RÉGION AUVERGNE-
RHÔNE-ALPES

RECUEIL DES ACTES ADMINISTRATIFS SPÉCIAL N° 84-2020-065

PUBLIÉ LE 28 MAI 2020

Sommaire

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie Grenoble

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Arrêté SJC n° 2020-32 portant subdélégation de signature

La rectrice de l'académie de Grenoble,
par délégation du Préfet de l'Ardèche

Vu le décret n°2004-374 du 29 avril 2004 relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'Etat dans les régions et départements, et notamment en son article 43-11° ;

Vu les articles R222-19, R 222-19-3, D222-20 et R222-36-2 du code de l'éducation ;

Vu l'arrêté rectoral n°2016-52 du 25 novembre 2016 portant création du service mutualisé de contrôle de légalité des actes transmissibles des collèges de l'académie ;

Vu l'arrêté du préfet de l'Ardèche n°07-2020-02-11-001 portant délégation de signature à madame la rectrice de l'académie de Grenoble en matière de contrôle de légalité des actes des collèges de l'Ardèche, pris en date du 11 février 2020 ;

Vu le décret du 22 mai 2020 portant nomination de M. Pascal CLEMENT aux fonctions de directeur académique des services de l'éducation nationale de la Drôme ;

ARRETE

Article 1er : Subdélégation de signature est donnée à monsieur Pascal CLEMENT, directeur académique des services de l'éducation nationale (DASEN) de la Drôme, en tant que responsable du service mutualisé du contrôle de légalité des actes transmissibles des collèges de l'académie, à l'effet de signer au nom de la rectrice, délégataire du préfet de l'Ardèche, l'ensemble des actes afférant au contrôle de légalité des actes des collèges relevant du représentant de l'Etat dans le département de l'Ardèche.

Article 2 : Le DASEN de la Drôme subdélèguera, en vertu des articles R222-19-3, D222-20 et R222-36-2 du code de l'éducation, la présente signature à la secrétaire générale de la direction des services départementaux de l'éducation nationale de la Drôme et au chef du service mutualisé.

Article 3 : La secrétaire générale de l'académie est chargée de l'exécution du présent arrêté.

Article 4 : Le présent arrêté entre en vigueur à compter du 1er juin 2020. A cette même date, l'arrêté rectoral n°2020-26 du 15 mai 2020 portant subdélégation de signature est abrogé.
Le présent arrêté est publié au recueil des actes administratifs de la préfecture de la région Auvergne-Rhône-Alpes et au recueil des actes de la préfecture de l'Ardèche.

Fait à Grenoble le 26 mai 2020

Hélène Insel

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie Grenoble

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Arrêté SJC n° 2020-33 portant subdélégation de signature

La rectrice de l'académie de Grenoble,

Vu le décret n°2004-374 du 29 avril 2004 modifié relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'Etat dans les régions et départements, et notamment en son article 43-11° ;

Vu les articles R222-19, R 222-19-3, D222-20 et R222-36-2 du code de l'éducation ;

Vu l'arrêté rectoral n°2016-52 du 25 novembre 2016 portant création du service mutualisé de contrôle de légalité des actes transmissibles des collèges de l'académie ;

Vu l'arrêté du Préfet de la Drôme n°26-2020-02-13-004 portant délégation de signature à madame la rectrice de l'académie de Grenoble en matière de contrôle de légalité des actes des collèges de la Drôme, pris en date du 13 février 2020 ;

Vu le décret du 22 mai 2020 portant nomination de M. Pascal CLEMENT aux fonctions de directeur académique des services de l'éducation nationale de la Drôme ;

ARRETE

Article 1er : Subdélégation de signature est donnée à monsieur Pascal CLEMENT, directeur académique des services de l'éducation nationale (DASEN) de la Drôme, en tant que responsable du service mutualisé du contrôle de légalité des actes transmissibles des collèges de l'académie, à l'effet de signer au nom de la rectrice, délégataire du préfet de la Drôme, l'ensemble des actes afférant au contrôle de légalité des actes des collèges relevant du représentant de l'Etat dans le département de la Drôme.

Article 2 : Le DASEN de la Drôme subdélèguera, en vertu des articles R222-19-3, D222-20 et R222-36-2 du code de l'éducation, la présente signature à la secrétaire générale de la direction des services départementaux de l'éducation nationale de la Drôme et au chef du service mutualisé.

Article 3 : La secrétaire générale de l'académie est chargée de l'exécution du présent arrêté.

Article 4 : Le présent arrêté entre en vigueur à compter du 1er juin 2020. A cette même date, l'arrêté rectoral n°2020-27 du 15 mai 2020 portant subdélégation de signature est abrogé.
Le présent arrêté est publié au recueil des actes administratifs de la préfecture de la région Auvergne-Rhône-Alpes et au recueil des actes de la préfecture de la Drôme.

Fait à Grenoble le 26 mai 2020

Hélène Insel

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie Grenoble

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Arrêté SJC n° 2020-34 portant subdélégation de signature

La rectrice de l'académie de Grenoble,

Vu le décret n°2004-374 du 29 avril 2004 modifié relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'Etat dans les régions et départements, et notamment en son article 43 -11° ;

Vu les articles R222-19, R 222-19-3, D222-20 et R222-36-2 du code de l'éducation ;

Vu l'arrêté rectoral n°2016-52 du 25 novembre 2016 portant création du service mutualisé de contrôle de légalité des actes transmissibles des collèges de l'académie ;

Vu l'arrêté n°38-2020-02-12-006 du Préfet de l'Isère portant délégation de signature à madame la rectrice de l'académie de Grenoble en matière de contrôle de légalité des actes des collèges de l'Isère, pris en date du 12 février 2020 ;

Vu le décret du 22 mai 2020 portant nomination de M. Pascal CLEMENT aux fonctions de directeur académique des services de l'éducation nationale de la Drôme ;

ARRETE

Article 1er : Subdélégation de signature est donnée à monsieur Pascal CLEMENT, directeur académique des services de l'éducation nationale (DASEN) de la Drôme, en tant que responsable du service mutualisé du contrôle de légalité des actes transmissibles des collèges de l'académie, à l'effet de signer au nom de la rectrice, délégataire du préfet de l'Isère, l'ensemble des actes afférant au contrôle de légalité des actes des collèges relevant du représentant de l'Etat dans le département de l'Isère.

Article 2 : Le DASEN de la Drôme subdélèguera, en vertu des articles R222-19-3, D222-20 et R222-36-2 du code de l'éducation, la présente signature à la secrétaire générale de la direction des services départementaux de l'éducation nationale de la Drôme et au chef du service mutualisé.

Article 3 : La secrétaire générale de l'académie est chargée de l'exécution du présent arrêté.

Article 4 : Le présent arrêté entre en vigueur à compter du 1er juin 2020. A cette même date, l'arrêté rectoral n°2020-28 du 15 mai 2020 portant subdélégation de signature est abrogé.
Le présent arrêté est publié au recueil des actes administratifs de la préfecture de la région Auvergne-Rhône-Alpes et au recueil des actes de la préfecture de l'Isère.

