. Cette pratique n'est pas, faute de précautions suffisantes, de nature à garantir l'effectivité du respect de durées de conservation raisonnables.

Je vous recommande donc, en votre qualité de responsable de traitement, d'inciter les ARS, par exemple, soit à cesser la transmission des fichiers Excel via des messageries sécurisées de santé et d'alimenter les données relatives aux cas contacts du patient zéro dans le logiciel CONTACT COVID prévu à cet effet, soit de procéder à la suppression immédiate des courriels contenant les fichiers Excel à la suite de leur envoi via les messageries sécurisées de santé, soit de procéder à un archivage régulier des courriels contenant ces fichiers Excel.

[redacted]

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

Marie-Laure DENIS

Copie [redacted] Déléguée à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE DE SANTE GUADELOUPE
SAINT-MARTIN ET SAINT-BARTHELEMY
MADAME LA DIRECTRICE GÉNÉRALE
RUE DES ARCHIVES
BISDARY
97113 - GOURBEYRE

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211007
Par LRAR n° 2C 141 002 1555 4
À rappeler dans toute correspondance

Madame la Directrice Générale,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur

individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

Je vous prie d'agréer, Madame la Directrice Générale, mes salutations distinguées.

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE DE LA MARTINIQUE
MONSIEUR LE DIRECTEUR GÉNÉRAL
CENTRE D'AFFAIRES AGORA
ZAC DE L'ETANG Z'ABRICOT
POINTE DES GRIVES
CS 80 656
97263 FORT DE FRANCE

Paris, le 21 JAN. 2021

N/Réf. [redacted]/CS201008
Par LRAR n° 2C 141 002 1554 7
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche

de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT

COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

Copie [redacted] Déléguée à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE
CENTRE-VAL DE LOIRE
MONSIEUR LE DIRECTEUR GÉNÉRAL
CITÉ COLIGNY
131 RUE DU FAUBOURG BANNIER
BP 74409
45044 - ORLÉANS

Paris, le 21 JAN. 2021

N/Réf. [redacted]/CS201009
Par LRAR n° 2C 141 002 1553 0
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur

individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE
AUVERGNE-RHONE-ALPES
MONSIEUR LE DIRECTEUR GENERAL
241 RUE GARIBALDI
CS 93383
69418 – LYON CEDEX 03

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211010
Par LRAR n° 2C 141 002 1552 3
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

Copie [redacted] Déléguée à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE SANTE DE CORSE
ARS CORSE
MADAME LA DIRECTRICE GENERALE
QUARTIER ST JOSEPH
CS13003
20700 - AJACCIO

Paris, le
21 JAN. 2021

N/Réf. [redacted]/CS211011
Par LRAR n° 2C 141 002 1550 9
À rappeler dans toute correspondance

Madame la Directrice Générale,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

Je vous prie d'agréer, Madame la Directrice Générale, mes salutations distinguées.

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE
PROVENCE-ALPES-CÔTE D'AZUR
MONSIEUR LE DIRECTEUR GENERAL
132 BOULEVARD DE PARIS
13003 - MARSEILLE CEDEX 03

Paris, le
21 JAN. 2021

N/Réf. [redacted]**/CS211012**
Par LRAR n° 2C 141 002 1549 3
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission

est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai

de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

Copi[redacted] Déléguée à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE RÉGIONALE DE SANTÉ OCCITANIE
MONSIEUR LE DIRECTEUR GÉNÉRAL
26-28 PARC CLUB DU MILLENAIRE
1025, RUE HENRI BECQUEREL
34067 - MONTPELLIER

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211013
Par LRAR n° 2C 141 002 1546 2
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE
NOUVELLE-AQUITAINE
MONSIEUR LE DIRECTEUR GÉNÉRAL
103 BIS RUE BELLEVILLE
CS 91704
33063 - BORDEAUX CEDEX

Paris, le 21 JAN. 2021

N/Réf. [redacted]/CS201014
Par LRAR n° 2C 141 002 1545 5
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

Copie [redacted] Déléguée à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE PAYS DE LA LOIRE
MONSIEUR LE DIRECTEUR GÉNÉRAL
17 BOULEVARD GASTON DOUMERGUE
CS 56233
44262 - NANTES CEDEX 2

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211015
Par LRAR n° 2C 141 002 1544 8
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE RÉGIONALE DE SANTÉ BRETAGNE
MONSIEUR LE DIRECTEUR GÉNÉRAL
CS14253
6, PLACE DES COLOMBES
35042 – RENNES CEDEX

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211018
Par LRAR n° 2C 141 002 1541 7
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

[redacted]

Marie-Laure DENIS

Copie [redacted] Déléguée à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE RÉGIONALE DE SANTÉ NORMANDIE
MONSIEUR LE DIRECTEUR GÉNÉRAL
ESPACE CLAUDE MONET
2 PLACE JEAN NOUZILLE
14050 - CAEN

Paris, le 21 JAN. 2021

N/Réf. [redacted]/CS211019
Par LRAR n° 2C 141 002 1532 5
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

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

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE D'ILE DE FRANCE
MONSIEUR LE DIRECTEUR GÉNÉRAL
MILLÉNAIRE 2
35 RUE DE LA GARE
75019 - PARIS

Paris, le 21 JAN. 2021

N/Réf. [redacted]/CS201020
Par LRAR n°2C 141 002 1529 5
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

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 à [redacted]

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE HAUTS-DE-FRANCE
MONSIEUR LE DIRECTEUR GÉNÉRAL
556 AV WILLY BRANDT
59777 - LILLE

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211021
Par LRAR n° 2C 141 002 1528 8
À rappeler dans toute correspondance

Monsieur le Directeur Général,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission

est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai

de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

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

Marie-Laure DENIS

Copie [redacted] Délégué à la protection des données)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE DE GUYANE
MADAME LA DIRECTRICE GÉNÉRALE
BP 696
66 AVENUE DES FLAMBOYANTS
97300 - CAYENNE CEDEX

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211022
Par LRAR n° 2C 141 002 1524 0
À rappeler dans toute correspondance

Madame la Directrice Générale,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

Je vous prie d'agréer, Madame la Directrice Générale, mes salutations distinguées.