Fait à Grenoble le 26 mai 2020

Hélène Insel

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie Grenoble

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Arrêté SJC n° 2020-35 portant subdélégation de signature

La rectrice de l'académie de Grenoble,

Vu le décret n°2004-374 du 29 avril 2004 modifié relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'Etat dans les régions et départements, et notamment en son article 43 -11° ;

Vu les articles R222-19, R 222-19-3, D222-20 et R222-36-2 du code de l'éducation ;

Vu l'arrêté rectoral n°2016-52 du 25 novembre 2016 portant création du service mutualisé de contrôle de légalité des actes transmissibles des collèges de l'académie ;

Vu l'arrêté SCPP-PCIT 05.2020 du Préfet de la Savoie portant délégation de signature à madame la rectrice de l'académie de Grenoble, en matière de contrôle de légalité des actes des collèges de la Savoie, pris en date du 17 février 2020;

Vu le décret du 22 mai 2020 portant nomination de M. Pascal CLEMENT aux fonctions de directeur académique des services de l'éducation nationale de la Drôme ;

ARRETE

Article 1er : Subdélégation de signature est donnée à monsieur Pascal CLEMENT, directeur académique des services de l'éducation nationale (DASEN) de la Drôme, en tant que responsable du service mutualisé du contrôle de légalité des actes transmissibles des collèges de l'académie, à l'effet de signer au nom de la rectrice, délégataire du préfet de la Savoie, l'ensemble des actes afférant au contrôle de légalité des actes des collèges relevant du représentant de l'Etat dans le département de la Savoie.

Article 2 : Le DASEN de la Drôme subdélèguera, en vertu des articles R222-19-3, D222-20 et R222-36-2 du code de l'éducation, la présente signature à la secrétaire générale de la direction des services départementaux de l'éducation nationale de la Drôme et au chef du service mutualisé.

Article 3 : La secrétaire générale de l'académie est chargée de l'exécution du présent arrêté.

Article 4 : Le présent arrêté entre en vigueur à compter du 1er juin 2020. A cette même date, l'arrêté rectoral n°2020-29 du 15 mai 2020 portant subdélégation de signature est abrogé.
Le présent arrêté est publié au recueil des actes administratifs de la préfecture de la région Auvergne-Rhône-Alpes et au recueil des actes de la préfecture de la Savoie.

Fait à Grenoble le 26 mai 2020

Hélène Insel

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie Grenoble

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Arrêté SJC n° 2020-36 portant subdélégation de signature

La rectrice de l'académie de Grenoble,

Vu le décret n°2004-374 du 29 avril 2004 modifié relatif aux pouvoirs des préfets, à l'organisation et à l'action des services de l'Etat dans les régions et départements, et notamment en son article 43 -11° ;

Vu les articles R222-19, R 222-19-3, D222-20 et R222-36-2 du code de l'éducation ;

Vu l'arrêté rectoral n°2016-52 du 25 novembre 2016 portant création du service mutualisé de contrôle de légalité des actes transmissibles des collèges de l'académie ;

Vu l'arrêté BOA n° 2020-012 du Préfet de la Haute-Savoie portant délégation de signature à madame la rectrice de l'académie de Grenoble en matière de contrôle de légalité des actes des collèges de la Haute-Savoie, pris en date du 10 février 2020;

Vu le décret du 22 mai 2020 portant nomination de M. Pascal CLEMENT aux fonctions de directeur académique des services de l'éducation nationale de la Drôme ;

ARRETE

Article 1er : Subdélégation de signature est donnée à monsieur Pascal CLEMENT, directeur académique des services de l'éducation nationale (DASEN) de la Drôme, en tant que responsable du service mutualisé du contrôle de légalité des actes transmissibles des collèges de l'académie, à l'effet de signer au nom de la rectrice, délégataire du préfet de la Haute-Savoie, l'ensemble des actes afférant au contrôle de légalité des actes des collèges relevant du représentant de l'Etat dans le département de la Haute-Savoie.

Article 2 : Le DASEN de la Drôme subdélèguera, en vertu des articles R222-19-3, D222-20 et R222-36-2 du code de l'éducation, la présente signature à la secrétaire générale de la direction des services départementaux de l'éducation nationale de la Drôme et au chef du service mutualisé.

Article 3 : La secrétaire générale de l'académie est chargée de l'exécution du présent arrêté.

Article 4 : Le présent arrêté entre en vigueur à compter du 1er juin 2020. A cette même date, l'arrêté rectoral n°2020-30 du 15 mai 2020 portant subdélégation de signature est abrogé.
Le présent arrêté est publié au recueil des actes administratifs de la préfecture de la région Auvergne-Rhône-Alpes et au recueil des actes de la préfecture de la Haute-Savoie.

Fait à Grenoble le 26 mai 2020

Hélène INSEL

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

académie Grenoble

RÉGION ACADÉMIQUE
AUVERGNE-RHÔNE-ALPES

MINISTÈRE
DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

MINISTÈRE
DE L'ENSEIGNEMENT SUPÉRIEUR,
DE LA RECHERCHE
ET DE L'INNOVATION

Arrêté SJC n°2020-37

LA RECTRICE DE L'ACADEMIE DE GRENOBLE

Vu le code de l'éducation en son article R421-62 ;

Vu la note de service ministérielle n°2008-110 du 22 août 2008 portant réforme de la carte des agences comptables des EPLE ;

Vu l'arrêté rectoral SG n°2019-21 du 15 juillet 2019 portant carte des groupements comptables dans l'académie de Grenoble à la rentrée 2019 ;

Vu la consultation du Comité Technique Académique réuni le 25 mars 2020 ;

Vu l'arrêté préfectoral 38-2020-05-19-005 du 19 mai 2020 portant création de l'établissement public local d'enseignement « collège de Champier » (RNE n° 0383542U) ;

ARRETE

Article 1er : La carte des groupements comptables dans l'académie de Grenoble mentionnée dans l'arrêté rectoral du 15 juillet 2019 susvisé, est modifiée comme suit à compter du 1er juin 2020 :

ISERE

Etablissement siège	**Etablissements rattachés**	**Commune - département**
Lycée Hector Berlioz		**La Côte St André (38)**
	Clg Jongkind	La Côte St André (38)
	Clg M. Mariotte	St Siméon de Bressieux (38)
	Clg J. Brel	Beaurepaire (38)
	Clg Liers et Lemps	Le Grand Lemps (38)
	Clg R. Valland	St Etienne de St Geoirs (38)
	Clg de Champier	Champier (38)

Article 2 : La secrétaire générale de l'académie est chargée de l'exécution du présent arrêté.

Article 3 : Le présent arrêté est publié au recueil des actes administratifs de la préfecture de la région Auvergne-Rhône-Alpes.

Fait à Grenoble le 26 mai 2020

Hélène Insel

Décision n° 2020-13-0024
Annexe n° 01

Agence Régionale de Santé Auvergne-Rhône-Alpes

DRAPAGE
DRoits APplicatifs des AGEnts

SORMAS

Liste des agents habilités

		Nom du profil	Acces donné par :	Le
ALLARD	Cécile			
		Superviseur de surveillance	*rboiron*	*20/05/2020*
AUGUSTE	Emmanuel			
		Agent de surveillance	*rboiron*	*20/05/2020*
BAO	Alassane			
		Agent de surveillance		*19/05/2020*
		Superviseur de surveillance	*aliardet*	*19/05/2020*
BARDOT	Blandine			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
BELMONTE	Pascale			
		Superviseur de surveillance		*20/05/2020*
BERTHO-FERNAN	Martine			
		Superviseur de surveillance	*aliardet*	*18/05/2020*
BERTRAND	Patricia			
		Agent de surveillance	*aliardet*	*19/05/2020*
BLANCHIN	Martine			
		Superviseur de surveillance	*rboiron*	*11/05/2020*
BLANC-LEFORT	Françoise			
		Agent de surveillance	*aliardet*	*19/05/2020*
BOIRON	Romain			
		Admin	*rboiron*	*11/05/2020*
CARBONE	Sarah			
		Superviseur de surveillance	*aliardet*	*20/05/2020*
CHAMPAVIER	Régis			
		Superviseur de surveillance	*aliardet*	*20/05/2020*
CLAPSON	André-Claude			
		Admin	*rboiron*	*11/05/2020*
COQUELIN	Magali			
		Superviseur de contact	*aliardet*	*18/05/2020*
		Superviseur de surveillance	*aliardet*	*18/05/2020*
DJEBAILI	Samia			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
GIRARDI	Amélie			
		Superviseur de surveillance	*aliardet*	*20/05/2020*
GUYOT-PACINI	Florence			
		Superviseur de surveillance	*aliardet*	*20/05/2020*
IMBERT	Natasa			
		Superviseur de surveillance	*aliardet*	*19/05/2020*

		Nom du profil	Acces donné par :	Le
JAVELET	Elisa			
		Superviseur de surveillance	*aliardet*	*20/05/2020*
LE	Viviane-Thanh			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
LE CALLOCH	Julie			
		Agent de surveillance	*rboiron*	*20/05/2020*
LIARDET	Anne			
		Admin	*rboiron*	*11/05/2020*
LOISY	Sophie			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
LUSTIERE	Catherine			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
MAMERT	Yohann			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
MICHEL	Marie			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
NATIVEL	Michèle			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
RASTOLL	Françoise			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
ROMAGGI	Brigitte			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
RONGIER	Alexandre			
		Superviseur de surveillance	*aliardet*	*19/05/2020*
RONNAUX-BARON	Anne-Sophie			
		Superviseur de surveillance	*rboiron*	*11/05/2020*
STENEGRE	Julien			
		Superviseur de contact	*aliardet*	*18/05/2020*
		Superviseur de surveillance	*aliardet*	*18/05/2020*
TCHINDA-DJOU	Youri			
		Admin	*aliardet*	*18/05/2020*
VANDROUX	Isabelle			
		Superviseur de surveillance	*aliardet*	*19/05/2020*

Le Directeur Général
Docteur Jean-Yves GRALL

Le Directeur Général
de l'Agence Régionale de Santé Auvergne-Rhône-Alpes

Docteur Jean-Yves GRALL

L'Assurance Maladie HAUTE-LOIRE	**Accès Tiers** **Au téléservice Contact Covid de la CPAM** **Convention de Service**	ars Agence Régionale de Santé Auvergne-Rhône-Alpes

Entre : La Caisse Primaire d'Assurance Maladie de [département],

Ci-après dénommée « la CPAM »

Et : La Délégation Départementale de .....de l'Agence Régionale de Santé,
Ci-après dénommée « le tiers accédant »

Il a été convenu et arrêté ce qui suit :

Préambule
Le diagnostic de cas d'infection respiratoire aigüe coronavirus (2019-nCoV / Covid 19) sur le territoire français a conduit les pouvoirs publics à prendre des mesures exceptionnelles adaptées à chaque stade de l'épidémie.

Pour accompagner la fin du confinement annoncée au 11 mai, l'Etat a prévu la mise en place de nouvelles mesures permettant de limiter la propagation du virus, reposant principalement sur trois piliers :

- la mise à disposition en quantité conséquente de tests de dépistage permettant d'assurer un dépistage systématique sur tout le territoire des patients symptomatiques et des personnes ayant été en contact rapproché avec une personne détectée positive ;
- la mise en place d'un dispositif réactif de suivi des patients détectés positif au Covid19 et d'identification, de contact et de suivi des personnes ayant été en contact avec elle par le biais d'enquêtes sanitaires conduites par les médecins généralistes, l'Assurance Maladie et les Agences Régionales de Santé (ARS) ;
- la mise à l'isolement (quatorzaine) des personnes concernées.

La loi d'urgence sanitaire modifiée et le Décret en Conseil d'Etat visé en son article 6 confient notamment à la Caisse Nationale d'Assurance Maladie la responsabilité d'un traitement dénommé « Contact Covid » permettant :

- 1° l'identification des personnes infectées, par la prescription et la réalisation des examens de biologie ou d'imagerie médicale pertinents ainsi que par la collecte de leurs résultats, y compris non positifs, ou par la transmission des éléments probants de diagnostic clinique susceptibles de caractériser l'infection ;
- 2° l'identification des personnes présentant un risque d'infection, par la collecte des informations relatives aux contacts des personnes infectées et, le cas échéant, par la réalisation d'enquêtes sanitaires, en présence notamment de cas groupés ;
- 3° L'orientation des personnes infectées, et des personnes susceptibles de l'être, en fonction de leur situation, vers des prescriptions médicales d'isolement prophylactiques, ainsi que le suivi médical et l'accompagnement de ces personnes pendant et après la fin de ces mesures.

Ces textes permettent notamment à l'Assurance Maladie de déléguer la réalisation de cette mission à des tiers dans la stricte limite des personnes identifiées par les textes susvisés.

Ainsi, les vocations respectives de la CPAM et du tiers accédant les conduisent à permettre l'accès à Contact Covid et donc aux informations nécessaires à l'accomplissement de leurs missions

Article 1 : Objet de la convention

La convention encadre l'autorisation d'accès à Contact Covid donné par la CPAM au tiers accédant.

Article 2 : Accès au service

La CPAM, via son service informatique, met à disposition du tiers accédant les équipements permettant d'accéder au réseau de l'Assurance Maladie, ainsi que les cartes d'identification nécessaires à leur fonctionnement et présentés en annexe 3.
Pour ce faire, le tiers accédant doit adresser à la Direction de la CPAM des demandes d'habilitations nominatives aux agents (cf. le formulaire présenté en annexe 1).

En cas de changement, le tiers accédant actualise en tant que de besoin et au fil de l'eau la liste des agents habilités sous sa responsabilité.

Article 3 : Engagement des parties et protection des données

Les Parties à la présente convention s'engagent à respecter, en ce qui les concerne, les dispositions 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 et celles de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Pour le traitement de données personnelles visé par cet accord, les parties s'engagent à se conformer strictement au RGPD, qui s'appliquera en toute circonstance, nonobstant toute éventuelle stipulation contraire.

3.1 Responsabilité des parties dans l'échange des données

La présente convention place le tiers accédant dans une situation de sous-traitance, au sens du RGPD. Cette sous-traitance porte uniquement sur la partie relative à l'accès aux données via le téléservice mentionné dans la présente convention.

Chaque des parties, s'engage à communiquer les coordonnées de contact de son délégué à la protection des données (DPO) si ces dernières sont tenues d'en désigner un selon les termes de l'article 37 du RGPD et à tenir à jour la documentation nécessaire à la preuve de la conformité du traitement (registre des traitements, documentation nécessaire à la preuve de la conformité).

3.2 Engagement de chacune des parties

La CPAM s'engage à :

- ne permettre l'accès au tiers accédant qu'aux seules données prévues par la présente convention ;
- prévoir une information des personnes précisant le ou les éventuels destinataires et à répondre aux demandes de droit d'accès, de rectification et d'opposition des personnes concernées ;
- octroyer les habilitations circonscrites au téléservice Contact covid (annexe 2 de la présente convention) pour permettre aux agents du tiers accédant d'accomplir leurs missions.