Marie-Laure DENIS

Copie à Madame ou Monsieur le/la Délégué(e) à la protection des données

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE DE LA REUNION
MADAME LA DIRECTRICE GÉNÉRALE
2 BIS, AVENUE GEORGES BRASSENS
CS 61002
97743 - SAINT DENIS CEDEX 9

Paris, le 21 JAN. 2021

N/Réf. [redacted]CS211023
Par LRAR n° 2C 141 002 1523 3
À rappeler dans toute correspondance

Madame la Directrice Générale,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

Je vous prie d'agréer, Madame la Directrice Générale, mes salutations distinguées.

Marie-Laure DENIS

Copie à Madame ou Monsieur le/la Délégué (e) à la protection des données.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE REGIONALE DE SANTE DE MAYOTTE
MADAME LA DIRECTRICE GÉNÉRALE
CENTRE KINGA
90, ROUTE NATIONALE 1
KAWENI -BP 410
97113 - MAMOUDZOU

Paris, le 21 JAN. 2021

N/Réf. [redacted]/CS211024
Par LRAR n° 2C 141 002 1522 6
À rappeler dans toute correspondance

Madame la Directrice Générale,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, entre mai et novembre 2020, plusieurs contrôles sur place auprès de différentes Agences régionales de santé (ci-après « ARS »).

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 « **CONTACT-COVID** ».

Dans le contexte de l'état d'urgence sanitaire lié à l'épidémie de covid-19, le gouvernement a mis en œuvre une stratégie dite de « déconfinement progressif » qui repose notamment sur la mise en place d'un dispositif dit de « contact tracing ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 (ci-après « patients zéro ») et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive (ci-après « cas contact »).

Ainsi, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT-COVID ».

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les ARS.

Le niveau 1 permet aux médecins de ville, établissements de santé et centres de santé d'initier une fiche de suivi du patient zéro et de ses cas contacts dans le téléservice CONTACT COVID.

Le niveau 2 permet au personnel habilité de l'assurance maladie (ou aux personnes à qui cette mission est déléguée par les textes) de compléter et d'affiner, si nécessaire, la fiche du patient zéro et la liste de ses cas contacts dans le téléservice CONTACT COVID. Ce personnel appelle ensuite les cas contacts pour leur communiquer les consignes de quarantaine, de tests et autres conduites à tenir.

Le niveau 3 est assuré par les ARS, établissements publics autonomes de l'Etat, réparties sur les territoires des différentes régions françaises. Les ARS sont chargées du pilotage régional du système de santé.

Sur la base des données du « contact tracing » réalisé par les niveaux 1 et 2 et collectées dans le téléservice CONTACT COVID, les ARS identifient les chaînes de transmission sur leur territoire et les « clusters ». Elles assurent aussi, en lien avec le niveau 2, la gestion des situations complexes, notamment la survenue des cas dans certains lieux déterminés (écoles, EHPAD ou établissements pénitentiaires par exemple). Si la situation le nécessite, elles déploient des moyens d'investigation sur le terrain, organisent des campagnes de dépistage ciblées et peuvent proposer au préfet de département des mesures de contrôle spécifiques (fermeture de structures par exemple). Elles sollicitent si nécessaire l'appui des préfectures, des collectivités territoriales et de tout autre acteur concerné, pour l'organisation de ces investigations de terrain.

Dans ce contexte, bien que la CNAM soit responsable de ce traitement en vertu de l'article 1 du décret n° 2020-551 du 12 mai 2020, chaque ARS est responsable des traitements qu'elle met en œuvre dans le cadre du *tracing* de niveau 3 et de tous traitements liés mis en œuvre sur la base des données exportées à partir du traitement « CONTACT COVID ».

Par conséquent, la Commission a tenu à adresser un courrier à l'ensemble des ARS afin de rappeler les bonnes pratiques à adopter, nécessaires à la protection des données des personnes concernées issues du téléservice CONTACT COVID, et les mauvaises pratiques à éviter.

En ce qui concerne les bonnes pratiques, au titre des vérifications effectuées, la Commission a pu constater, lors de ses contrôles, que la mise en œuvre de nombreuses mesures garantissant le traitement des données à caractère personnel de manière satisfaisante :

- la mise à jour du registre des traitements relatifs au téléservice « CONTACT COVID » par l'ensemble des ARS ;
- l'utilisation d'un outil approprié à la gestion de l'épidémie ainsi que son hébergement par un hébergeur de données de santé « HDS » (voulu par l'ARS en question) et l'implémentation dans ce logiciel d'une suppression automatique des données « signalées » depuis plus de trois mois ;
- la mise en place de mesures de sécurité (telles que l'authentification forte lors de la connexion à l'outil susmentionné) afin de protéger les données traitées dans le cadre du *tracing* de niveau 3.

En ce qui concerne les mauvaises pratiques, la CNIL a constaté que certaines ARS ne mettaient pas en œuvre des garanties suffisantes permettant le respect des obligations prévues par la loi n° 2020-546 du 11 mai 2020 et le décret n° 2020-551 du 12 mai 2020.