Le tiers accédant s'engage à :

- prendre l'ensemble des mesures nécessaires afin que les équipements ne soient utilisés que par les agents habilités et uniquement pour accéder aux données des dossiers qu'ils ont à traiter ;
- à désigner uniquement des personnes disposant d'une compétence leur permettant d'accomplir ces missions (notamment la maitrise de la relation au public et la pratique des données sensibles). Ceci exclut donc notamment le personnel intérimaire et étudiant ;
- à respecter les modes opératoires émis par la CPAM notamment concernant le principe de confidentialité et l'exercice des droits des personnes concernées ;
- respecter la finalité de traitement pour laquelle l'accès aux données est nécessaire. Toute autre utilisation des données pour une autre finalité restera de la responsabilité propre de chacune des Parties (détournement de finalité) ;

- garantir la confidentialité des données à caractère personnel ;
- à tenir informée la CPAM en cas de suspicion ou de violation de données avérée lors de l'accès aux données. A cet effet, il reviendra à la CPAM de prendre toute décision utile quant à la notification auprès des autorités compétentes et à l'obligation d'informer les personnes en cas de risque élevé sur la vie privée.

Article 4 : Sécurité et confidentialité

Le tiers accédant s'engage à respecter et à faire respecter par ses agents :

- la charte informatique objet de l'annexe 4 de la présente convention ;

- les règles de confidentialité : elle s'engage, en conséquence, à prendre l'ensemble des mesures nécessaires afin qu'aucune information issue du téléservice ne soit divulguée à des tiers hormis aux personnes concernées devant être accompagnés. S'agissant des personnes concernées, la transmission d'information ne devra être réalisée que dans le cadre stricte d'un accompagnement individuel et en complémentarité des services de la CPAM.

Article 5 : Fin de mission

Le tiers accédant s'engage à :

- signaler à la CPAM toute fin de mission concernant les agents habilités dès *la fin de leur mission* afin que la CPAM supprime les accès ;

- récupérer et restituer à la CPAM les cartes d'identification ayant été mises à la disposition des agents habilités ;

- rappeler aux agents que :
  - conformément à l'article 226-22 du Code pénal : « le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité à les recevoir » est passible de sanction ;
  - l'obligation du respect du secret professionnel perdure au-delà du terme du contrat.

Article 6 : Durée et résiliation de la convention

La présente convention prend effet pour la durée prévue par les textes mentionnés au préambule à compter de la date de la signature.

En cas de manquement aux obligations suscitées, chacune des parties pourra être dénoncée la présente convention deux mois avant l'échéance par lettre recommandée.

Fait en double exemplaire, à ....., le 11 mai 2020

Le Directeur
de la CPAM

Le Directeur Départemental
de la DD ARS de .....,

Annexe 1

Demande de création ou de suppression des droits d'accès

Nom	Prénom	Date de suppression des droits	Accès aux locaux de la CPAM

Le Directeur de la structure s'engage à mettre à jour la liste et à la communiquer à la CPAM.

Fait à ....., le 11 mai 2020

Annexe 2

Liste des applicatifs mis à disposition

Téléservice CONTACT COVID :

- Ecriture
- Consultation

Fait à ....., le 11 mai 2020

Le Directeur,
de la CPAM

Accès de
La délégation territoriale de l'Agence Régionale de Santé [Département]
au système d'information
de la CPAM [Département]
Convention de Service

Annexe 3

Liste des équipements mis à disposition

CPAM de ..... :

- Unité centrale fixe complet (souris clavier)
- Ecran de marque LG Etiquette

Fait à ....., le 11 mai 2020

Pour l'organisme

Le Directeur
de la CPAM

Décision n° 2020-23-0023

Annexe n° 02

VALIDE AU 31/05/2023

18 MAI 2020

Le Directeur Général

Docteur Jean-Yves GRALL

l'Assurance Maladie
Caisse Nationale

Charte informatique de l'Assurance Maladie

1. Préambule

L'organisme met à la disposition des utilisateurs, dans le cadre de leur activité professionnelle, des ressources informatiques et de communication électronique, dont l'usage est source de responsabilité.
Il est important de rappeler que le statut des personnels de l'organisme ne protège en aucune manière l'utilisateur d'une mise en cause de sa responsabilité civile ou pénale en cas d'utilisation illicite de ces moyens.

Compte tenu de la présomption de caractère professionnel des données présentes sur le poste de travail, la présente charte vise à informer et sensibiliser chaque salarié de l'Assurance Maladie sur ses droits et obligations dans l'usage des Technologies et l'Information et la Communication (TIC).

L'usage correct des ressources informatiques et de communication électronique permet de garantir l'intégrité et la disponibilité du système d'information pour une utilisation conforme à son objet.
Il participe au respect du secret professionnel (et/ou médical), et de la confidentialité des données.
Enfin, il permet de préserver l'image de marque de l'organisme en évitant de porter atteinte à sa réputation.

2. Champ d'application de la Charte

La présente charte s'applique à l'outil professionnel que constitue le Système d'Information de l'organisme et à l'infrastructure associée.

L'organisme est responsable de toutes les ressources mises à disposition des utilisateurs :

- les équipements informatiques (stations de travail, ordinateurs portables, serveurs, équipements réseaux,...),
- les logiciels et leurs mises à jour conformes aux préconisations Cnamts et répondant aux exigences de sécurité,
- les moyens de communication (téléphone, smartphone, messageries électronique et instantanée, Internet, Visio conférence, accès à distance tel que le télétravail, ...),
- les fichiers, informations, données...,
- les périphériques externes (Imprimantes, Scanner, Fax, les supports de stockage type clés USB, ...).

Cette charte s'applique aux usages du Système d'Information dans et en dehors des locaux de l'organisme (nomadisme, télétravail).

Toute ressource ou moyen de communication utilisé à des fins professionnelles mais appartenant aux utilisateurs est interdit, sauf dérogation obtenue auprès de la Direction et validée par la Direction des Systèmes d'Information.

2.1. Personnes concernées

Les obligations décrites dans la présente charte s'appliquent de droit aux utilisateurs de l'Assurance Maladie et assimilés mais aussi, à titre exceptionnel, aux tiers accédants qui doivent utiliser le système d'information mis à leur disposition.

Les utilisateurs : Agents de l'assurance maladie amenés à créer, consulter, modifier et/ou mettre en œuvre les ressources informatiques et de communication électronique.

Les personnels assimilés : personnes en situation de mise à disposition ou détachement dans l'Assurance Maladie.

Les administrateurs : Agents de l'assurance Maladie pour lesquels il convient de se référer aux conditions d'utilisation des droits administrateur imposés par le Système d'information de l'Assurance Maladie.

A titre exceptionnel, les tiers d'entités extérieurs à l'organisme (prestataires notamment) qui peuvent avoir accès aux ressources informatiques et de communication électronique ou traiter des informations extraites du système d'information.

2.2. Diffusion

La diffusion de la charte sera réalisée par voie de note de service après modification du Règlement Intérieur pour ce qui concerne les organismes du réseau.

3. Règles d'utilisation du Système d'Information

3.1. Règles générales

Les ressources informatiques et moyens de communication électronique mis à disposition des utilisateurs doivent être utilisés dans la stricte application de la charte.
Toute modification de la ressource ou d'un élément du SI ne peut être réalisée que par du personnel habilité.

Les utilisateurs du SI doivent être vigilants par rapport à la sécurisation des équipements qui leur sont confiés.

L'utilisation des ressources informatiques et des moyens de communication électronique est limitée à un usage professionnel.

3.2. Utilisation privée résiduelle et nommage des données privées

L'utilisation des moyens de communication électroniques (messagerie et Internet) à titre privé est tolérée dans le cadre d'un usage raisonnable.

Dans tous les cas, l'utilisateur doit supprimer toute mention relative à l'employeur ou indication qui pourrait laisser croire que le message est rédigé dans le cadre de son exercice professionnel.

L'Organisme ne pourra prendre connaissance du contenu des messages privés, à la condition que ceux-ci soient clairement identifiés comme tels et sous réserve des dispositions de l'article 33.

L'Organisme se réserve la possibilité de se retourner contre l'utilisateur si sa responsabilité venait à être engagée.