En effet, il a ainsi été relevé, individuellement, auprès des ARS contrôlées que :

- aucune procédure d'exercice des droits « Informatique et Libertés » à destination des « patients zéro » et des « cas contacts » n'a été formalisée par une ARS ayant fait l'objet de contrôles ;
- le consentement du patient « zéro » n'était pas toujours recueilli avant la divulgation de son identité à la collectivité à laquelle il appartient (employeur, hébergement, école, etc.) ;
- le développement d'un logiciel spécifique pour les besoins du « contact tracing » d'une ARS contrôlée en lien avec le traitement des données personnelles issues du téléservice « CONTACT COVID », ne dispose ni d'authentification, ni de profil d'habilitation, ni de compte utilisateur individuel. Aucune traçabilité des accès n'est, dès lors, possible. Sur ce point, il a été constaté que

l'ARS en question n'a pas implémenté de procédure de suppression des fichiers à l'issue d'un délai de trois mois à compter de la collecte des données. Elle n'a pas non plus procédé à une purge ou à un archivage des données collectées à partir du téléservice « CONTACT COVID » ;

- au lieu de directement inscrire les informations relatives aux cas contacts dans le téléservice « CONTACT COVID » et ce, pour des raisons organisationnelles, une ARS complète des fichiers de type « Excel » qu'elle adresse ensuite aux CPAM par messagerie. Or, cette pratique conduit à la dispersion de ces fichiers dans les messageries et ne permet pas de garantir l'effectivité des durées de conservation sur les données concernées en l'absence de mécanisme de gestion du cycle de vie des données au sein de ces fichiers Excel (notamment de purge).

Enfin, il est à relever que certaines mauvaises pratiques constatées sont communes aux ARS contrôlées. Il est ainsi apparu que :

- l'information qui est délivrée aux personnes concernant la réutilisation des données issues du téléservice « CONTACT COVID » à des fins de suivi épidémiologique est, soit absente, soit incomplète, soit difficilement accessible ;
- des « champs commentaires » sont présents au sein des outils utilisés dans le cadre de la gestion de l'épidémie de Covid-19, alors que de telles de zones de saisie de texte libre favorisent le risque de renseigner des commentaires inappropriés ou non pertinents en lien avec la vie privée des personnes concernées. Sur ce point, la CNIL recommande donc de limiter le recours aux zones de commentaires libres et de favoriser l'utilisation de menus déroulants proposant des appréciations objectives.
- aucune des ARS contrôlées n'a réalisé d'analyse d'impact relative à la protection des données et ce contrairement aux obligations prévues à l'article 35 du règlement précité.

Par conséquent, je vous invite à faire preuve de vigilance quant au respect du traitement des données des personnes issues du téléservice « CONTACT COVID » dans le cadre des traitements réalisés par votre ARS.

Je vous indique d'ores et déjà que, conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et ainsi qu'il a été annoncé par la Commission dans le cadre de son avis public du 14 janvier 2021[1] relatif notamment au téléservice « CONTACT COVID », des contrôles auprès de plusieurs ARS se poursuivront jusqu'à la fin de la mise en œuvre de ce traitement.

[redacted]

Je vous prie d'agréer, Madame la Directrice Générale, mes salutations distinguées.

Marie-Laure DENIS

Copie [redacted]

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ

Liberté
Égalité
Fraternité

Le Directeur de Cabinet

Paris, le 15 FEV. 2021

CAB OV/SSD/Pégase D-21 004779
Vos Réf : [redacted]/CS201049

Madame la présidente,

Par courrier du 18 janvier 2021, vous attirez l'attention du ministre des Solidarités et de la Santé sur les constatations effectuées par la CNIL lors de ses contrôles sur les systèmes d'information de contact tracing de niveau 3 (CT3) au sein d'ARS.

Dès le 21 janvier, la DPD des ministères sociaux a organisé des réunions avec les DPD des ARS afin de les sensibiliser sur les différentes préconisations mentionnées dans votre courrier.

En premier lieu, s'agissant de la présence de **zones de commentaires**, il a été rappelé le principe de minimisation des données et le fait que ces zones favorisent la présence de commentaires inappropriés (art. 5-1.c du RGPD). Cette réunion fut également l'occasion de renvoyer les DPD des ARS vers la fiche de la CNIL « Zone de bloc-notes et commentaires » disponible sur son site.

En deuxième lieu, sur les **durées de conservation excessives** constatées par la CNIL dans l'outil de CT3, un « SharePoint » et la messagerie sécurisée, il a été rappelé les durées de conservations des données figurant dans les textes et la nécessité de gérer cette durée de conservation sur l'ensemble des supports.

En outre, un groupe de travail ministériel a été constitué, avec notamment les archivistes et la DPD des ministères sociaux ainsi que les ARS volontaires (DPD, médecins épidémiologistes, juristes), afin d'apprécier la nécessité d'effectuer un archivage intermédiaire de certaines données de CT3 pour répondre aux enjeux administratifs de gestion du contentieux et à des fins d'études épidémiologiques.

L'objectif de ce groupe qui s'est réuni le 1er février est de livrer rapidement un premier référentiel pour un archivage intermédiaire directement utilisable par les ARS dans le cadre de leur traitement de CT3. Un premier document de travail synthétisant les catégories de données qui mériteraient a priori un archivage intermédiaire a été partagé avec les DPD des ARS le 10 février.

En troisième lieu, sur **l'information relative à la réutilisation des données** issues de Contact Covid dans les outils de CT3 des ARS, il a été rappelé aux DPD des ARS la nécessité de définir une procédure formalisée pour répondre aux demandes d'exercice des droits des personnes ainsi que d'informer les personnes concernées d'une manière transparente, compréhensible et facile d'accès.

.../.