La participation à un service de type communautaire, en particulier forums, réseaux sociaux… est interdite, sauf autorisation expresse de la Direction.

L'utilisateur peut stocker des données privées dans un répertoire nommé « PERSONNEL» en veillant toutefois à ce que la taille du dossier reste dans les limites d'une volumétrie raisonnable et qu'il ne comporte pas de données professionnelles.

En cas d'abus, l'organisme se réserve le droit de prendre toute sanction appropriée.

3.3. Droits d'accès aux données

Les dossiers, fichiers y compris sur supports amovibles (même personnels) créés par un salarié grâce à l'ordinateur mis à sa disposition par son employeur pour l'exécution de son contrat de travail sont présumés avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors de sa présence, sauf si le salarié les a identifiés comme étant personnels.

L'employeur n'est autorisé à accéder aux fichiers personnels de ses salariés que par une décision de justice ou par une autorité habilitée (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes, etc.) ou en présence d'un risque avéré en termes notamment de sécurité, de continuité de service, d'un risque grave de voir sa responsabilité engagée, ou en cas de suspicion d'acte malveillant pouvant impacter le SI. Les modalités et les circonstances d'accès ainsi que les données accédées sont notifiées par écrit au salarié.

Les connexions internet établies par un salarié sur des sites internet pendant son temps de travail sont également présumées avoir un caractère professionnel.

Les courriels adressés ou reçus par le salarié à l'aide de l'outil informatique mis à sa disposition par l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel en sorte que l'employeur est en droit de les ouvrir hors la présence de l'intéressé sauf s'ils sont identifiés comme personnels

Les conditions d'accès par l'employeur à la messagerie électronique professionnelle des agents sont précisées dans la Charte de messagerie.

4. Attribution et retraits du droit d'accès au Système d'Information

4.1. Attribution

Chaque utilisateur reçoit un droit d'accès individuel, personnel et confidentiel qui se matérialise par une carte agent avec un code PIN et parfois des identifiants et mots de passe qui ne doivent pas être communiqués.

La carte agent doit faire l'objet d'une attention particulière dans le cadre de l'activité professionnelle.

A ce titre, elle ne doit donc pas être prêtée à un tiers et elle doit être systématiquement enlevée du lecteur en cas d'absence, même momentanée.

L'utilisateur s'engage à respecter la politique de gestion des mots de passe (changement régulier, complexité…) énoncée au niveau national.

Celui-ci devra donc signaler à son responsable, la perte ou le vol de sa carte de même que tout événement faisant suspecter un usage frauduleux, afin de dégager sa responsabilité.

La protection de ces moyens est placée sous la responsabilité de l'utilisateur, qui reconnaît que l'usage de son droit d'accès peut engager sa responsabilité.

L'identifiant est strictement confidentiel. Cela emporte pour conséquence que l'accès aux ressources informatiques et de communication électronique via cet identifiant est réputé avoir été réalisé par le titulaire, qui devra donc assumer la responsabilité d'usage non conforme, sauf à démontrer avoir demandé, préalablement, une suspension ou une suppression de son droit d'accès.

L'utilisateur ne doit accéder qu'aux seules informations nécessaires à son activité professionnelle au titre du «besoin d'en connaître».

Il est interdit d'user, par quelque moyen que ce soit, de l'identité et du droit d'accès d'un autre utilisateur.

4.2. Gestion des absences

En cas d'absence prolongée, l'organisme « suspend » le droit d'usage et/ou d'accès d'un utilisateur.

Pour des raisons de service, la Direction de l'organisme se réserve le droit d'accéder directement aux fichiers et/ou messages professionnels (cf. Modalités d'accès aux données au §3.3).

4.3. Gestion des départs

Au moment de son départ de l'organisme, il appartient à l'utilisateur de :

- détruire son répertoire « PERSONNEL ›› et tous les messages de nature privée,
- restituer l'ensemble des informations professionnelles, des moyens d'accès informatiques et de communications électroniques, y compris les matériels nomades, selon la procédure nationale de sortie du personnel.

A son départ, l'utilisateur perd tout droit d'accès au système d'information.

5. La protection du Système d'Information

5.1. Protection des ressources et des informations

L'utilisateur doit systématiquement verrouiller son poste de travail en cas d'absence, même momentanée.

L'utilisateur doit veiller à ce que des informations sensibles ne soient pas affichées sur son écran, en son absence.

Les utilisateurs doivent signaler tout incident de sécurité, toute suspicion de compromission d'une information, toute tentative d'intrusion extérieure sur le SI, de falsification, d'usurpation de droit ou de présence de virus selon les modalités décrites dans la procédure nationale de gestion des incidents de sécurité.

L'utilisateur ne doit pas, sauf autorisation préalable de la Direction de l'organisme :

- communiquer à des tiers toute information du système d'information,
- modifier les configurations informatiques,
- déroger aux consignes d'utilisation des outils informatiques,
- désactiver ou contourner le dispositif technique de sécurité.

5.2. Virus informatiques et autres événements malveillants

Le poste de travail est équipé d'un logiciel antivirus et d'autres dispositifs de lutte contre la malveillance dont le paramétrage ne doit pas être modifié.
De plus, son fonctionnement ne doit pas être entravé ou arrêté.
L'utilisation des applications communicantes (navigateur Internet et messagerie en particulier) et des supports de stockage externes peut provoquer la transmission et l'installation, de programmes ou de fichiers, qui altèrent ou suppriment les données et logiciels du poste.
Si un utilisateur suspecte ou constate un dysfonctionnement de l'anti-virus sur son PMF, il doit cesser toute activité sur le poste et avertir le service informatique.

5.3. Utilisation des supports amovibles

Il existe de nombreux supports informatiques amovibles capables de se connecter aux ordinateurs : clés USB, CD-ROM, baladeurs numériques, mémoires flash, appareils photos, assistants personnels numériques, clés U3, téléphones, smart phones, tablettes…

Ces supports présentent un risque pour le système d'information car ils peuvent contenir des logiciels malveillants (virus, logiciels espions, logiciels de prise de contrôle à distance).
Par conséquent, la connexion de supports amovibles personnels à un PMF de l'Assurance Maladie est interdite.

Toutefois, l'utilisation de supports amovibles professionnels est tolérée sous certaines conditions :

- le support est fourni par l'organisme (ou par les circuits de la Diffusion Nationale), ou son utilisation a obtenu l'accord de la fonction sécurité de l'organisme (RSSI ou MSSI),
- le support est apporté par un représentant d'un autre organisme de l'Assurance maladie ou un tiers habilité et doit être utilisé par nécessité de service.

Recommandations d'utilisation de supports amovibles

- Faire un examen systématique à l'antivirus lors de l'utilisation d'un support amovible.
- Procéder au chiffrement des données sensibles.
- Sauvegarder les documents nécessaires dans un espace sécurisé après chaque utilisation.

- Effacer les données et déconnecter le support du PMF.

Toute connexion de supports amovibles extérieurs, à l'organisme, est interdite sur le poste de travail.
Toutefois, si la connexion est indispensable pour des raisons de service, il convient de prendre les précautions complémentaires suivantes :

- Ne jamais utiliser de support amovible dont l'origine ne peut être garantie.
- Ne pas double-cliquer sur les documents, mais les ouvrir à partir des logiciels de son PMF (par exemple : exécuter Word puis menu fichier/ouvrir un fichier Word sur la clé),
- Ne pas exécuter de logiciels situés sur le support (.exe, .jar, .bat etc.), et de manière générale ne pas double-cliquer sur des fichiers inconnus ni les importer sur le PMF.

Dans tous les cas il convient d'être prudent et vigilant, de signaler tout incident ou anomalie et ne pas hésiter à se rapprocher du service informatique de l'organisme pour connaître la conduite à tenir.

5.4. Chiffrement

La transmission en interne ou en externe de données sensibles (données classées « secret » et « confidentiel ») doit impérativement répondre aux préconisations de la LR-DDO-214/2013 portant sur la « Classification des informations ».
L'utilisation d'outils de chiffrement est encadrée par le service informatique et le MSSI de l'organisme.

6. Utilisation des moyens de communication messagerie, Intranet, Internet

6.1. La messagerie

Elle fait l'objet d'une charte spécifique qui définit les droits et obligations que l'organisme et l'utilisateur s'engagent à respecter, notamment les conditions de contrôles portant sur l'utilisation de la messagerie électronique ainsi que le cadre légal dans lequel s'inscrit son usage.

Elle précise les sanctions prévues en cas de non respect des règles établies.
Elle est complétée d'un guide de bonnes pratiques auquel chaque utilisateur doit se référer.

6.2. Intranet

L'organisme met à la disposition de chaque agent un site Intranet avec les informations et services nécessaires à l'exercice de son activité (réglementation liée aux règlements des prestations, circulaires, modes opératoires, processus qualité, information assurés, SSI,…) et à la vie dans l'entreprise (projet d'entreprise, actualités, vacances de poste, réservation de salles en ligne...).
Il s'agit d'un outil d'information et de travail.

Les responsabilités et les engagements de chaque agent avec l'Intranet sont les suivants :

- Les informations en ligne doivent être utilisées à des fins professionnelles et ne pas être divulguées ni diffusées à des tiers non autorisés,
- L'enregistrement pour modification et diffusion interne ou externe de documents ou d'informations présents dans l'Intranet est interdit sans autorisation de la Direction,
- Les contributions à caractère diffamatoire, discriminatoire ou incorrect sont interdites.

6.3. Internet

L'Internet est un espace à risques dans lequel sont présentes de nombreuses sources de menaces pouvant porter atteinte à l'organisme mais également à la vie privée de l'utilisateur.
La loi précise que « la sécurité est un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives ».
L'obligation de protection de ses personnels pesant sur l'organisme justifie les règles de conduite et les interdictions édictées par la charte d'utilisation du système d'information.

L'accès à Internet est soumis à autorisation pour l'ensemble des utilisateurs.
Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle.
La Direction du Système d'Information, s'autorise le droit d'opérer tout filtrage nécessaire pour protéger le système d'information, garantir la disponibilité du réseau informatique et respecter la législation en vigueur.

De par le droit du travail, l'utilisateur ne doit pas accomplir d'opérations susceptibles de représenter un manquement aux obligations professionnelles ou à la préservation des ressources informatiques mises à sa disposition comme :

- la consultation, l'importation, la diffusion et l'exploitation d'informations de nature à porter atteinte individuellement ou collectivement au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,
- le téléchargement, l'installation/exécution de scripts, de logiciels ou de programmes informatiques sans autorisation préalable de la Direction,
- le téléchargement, la diffusion ou l'impression de données dont les volumes et/ou les fréquences d'usage risquent de mettre en danger l'intégrité et/ou la disponibilité du réseau,
- le téléchargement, la consultation ou la copie à partir d'un site illicite (sites à caractère pornographique, pédophile, négationniste, extrémiste, raciste, xénophobe, violent ou contraire aux bonnes mœurs ou à l'ordre public…) qui revêt le caractère d'une infraction pénale,
- la communication d'informations appartenant au patrimoine informationnel de l'Assurance Maladie sans autorisation préalable,
- le raccordement au poste de travail d'un matériel externe non professionnel ayant sa propre connectique à l'Internet (risque de rebond),
- la communication de l'adresse de messagerie professionnelle en dehors des sites Internet de confiance. Il est rappelé que les utilisateurs et les services des organismes de l'Assurance Maladie utilisent une adresse de type @xxx-organisme.cnamts.fr (exemple: eric.dupont@cpam-paris.cnamts.fr), qui est une signature institutionnelle susceptible, dans les rapports avec les tiers, d'engager la responsabilité civile et pénale des organismes et de leurs représentants.

La reproduction d'objets issus de sites Internet, (textes, images, sons) n'est possible que dans la mesure où ils sont libres de droits et diffusés avec l'autorisation de leurs auteurs, et avec indication de leur source, conformément aux lois en vigueur.
En effet, en vertu des règles du Code de la propriété intellectuelle, l'auteur d'une oeuvre de l'esprit originale jouit, sur cette oeuvre, du seul fait de sa création, "d'un droit de propriété incorporel et exclusif opposable à tous".

La consultation, pour un motif personnel, est tolérée dans la mesure où celle-ci est exceptionnelle et raisonnable et lorsque le contenu n'est contraire à aucune des prescriptions de cette charte.

La participation des utilisateurs à un service de type communautaire, forums, réseaux sociaux…, est interdite à partir du poste de travail, sauf autorisation expresse de la Direction.

Les connexions Internet font l'objet de supervisions, de vérifications et d'audits réguliers selon des directives définies au niveau national.
Les identifiants et les adresses de connexion sont ainsi enregistrés.
L'historique constitué permet de retracer le trafic Internet et peut être exploité par la Direction à des fins de statistiques, de qualité de service et de sécurité, pour vérifier :

- les durées des connexions
- et les sites les plus visités

Les traces seront conservées pendant une durée maximale de 6 mois, sauf si des dispositions légales ou réglementaires venaient à imposer des délais de conservation différents.

En cas d'utilisation illicite ou non conforme aux règles fixées par l'organisme, l'utilisateur s'expose à des poursuites disciplinaires, civiles et/ou pénales.

7. Mobilité et matériels mis à disposition par l'organisme

Tout utilisateur qui dispose de matériels nomades est informé des consignes de sécurité particulières lors de la mise à disposition de la ressource.

Seuls les matériels nomades autorisés peuvent être connectés au réseau de l'Assurance Maladie.

L'attention de l'utilisateur est attirée sur le fait que l'utilisation de ces matériels nomades à l'extérieur de l'organisme, engage sa responsabilité.
L'utilisation des matériels nomades impose donc à chacun un niveau de surveillance et de confidentialité renforcé.

8. Données nominatives

La présence de données nominatives au sein du système d'information, en particulier celles d'assurés, de professionnels de santé et d'employeurs n'est possible et autorisée qu'en respect de formalités préalables et d'obligations pour le responsable du traitement.
Ainsi, les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitement automatisé ou non, de données à caractère personnel.

Définition d'une donnée à caractère personnel :

Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement par référence à un numéro d'identification (par exemple le n° de sécurité sociale) ou par référence à un ou plusieurs éléments qui lui sont propres (par exemple les initiales du nom et du prénom) ou par recoupement d'informations du type : date de naissance, commune de résidence, éléments biométriques, etc.

La donnée de santé à caractère personnel

Toute information relative à la santé d'une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
Dans le domaine sanitaire, une donnée de santé à caractère personnel se définit comme une donnée susceptible de révéler l'état pathologique de la personne. Cette indication doit toutefois être aujourd'hui appréciée au regard de la définition d'une donnée de santé issue de la proposition de règlement du parlement européen et du conseil du 5 janvier 2012 sur la protection des données : «toute information relative à la santé physique ou mentale d'une personne, ou à la prestation de services de santé à cette personne».
Elle traduit un concept plus large de la donnée de santé, qui aujourd'hui ne peut se limiter à la seule indication d'une maladie tant la prise en charge sanitaire d'une personne emporte également la connaissance de sa situation familiale ou sociale et fait intervenir des acteurs multiples professionnels de santé et personnels sociaux.