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

Pour mémoire, la prise en charge des cas et des personnes contacts repose sur une organisation en 3 niveaux. Les deux premiers niveaux visent à prendre en charge uniquement les personnes pour lesquelles les mesures de prévention ne posent pas de difficultés de mise en œuvre. L'assurance maladie en assure la mise en œuvre. Les situations relevant des chaines de transmission ou de cluster ainsi que les cas ayant eu des contacts multiples relève du niveau 3. Les ARS sont chargés de ce niveau 3.

Pour le contrat tracing de niveau 3, les enquêteurs des ARS sont rarement en contact direct avec les « Patients 0 » et encore moins avec les personnes contacts (contrairement aux enquêteurs de l'assurance maladie). En effet, leur mission consiste à contacter les responsables des collectivités (écoles, entreprises...) pour déterminer avec eux la liste des personnes contacts. Les enquêteurs des ARS ne contactent les P0 que lorsqu'ils ont besoin d'obtenir les coordonnées du responsable de la collectivité.

Dans la circulaire interministérielle du 14 janvier 2021 relative au nouveau dispositif d'accompagnement à l'isolement par les cellules territoriales d'appui à l'isolement (CTAI), il est prévu que l'assurance maladie propose aux P0 l'organisation d'une visite à domicile par un infirmier et une offre d'accompagnement matériel, social et psychologique aux P0 et aux cas contacts. Cet accompagnement est réalisé par les CTAI. Les ARS n'adressent donc plus par courriel ou SMS l'offre d'une aide à l'isolement et les consignes sanitaires à respecter contrairement à ce qui est mentionné dans le point 78 de la délibération de la CNIL 2021-004 du 14 janvier 2021.

Les préconisations de la CNIL consistant à fournir une information sur le traitement de CT3 (ou un lien) par courriel ou SMS aux P0 et aux personnes contacts lors de l'envoi des consignes sanitaires ne sont adaptées que lorsqu'un tel échange existe.

Les personnes concernées sont informées par la CNAM que les données sont utilisées pour la réalisation d'enquêtes sanitaires pour établir les chaines de transmission et les « cluster ».

Pour compléter cette information, le ministère a également préconisé aux ARS :

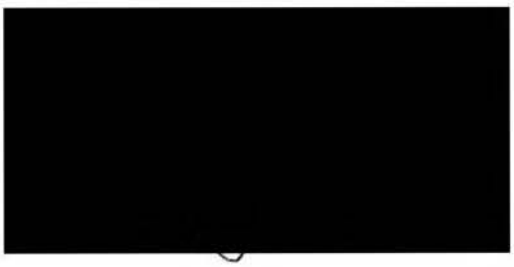
- d'intégrer sur les serveurs vocaux des ARS une information succincte sur les traitements de CT3 et comment trouver l'information complète sur le dispositif ;
- de prévoir une information succincte à donner par l'enquêteur dès lors qu'il appelle un P0 et que ces éléments figurent dans la fiche de procédure remise aux enquêteurs ;
- de demander au responsable de la collectivité d'informer les personnes concernées qu'elles peuvent obtenir de l'information sur le traitement CT3 en consultant la page « données personnelles de l'ARS » et spécifier le lien hypertexte dans le cadre de l'échange par courriel sécurisé avec l'ARS. Ce point doit figurer dans la procédure remise aux enquêteurs ;
- dans l'hypothèse d'un échange par sms ou courriel avec le P0 ou un cas contact, un lien vers la mention d'information sur le traitement doit être ajouté.

Des évolutions de la procédure, notamment en lien avec les variants, sont prévues. En cas de contact avec les P0 ou les personnes contacts, il a été rappelé la nécessité de les informer de manière claire.
En quatrième lieu, la réunion de travail du 21 janvier a également été l'occasion d'insister sur le fait que l'accès à l'application de CT3 doit bénéficier d'une double authentification reposant sur des comptes individuels et nominatifs.

En cinquième lieu, en matière d'analyse d'impact sur la protection des données (AIPD), il a été rappelé aux ARS que les traitements de CT3 sont des traitements à risques élevés qui nécessitent une AIPD conformément à l'article 35 du RGPD. L'article 67 de la LIL n'exonère en effet pas les traitements pris sur ce fondement de la réalisation d'une AIPD.

Il a également été indiqué aux DPD des ARS que la dérogation à l'obligation d'effectuer des formalités préalables pour les traitements de gestion d'alerte sanitaire prend fin **un an** après la création du traitement. Des travaux ministériels sont en cours pour évaluer la nécessité de compléter le décret du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions sur ce point.

Je vous prie d'agréer, Madame la présidente, mes salutations distinguées.



l'Assurance Maladie
Caisse Nationale
Le Directeur Général

Madame Marie-Laure Denis
Présidente
Commission Nationale Informatique & Libertés
3, Place de Fontenoy, TSA 80715
75 334 Paris Cedex 07

Date 0 1 MARS 2021

N/Ref. : [redacted]/CS201051 – LRAR n°156 060 2426 8

Madame la Présidente,

A l'issue des nouveaux contrôles diligentés au titre de la décision n°2020-091C du 20 mai 2020, vous m'avez adressé une série d'observations sur le traitement de données « Contact Covid ».

- S'agissant du [redacted]

A la suite de votre alerte quant à l'utilisation de ce recaptcha, nous l'avons immédiatement retiré de la page « declare.ameli.fr/sms» et nous avons étudié les solutions qui pouvaient être implémentées afin de retirer également ce dernier de nos autres pages web. En effet, il n'est, à ce stade, pas possible de procéder à un retrait pur et simple ou d'intégrer un module de gestion des consentements, dès lors que le [redacted]est utilisé pour une finalité de sécurité. Il permet notamment de limiter le risque d'attaque par robot pouvant générer un déni de service.