9. Propriété intellectuelle

L'utilisation du système d'information de l'organisme implique le respect des droits de propriété intellectuelle et notamment de la réglementation relative à la propriété littéraire et artistique.

10. Analyse et contrôle de l'utilisation des ressources du système d'information

10.1. Principe directeur

L'organisme doit s'assurer du bon fonctionnement du système d'information et empêcher son utilisation dans un cadre non conforme aux règles définies dans la présente Charte.

10.2. Actions des administrateurs du système d'information

Les administrateurs sont nommément désignés et assurent le bon fonctionnement des moyens informatiques de l'organisme.

Les administrateurs sont tenus au secret professionnel concernant toute information confidentielle qu'ils pourraient être amenés à consulter et tout particulièrement celles couvertes par le secret de la correspondance privée.
Aucune exploitation à des fins autres que celles découlant de leur mission ne saurait être opérée et tolérée.

11. Sauvegarde et archivage

11.1. Données générales

L'utilisateur doit stocker ses fichiers et données électroniques dans des espaces définis par le service informatique.

La sauvegarde des données locales résidantes sur le disque dur du poste de travail est à la charge de l'utilisateur. Les moyens d'archivage locaux peuvent être mis à disposition à cette fin.

La sauvegarde des données déposées sur les serveurs est à la charge du service informatique.

Les informations médicales à caractère personnel doivent être impérativement déposées sur un serveur dédié. Elles ne doivent donc, en aucun cas, être conservées sur le poste de travail.

11.2. Données techniques

Les données de connexion (statistiques, Internet, serveurs, applications, etc.) sont conservées pendant 6 mois.

11.3. Archivage et destruction

L'archivage des données est effectué conformément à la réglementation applicable ainsi qu'aux préconisations de la LR-DDO-214/2013 concernant la « classification des informations ».
Les données sont détruites lorsque le besoin de conservation de l'information n'est plus exprimé.

12. Contrôle de l'application de la charte

L'organisme doit pour des nécessités de maintenance et de sécurité, procéder périodiquement, par les moyens les plus appropriés, à des audits de contrôle de la bonne application de la présente charte, dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.
Les audits peuvent viser le contrôle de tout ou partie de la présente charte.
Dans le cas d'identification d'axes d'amélioration, des plans d'actions correctifs doivent être mis en place.

13. Journaux d'événements

Tout accès et utilisation du système d'information génère automatiquement une trace collectée dans des journaux d'événements qui sont confidentiels et accessibles uniquement aux personnels habilités ainsi qu'à la Direction de l'organisme.
Cette collecte participe à la garantie d'un bon fonctionnement et d'une utilisation normale des ressources du système d'information et le cas échéant permet l'identification d'usages illégitimes.

14. Sanctions

Les sanctions prévues à la convention collective ou à toute autre disposition conventionnelle ou réglementaire existante dans l'organisme sont applicables en cas de non-respect de la présente charte.

15. Dispositions spécifiques liées aux organisations syndicales

La mise à disposition des organisations syndicales qui le souhaitent d'un espace dédié relève de la négociation locale.

16. Suivi de la mise en application de la Charte

La Direction se charge du respect de la Charte et de son suivi.

Toute difficulté d'application de la Charte doit être signalée au MSSI/RSSI.

17. Entrée en vigueur

Cette charte fait l'objet d'une publication auprès de l'Inspection du Travail.

Elle entre en vigueur un mois après l'accomplissement des formalités de communication à l'Inspection du travail, de dépôt et de publicité telles que prévues à l'article L 1321 4 du code du travail.

Toute modification ultérieure, adjonction ou retrait de clause de la présente charte sera soumis à la même procédure, conformément aux prescriptions de l'article L 1321 4 du code du travail, étant entendu que toute clause de la charte qui deviendrait contraire aux dispositions légales, réglementaires ou conventionnelles applicables à l'organisme du fait de l'évolution de ces dernières, serait nulle de plein droit.

Chaque personnel de l'Assurance Maladie et assimilé en est destinataire et doit s'engager à en prendre connaissance et à en respecter les termes.
De même, la charte devra être diffusée aux tiers qui se verront doté d'un accès au Système d'information et qui s'engageront à la respecter.

Décision n° 2020-23-0024

Annexe n° 02

NÉANT AU 19/05/2020

Le Directeur Général

Docteur Jean-Yves GRALL

Le Directeur Général
de l'Agence Régionale de Santé Auvergne-Rhône-Alpes

Docteur Jean-Yves GRALL

Agence Régionale de Santé
Auvergne-Rhône-Alpes

Charte de Sécurité des données de contact tracing

Version du 20 mai 2020

Au quotidien > Informatique et bureautique > Sécurité des systèmes d'information

Sécurité des Systèmes d'Information

Le suivi des cas d'infection respiratoire aigüe coronavirus (2019-nCoV / Covid 19) sur le territoire a conduit les pouvoirs publics à prendre des mesures exceptionnelles adaptées à chaque stade de l'épidémie avec la mise en place d'un dispositif de suivi des patients détectés positif au Covid19 et d'identification, de contact et de suivi des personnes ayant été en contact avec eux.

Ce suivi est réalisé par le biais de diverses applications ; la présente charte vise à assurer l'utilisation et la protection des données contenues dans ces dispositifs de contact-tracing conformément :

- Au code de la santé publique, notamment ses articles L. 1431-1 et L. 1431-2 ;
- Au décret n° 2010-336 du 31 mars 2010 portant création des ARS ;
- Au 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 ;
- A la Politique de Sécurité des Systèmes d'Information de l'Etat et sa déclinaison pour l'ARS Auvergne Rhône-Alpes ;
- A la Charte de Sécurité des Systèmes d'Information définit les droits, les devoirs et les responsabilités de tous ;
- Aux décisions 2020-23-0022 et 2020-23-0023 du directeur général de l'ARS ARA.

La liste des applications mises à disposition dans le cadre du contact tracing n'est pas exhaustive, elle comprend à la date de rédaction de la présente charte :

- Les applications **SORMAS** nationale et locale : applications de recueil de données, de suivi épidémiologique des cas (possibles, probables et confirmés) d'une infection à SARS-CoV-2, ainsi que des personnes contact d'un cas de cette maladie, gérées par l'Agence Régionale de Santé.

- L'application **SIDEP** : collecte les données traitées dans le cadre des examens de détection du génome du SARS-CoV-2 par RT-PCR de l'ensemble des laboratoires de biologie médicale, en colligeant tous les résultats d'analyses pour le COVID-19, avec les données d'identification des personnes prélevées.

- L'application **« Contact COVID »** : téléservice pour l'identification et la prise en charge des personnes contacts à risque, élaboré par l'Assurance Maladie et accessible via Amelipro. Cette application collige l'ensemble des données du contact-tracing (données d'investigation collectées lors des interrogatoires des cas et des personnes contacts à risque par le Niveau 2) et qui sera accessible aux acteurs de niveau 1 et 2 et aux ARS. La base permettra également de produire les indicateurs quotidiens de suivi du contact-tracing.

Les dispositions de la présente charte s'appliqueront à toutes nouvelles applications, validées par l'Agence Régionale de Santé Auvergne-Rhône-Alpes, dans le cadre de ses missions du contact tracing.

Décision n° 2020-23-0024
Annexe n° 03

Les objectifs de la charte

Tous les utilisateurs des systèmes d'information liés à la gestion du contact tracing, et plus généralement du suivi des cas de Coronavirus (Covid-19), au sein de l'Agence doivent prendre connaissance et appliquer les règles présentes dans la charte.