Après examen des différentes solutions proposées sur le marché, nous avons opté pour la solution offerte par [redacted] Cette solution n'étant pas en mode SAS, nous devons planifier plusieurs développements nécessaires à son intégration. Ces derniers, qui impliquant des équipes déjà très fortement mobilisées par les systèmes d'information liés à la gestion de la crise sanitaire, n'ont pas pu être finalisés à ce jour. Nous vous tiendrons informés dès que nous serons en capacité de nous engager sur une date d'intégration de cette nouvelle solution.

- S'agissant de la **sécurisation des comptes partenaires**

Nous rappelons systématiquement l'obligation d'utilisation d'une adresse e-mail professionnelle liée à la structure d'exercice avec l'utilisation d'un même nom de domaine entre l'administrateur local et l'utilisateur. Ces consignes ont été correctement respectées sauf effectivement pour quelques cas isolés et ponctuels. A la suite de votre courrier, nous avons procédé à une nouvelle revue des comptes et procédé à la suppression de ceux qui ne respectaient pa l'exigence quant à l'adresse e-mail utilisée.

Sur 6600 comptes ouverts à cette date, nous avons détecté 1 compte ouvert avec une adresse wanadoo et 6 avec une adresse orange. Bien qu'en wanadoo, l'adresse correspond bien à une adresse professionnelle. Nous allons prendre contact avec les agents du réseau de l'Assurance Maladie à l'origine de ces créations pour leur faire un rappel des consignes.

Pour assurer la meilleure conformité possible, nous allons également réaliser un rappel général à l'ensemble du réseau pour réaffirmer la consigne. Le message écrit, mais aussi relayé lors des webinaires organisés avec tous les organismes, est le suivant :

« L'adresse mail doit être une adresse professionnelle attribuée à une seule personne uniquement. Les noms de domaines « grand public » comme @gmail, @orange, @hotmail ne sont pas autorisés. De plus, une adresse mail non nominative comme secretariat_accueil@structure.fr pouvant se rapporter à une liste de diffusion, ne doit pas être acceptée ».

Par ailleurs, nous vous confirmons la bonne mise en œuvre du renforcement des conditions d'authentification aux comptes partenaires. En effet, nous allons fonctionner en deux étapes consécutives reposant sur une procédure de type TOTP. Cette solution est mise en œuvre progressivement depuis la fin février pour devenir à terme obligatoire pour tous les administrateurs locaux (avec reprise du stock) et pour les utilisateurs qui ne disposeront pas d'une solution ProsantéConnect.

- S'agissant des **échanges avec les ARS**

Depuis les circulaires MINSANTE n° 99 et n°155, les consignes ont substantiellement évolué dès lors que les ARS disposent désormais toutes de comptes partenaires.
Ainsi, si le recours à une messagerie sécurisée de santé avait été mis en place au lancement de contact covid pour permettre l'envoi sécurisé de données sensibles en l'absence de solution alternative (avec des consignes de suppression des fichiers à très brève échéance), les ARS sont désormais invitées à intégrer toutes les données utilisées dans le cadre du contact tracing directement dans Contact Covid. Les organismes d'assurance maladie, lorsqu'ils saisissent les ARS au titre notamment du tracing de niveau 3, le font par courriel, mais ceux-ci ne contiennent, conformément aux demandes issues de vos services, que les numéros de fiches à traiter. Ainsi, seul un agent d'une ARS disposant d'un moyen d'authentification à contact covid peut se rendre sur la fiche à traiter pour la prendre en charge dans les délais contraints. Ces consignes sont normalement connues des utilisateurs qui disposent de modes opératoires.

Dans la continuité des échanges réguliers déjà intervenus sur ce traitement de données, la déléguée à la protection des données de la Cnam se tient à la disposition de votre service des contrôles pour apporter toute information complémentaire.

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

[redacted]

Caisse Nationale de l'Assurance Maladie
50, avenue du Professeur André Lemierre - 75986 Paris cedex 20
Tél.: 01 72 60 10 00 - Fax : 01 72 60 10 10 - www.ameli.fr

MINISTÈRE
DE L'ÉDUCATION
NATIONALE,
DE LA JEUNESSE
ET DES SPORTS

Liberté
Égalité
Fraternité

Le ministre

Paris, le 23 DEC. 2021

Madame la Présidente,

A la suite du contrôle exercé par la Commission nationale de l'informatique et des libertés au sein des locaux du rectorat de l'académie d'Orléans-Tours le 23 novembre 2021, vous me transmettez le rapport d'expertise que le docteur [redacted] médecin expert près la Cour d'appel d'Orléans, a établi en application de la décision de contrôle de la CNIL n°2020-091C.

Vigilant sur la question de la gestion des données numériques à caractère personnel au sein de l'éducation nationale, j'ai pris connaissance de ce document ainsi que des éléments transmis le 29 novembre 2021 [redacted] avec la plus grande attention.

A cet égard, je vous informe que j'ai, d'ores et déjà, transmis l'ensemble de ce dossier à Monsieur le directeur des affaires juridiques afin qu'il suive attentivement l'évolution de la procédure de contrôle en cours.

Je vous prie d'agréer, Madame la Présidente, l'expression de mes respectueux hommages.

Jean-Michel BLANQUER

Madame Marie-Laure DENIS
Présidente de la Commission nationale
Informatique & Libertés
CNIL
3 Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

110 rue de Grenelle
75357 Paris SP 07
Tél : 01 55 55 10 10

Référence à rappeler : BDC/2021021104/SC/IR
BDC/2021020931/SC/IR
V/Ref : [redacted] Décision n°2020-091C

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Service des contrôles

AGENCE RÉGIONALE DE SANTÉ
ILE DE FRANCE
MONSIEUR LE DIRECTEUR
GÉNÉRAL
Immeuble "Le Curve"
13 rue du Landy
93200 Saint-Denis

Paris, le 31 MARS 2021

N/Réf. : DI211061
À rappeler dans toute correspondance
LRAR n° 2C 156 060 2562 3

Monsieur le Directeur général,

En application de la **décision n° 2020-091C** de la Présidente de la Commission en date du 12 mai 2020, la Commission a décidé d'effectuer, dans les conditions prévues à l'article 19 de la loi du 6 janvier 1978 modifiée, un contrôle visant à 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 « Contact Covid », résultant de l'adaptation du système d'information « amelipro » 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 la caisse nationale de l'assurance maladie et de tout traitement lié.

Vous trouverez ci-joint à cet effet copies de la décision de contrôle, de l'ordre de mission désignant les personnes habilitées à effectuer les vérifications ainsi que d'un questionnaire relatif aux conditions de traitement des données. Les réponses au questionnaire sont à apporter à la Commission **au plus tard le 1er mai 2021.**

La communication des informations demandées pourra s'effectuer par courrier postal ou, de préférence, de manière dématérialisée. L'envoi dématérialisé devra être effectué par un moyen sécurisé (utilisation d'une plateforme d'échange sécurisée ne nécessitant pas la création d'un compte ou chiffrement du document de réponse adressé aux adresses électroniques figurant ci-dessous). La Commission pourra utilement mettre à votre disposition un lien de téléversement vers sa plateforme de dépôt de fichiers sécurisée. Le cas échéant, je vous invite à nous communiquer votre adresse électronique.

Je vous précise que les modalités de contrôle ainsi arrêtées n'excluent pas la possibilité pour la Commission de procéder, dans un second temps, à des vérifications sur place, notamment selon la qualité et la pertinence des éléments de réponse apportés.

[redacted]

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

[redacted]

[redacted]

P. J : Décision n°2021-091C
Ordre de mission
Questionnaire

Questionnaire portant sur la mise en œuvre du traitement « COVI CONTACT »

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.).

À titre liminaire, la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire, complété par le décret n° 2020-551 du 12 mai 2020 modifié, a notamment autorisé la création d'un traitement de données à caractère personnel dénommé « CONTACT COVID ». Ce traitement s'est traduit par l'adaptation, par la Caisse nationale de l'assurance maladie (ci-après « CNAM »), du système d'information « amelipro » afin de mettre en œuvre le téléservice « CONTACT COVID ».

Ce dispositif vise au suivi des patients testés positifs à la covid-19 et à l'identification des personnes ayant été en contact rapproché avec une personne détectée positive.

Dans ce cadre, l'identification des patients zéro et de leurs cas contacts s'appuie sur un dispositif à trois niveaux utilisant le téléservice « CONTACT COVID ». Les trois niveaux sont assurés successivement par les médecins, la CNAM et les Agences régionales de santé (ci-après « ARS »).

Il apparait que dans la continuité de l'activité de « contact tracing », l'ARS Île-de-France a mis œuvre un dispositif multicanal d'accompagnement dénommé « COVI CONTACT » destiné à toutes les personnes concernées par des mesures d'isolement à domicile afin d'être accompagnées régulièrement et à distance.

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.

1. **Les traitements mis en œuvre dans le cadre du dispositif « COVI CONTACT »**

4.1. Veuillez décrire le traitement de données à caractère personnel dénommé « COVI CONTACT ».

4.2. Veuillez indiquer, à l'aide de tout document, le parcours de la donnée dans le cadre des traitements « COVI CONTACT ».

4.3. Veuillez communiquer tout document permettant de décrire l'architecture du dispositif « COVI CONTACT ».

4.4. Veuillez communiquer le calendrier du déploiement du dispositif « COVI CONTACT » en précisant, le cas échéant, les dates différentes phases de mise en œuvre.

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

4.6. Veuillez préciser la date à laquelle le traitement « COVI CONTACT » a été mis en œuvre.

4.7. Dans l'éventualité d'un contrôle sur place, indiquez les adresses où pourrait se rendre la délégation de la CNIL ainsi que les noms et courriels des personnes compétentes pour la recevoir, notamment siège social et locaux informatiques.

2. **La détermination du responsable du traitement**

2.1. Indiquer qui est le responsable des traitements de données à caractère personnel mis en œuvre à partir du traitement « COVI CONTACT ».

2.2. Indiquer si les traitements concernés font l'objet d'une responsabilité conjointe et dans l'affirmative, fournir l'analyse ayant conduit à cette qualification ainsi que tout document contractuel organisant les obligations respectives des parties.

3. **Les données collectées, finalité de la collecte et base légale des traitements**

3.1. Indiquer quelles sont les données collectées et les différentes modalités de collecte des données associées (site internet, application mobile, etc.).

3.2. Indiquer si le dispositif « COVI CONTACT » contient des zones de commentaires / textes libres. Le cas échéant, fournir une extraction depuis la base de données du contenu des champs de texte libres renseignés u depuis la date de début de la mise en œuvre du dispositif précité, en précisant pour chaque commentaire le numéro identifiant la personne associée ainsi que la liste des éléments qui y sont rattachés en base de données (date de création du commentaire, date de modification du commentaire, données additionnelles requises ou facultatives pour la rédaction du commentaire, etc.).

3.3. Indiquer si le traitement « COVI CONTACT » procède à la collecte des données de localisation des utilisateurs. Si oui, préciser en particulier la finalité et la base légale de cette collecte.

3.4. Indiquer pour chaque catégorie de données collectées, quelles sont les finalités de la collecte et la base légale associée.

3.5. Dans le cas où la base légale est le consentement :

a. Indiquer comment est recueilli le consentement. Dans le cas où plusieurs modalités différentes de recueil du consentement existent, détailler chaque modalité de recueil du consentement.
b. Indiquer si l'organisme conserve une trace du consentement de l'utilisateur. Le cas échéant, préciser selon quelles modalités et si ce dernier est horodaté.
c. Indiquer quelles sont les conséquences pour la personne concernée du refus de donner son consentement.
d. Indiquer si les personnes concernées ont la possibilité de retirer leur consentement et selon quelles modalités. Le cas échéant, préciser quelles sont les conséquences pour la personne concernée si elle décide de retirer son consentement.

4. Les formalités mises en œuvre dans le cadre du traitement « COVI CONTACT »

4.1. Veuillez fournir une extraction du registre des activités de traitement liées à la mise en œuvre de « COVI CONTACT ».

4.2. Veuillez fournir la dernière version de l'analyse d'impact réalisée dans le cadre de la mise en œuvre de « COVI CONTACT ».

5. S'agissant des sous-traitants dans le cadre du traitement « COVI CONTACT »

5.1. Fournir, de façon exhaustive, la liste des sociétés ayant un accès/hébergeant des données à caractère personnel pour le compte de votre organisme.

5.2. Préciser, le cas échéant, si l'hébergeur a la qualité d'hébergeur de données de santé au sens du Code de la santé publique.

5.3. Indiquer, pour chaque sous-traitant mentionné, le cas échéant, toute mesure mise en œuvre par votre organisme afin de se conformer aux obligations de l'article 28 du RGPD (avenants, etc.).

5.4. Fournir, pour chacun des sous-traitants mentionnés, le contrat de sous-traitance conclu avec votre organisme.

6. Les données à caractère personnel collectées dans le cadre des traitements « COVI CONTACT »

6.1. Veuillez indiquer de manière exhaustive, pour chaque catégorie de personnes concernées, quelles sont les données enregistrées dans « COVI CONTACT » en précisant leur rôle.

6.2. Il conviendra de joindre également la liste des autres données enregistrées dans COVI CONTACT (qui ne sont pas déjà décrites ci-dessus) en précisant leur rôle dans le traitement concernant le l'activité de « *contact tracing* », par exemple les données concernant les utilisateurs du traitement « COVI CONTACT », les données relatives aux agents des Agences régionales de santé (ci-après « ARS »), etc.

7. L'information des personnes concernées dans le cadre des traitements « COVI CONTACT »

Veuillez indiquer, pour chaque catégorie de personne concernée (« patients zéro », « cas contacts » ou « contact à risque de contamination »...), de quelle manière elles sont informées du traitement de leurs données dans le cadre de « COVI CONTACT ». En ce sens, veuillez communiquer les supports d'informations fournies aux personnes concernées.

8. L'exercice des droits des personnes concernées dans le cadre des traitements « COVI CONTACT »

8.1. Indiquer le nombre de demandes qui ont été reçues et traitées depuis la mise en œuvre du traitement « COVI CONTACT » en distinguant par typologie de droits exercés (accès, opposition, effacement, portabilité, etc.).

8.2. Indiquer les mesures organisationnelles permettant de prendre en compte de façon effective les demandes d'exercice de droit, en précisant le cas échant si vous disposez d'un service dédié qui centralise les demandes.

9. Les durées de conservation

9.1. Indiquer la politique de conservation des données définie en distinguant, si nécessaire, selon les types et catégories de données et justifier de la finalité de chacune des durées de conservation définies.

9.2. Le cas échéant, fournir cette politique dans son intégralité.

9.3. Le cas échéant, indiquer comment cette politique de conservation de données est mise en œuvre, en précisant par exemple les moyens techniques (purge automatique, anonymisation des données, fréquence de déclenchement de la procédure de purge/anonymisation, etc.) mis en place. Fournir, le cas échéant, la copie du script de purge des données, du script d'anonymisation ou de tout autre élément permettant d'attester la suppression effective des données.

9.4. Préciser si les données font l'objet d'un archivage et si oui, détailler en quoi consiste cet archivage (cloisonnement logique et/ou physique) et les finalités de l'archivage.

9.5. 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. Veuillez préciser le nombre de personnes, par catégorie, dont les données ont été enregistrées à la date de réception du présent questionnaire.

9.6. Préciser les 50 plus anciennes fiches enregistrées dans la base « COVI CONTACT », avec leurs dates.

10. La sécurité des données

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

- localisation des serveurs et prestataires en charge de l'hébergement ; fournir, le cas échéant tout document contractuel encadrant la prestation d'hébergement ;
- modalité de stockage des mots de passe en base de données (algorithme utilisé) ;
- pseudonymisation et/ou anonymisation de données ; préciser le cas échéant, la liste des données concernées, la méthode et les algorithmes employés ;
- opérations faisant l'objet d'une procédure de traçabilité, contenu des fichiers journaux, hébergement, chiffrement éventuel et mesures garantissant l'intégrité et la confidentialité de ceux-ci.

10.2. Concernant les accès aux données, indiquer quelles mesures de sécurité sont mises en œuvre, en distinguant le cas échéant selon qu'il s'agisse des personnes ou des employés participant à la mise en œuvre des traitements 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…) ?
- Si un renouvellement des identifiants par l'utilisateur est permis, préciser les modalités de celui-ci.

10.3. Lister les catégories de personnes habilitées à accéder aux données collectées, que ce soit en lecture ou en écriture, en distinguant au besoin les données auxquelles peuvent accéder les différents profils d'utilisateurs (données complètes ou partielles, pseudonymisées ou non…).

Préciser pour chacun de ces accès la finalité de celui-ci.

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 09 JUIN 2021

N/Réf. : [redacted]**CS211051**
Par LRAR n° 2C 156 060 2963 8
À rappeler dans toute correspondance

Monsieur le Ministre,

Conformément à la décision n° 2020-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, le 4 février 2021, un contrôle sur place dans les locaux de l'agence régionale de santé Nouvelle-Aquitaine situés 103 bis rue Belleville à Bordeaux (33000) et le 17 mars 2021, un contrôle sur place dans les locaux de l'ARS Centre-Val de Loire situés Cité Coligny, 131 rue du faubourg Bannier à Orléans (45044).

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 « **CONTACT-COVID** », résultant de l'adaptation du système d'information « amelipro » 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.

Comme vous le savez, en application de l'article 1 du décret n° 2020-551 du 12 mai 2020 précité, la Caisse nationale de l'assurance maladie est responsable du traitement de données à caractère personnel « CONTACT-COVID ». Pour autant, chaque agence régionale de santé est responsable des traitements de données à caractère personnel qu'elle met en œuvre dans le cadre du « *tracing* » de niveau 3 du traitement « CONTACT COVID » et des traitements liés.

A cet égard, les ARS étant des établissements publics de l'État à caractère administratif placées sous la tutelle des ministres chargés de la santé, de l'assurance maladie, des personnes âgées et des personnes handicapées conformément à l'article L.1432-1 du Code de la santé publique, il m'apparaît utile de vous transmettre la mise en demeure non publique adressée à l'ARS Centre-Val de Loire ainsi que le courrier d'observation envoyé à l'ARS Nouvelle-Aquitaine clôturant la procédure de contrôle.

Compte tenu des constats figurant dans ce deux documents et dans le prolongement de votre courrier adressé à la CNIL le 13 février 2021, dans lequel vous indiquiez que votre ministère a mené différentes actions visant à rappeler aux ARS leurs obligations et à les accompagner dans leurs démarches de mise en conformité, je vous invite, en votre qualité de ministre de tutelle, à rappeler à **l'ensemble des ARS leurs obligations respectives** tant en vertu du RGPD qu'en vertu de l'article 11

de la loi n° 2020-546 du 11 mai 2020 de prorogation de l'état d'urgence sanitaire modifiée et du décret n° 2020-551 du 12 mai 2020.

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.

Bien à vous,

Marie-Laure DENIS

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

[redacted] adressée à l'ARS Centre-Val de Loire
PJ courrier de clôture avec observations adressé à l'ARS Nouvelle-Aquitaine.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

La Présidente

AGENCE RÉGIONALE DE SANTÉ
NOUVELLE AQUITAINE
Monsieur le Directeur Général
103 bis rue Belleville
33000 BORDEAUX

Paris, le 09 JUIN 2021

N/Réf. : [redacted]/DI211092
LRAR n° 2C 156 060 2965 2
À rappeler dans toute correspondance

Monsieur le Directeur général,

Conformément à la décision n° 2021-091C du 22 mai 2020, la Commission nationale de l'informatique et des libertés (CNIL) a effectué, le 4 février 2021, un contrôle sur place dans les locaux de l'agence régionale de santé Nouvelle-Aquitaine (ci-après « ARS NA ») situés 103 bis rue Belleville à Bordeaux (33000).

Ce contrôle avait 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 « **CONTACT-COVID** », résultant de l'adaptation du système d'information « amelipro » 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.

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 par l'ARS NA le 17 février 2021, me conduisent d'ores et déjà à vous faire part des observations suivantes.

Tout d'abord, je tiens à souligner la volonté de collaboration et de transparence des personnes rencontrées au sein de vos services, laquelle a permis la réalisation de ce contrôle dans de bonnes conditions, et ce, malgré le contexte sanitaire.

Toutefois, des corrections doivent encore être apportées sur les points listés ci-après.

À titre liminaire, il résulte des vérifications opérées que conformément à l'article 11 de la loi n° 2020-546 du 11 mai 2020 et à l'article 1 du décret n°2020-551 du 12 mai 2020, la Caisse nationale de l'assurance maladie est responsable du traitement de données à caractère personnel dénommé « CONTACT-COVID ».

Pour autant, conformément à la loi susmentionnée, et ainsi qu'il nous a été confirmé par vos services lors du contrôle du 4 février 2021, l'ARS NA est responsable des traitements de données qu'elle met en œuvre dans le cadre du « *contact tracing* » de niveau 3 en lien notamment avec le traitement « CONTACT COVID ».

La délégation a relevé que les tableaux de suivis des « clusters » ainsi que les exports de données de CONTACT COVID sont stockés dans un lecteur réseau hébergé par l'ARS NA.

L'accès à ce lecteur est réalisé par l'intermédiaire de la session WINDOWS des utilisateurs. L'authentification des utilisateurs à la session WINDOWS par l'ACTIVE DIRECTORY repose sur un mot de passe d'une longueur minimale de 8 caractères, dont au moins une lettre et un chiffre, sans contrainte supplémentaire.

Or, 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, pour satisfaire aux exigences de l'article 32 précité, il conviendra de mettre en œuvre une politique de gestion des mots de passe plus contraignante et d'obliger l'utilisateur à choisir un mot de passe robuste. Il est ainsi recommandé qu'il soit composé de 12 caractères minimum comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux. La complexité de ces mots de passe pourrait être réduite si des restrictions d'accès au compte sont mises en place. 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.

[redacted]

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

Marie-Laure DENIS

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