Définir vos droits et devoirs

En tant qu'utilisateur des outils de suivis et de contact-tracing, vous devez assurer :

- Le droit au respect de la vie privée ;
- Les devoirs en matière de protection de l'information ;
- Le devoir d'alerte lors de la détection d'un problème de sécurité.

Votre engagement est attendu

L'utilisation des outils mis à disposition par le biais d'une habilitation informatique vaut acceptation de la présente charte. Cette acceptation est matérialisée par l'ouverture de session sur un poste de travail de l'Agence Régionale de Sante Auvergne-Rhône-Alpes avec votre identifiant unique Windows ou l'utilisation de la carte d'accès Assurance Maladie sur un poste de travail de la CNAMTS.

Qui contacter en cas d'incident informatique ?

Incident sur le poste de travail :

En cas de doute sur la sécurité de votre poste de travail, vous devez appeler directement le :

✆ 04 72 34 **31 84**

Perte ou vol de matériel :

Si l'incident arrive en journée, contactez directement la DDSIAIG au :

✆ 04 72 34 **31 84**

Besoin d'informations, d'assistance sur la sécurité informatique ou pour signaler un évènement inhabituel, contacter le RSSI :

✆ 04 72 34 **74 48**

ars-ara-ssi@ars.sante.fr

Pour un incident survenu sur le Smartphone ou la clé 4G, le soir, le week-end ou en déplacement, appeler l'opérateur pour bloquer la ligne :

✆ **0 800 291 000**

Pour la calculette : ✆ **01 40 56 56 56**

Les règles générales de sécurité

Vous êtes responsable des opérations réalisées avec vos accès sur les systèmes d'information, vous devez vous engager à protéger les moyens d'authentification qui

vous ont été affectés (code, carte ou OTP[1]). Pour garantir votre utilisation et sécuriser vos accès, appliquez les consignes de la charte SSI de l'ARS Auvergne-Rhône-Alpes.

Protégez les données de santé

Les applications de contact-tracing contiennent un grand nombre d'informations liées aux données de santé ainsi qu'au déplacement des personnes, c'est pourquoi une sécurisation accrue de ces outils doit être mise en place :

- Obligation de demande d'accès validée par le hiérarchique et le SG (ou DDSIAIG) ;
- Ne réalisez pas d'export des données sur le réseau ARS ;
- Veillez au strict respect du secret professionnel ;
- Non divulgation, communication ou diffusion des informations contenues dans les bases à des tiers non autorisés ;
- Veillez à ne pas utiliser ou copier les données pour une autre finalité que celle du contact-tracing ;
- Prenez toutes les précautions pour préserver la sécurité des données ;
- Assurez-vous que seuls des moyens de communication sécurisés sont utilisés pour transférer ces données ;
- Respecter les consignes d'utilisation des matériels et logiciels ;
- Ne pas entraver le fonctionnement des outils de sécurité tels que les antivirus, les sauvegardes de données, les outils de contrôle d'accès.

Utilisation du SI Assurance Maladie

L'application spécifique Contact Covid est accessible via l'utilisation de matériel mis à disposition des ARS par les différentes Caisses Primaires d'Assurance Maladie pour le compte de la CNAMTS. L'utilisation de ces équipements est soumise à la lecture et l'acceptation de la charte complémentaire qui est affichée dans les salles ainsi que sur l'Intranet (Volet Sécurité des Systèmes d'information).

Ouverture de session

L'ouverture d'une session sur un poste Assurance Maladie est soumise à l'utilisation d'une carte à puce liée au poste informatique. Celle-ci est sous la responsabilité de l'agent et ne doit en aucun cas être transmise à un agent non habilité.
Les cartes doivent être stockées dans un endroit sécurisé en dehors de leur utilisation (armoire fermée à clé par exemple).

[1] OTP : One Time Password : code à usage unique pour l'accès à une application, il s'agit par exemple d'un code réceptionné par SMS. Dans ce cas, celui-ci ne doit pas être transmis à un tiers.

⇨ En cas d'absence, même de courte durée, l'agent doit retirer la carte de l'ordinateur afin de procéder à un verrouillage de la station.

Utilisation des logiciels

L'utilisation des logiciels Assurance Maladie est soumise à la connexion au VPN installée sur le poste, une procédure est fournie aux agents concernés.

Dans tous les cas de figure, il est interdit de tenter de connecter un périphérique (tel qu'une clé USB) sur le poste sans accord préalable de la hiérarchie et du RSSI de l'ARS.

⇨ Il est rappelé que les postes Assurance Maladie doivent être utilisés sur un réseau indépendant de celui de l'ARS Auvergne-Rhône-Alpes.

Respect de la confidentialité des données

Les applications liées au contact-tracing permettent une identification précise des patients et des cas contacts, voir une géolocalisation de ces personnes. N'utilisez ces données que dans le cadre strict de la gestion de la pandémie et ne réalisez aucun export des données dans une autre base que celle initialement prévue au suivi des cas contacts.

Les exports de données doivent être limités à ce qui est strictement nécessaire pour la réalisation de la mission. Les exports sont sous la responsabilité de l'utilisateur, qui s'assure de la mise en œuvre selon des modalités de sécurité organisationnelles et techniques adaptées : stockage sur un espace sécurisé des serveurs ou à défaut dans le cas d'une mobilité obligatoire sur une clé USB Chiffrée délivrée par la DDSIAIG. Les exports ne doivent pas être conservés au-delà de la durée nécessaire à la réalisation de la mission confiée à l'utilisateur et doivent impérativement être supprimés à l'issue de sa mission et au plus tard à l'issue de l'investigation.

Tout nouvel export de données devra faire l'objet d'une déclaration à la Déléguée à la Protection des Données de l'Agence via la boîte mail : ars-ara-dpd@ars.sante.fr en précisant la finalité de l'export et les méthodes de sécurisation des données. Dans le cas contraire, l'export pourra être considéré comme un détournement de finalité.

Les données collectées et conservées dans les applications précitées sont couvertes par le secret professionnel et engagent à ce titre la responsabilité pénale des personnes y accédant (article 226-13 du code pénal).

Les atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques et les atteintes aux systèmes de traitement automatisé de données sont également sanctionnées par le code pénal (articles 226-16 et suivants, et 323-1 et suivants du code pénal).

Portée de la présente charte de sécurité

Les consignes de sécurité du présent document sont applicables à tous, agents ARS, agents en renfort (intérimaire, personnel mis à disposition) mais également aux prestataires et partenaires extérieurs - les documents contractuels doivent en faire mention avant tous travaux en commun.

Les partenaires ou prestataires n'ont pas l'autorisation de connecter leurs équipements sur le réseau informatique de l'Agence. En cas de besoin, ils doivent se munir de leur propre solution de connexion internet.

Le contrôle de l'utilisation des SI

Les traces de vos actions sont enregistrées et conservées dans le respect de la législation applicable, notamment de la loi « Informatique et Libertés » et le Règlement Général sur la Protection des Données - (UE) 2016/679 du Parlement européen :

- Au niveau des MCAS, de l'ARS ARA et de la CNAMTS ;
- Pour garantir le fonctionnement et la sécurité des systèmes ;
- Sous la responsabilité du responsable de la sécurité des systèmes d'information et des administrateurs des systèmes d'information qui ont un engagement de confidentialité.

Décision n° 2020-23.0024
Annexe n°04

ACCORD DE SOUS-TRAITANCE - PROTECTION DES DONNEES PERSONNELLES DANS LE CADRE DES TRAITEMENTS MIS EN ŒUVRE PAR LES AGENCES REGIONALES DE SANTE POUR LE SUIVI DE LA CRISE DU COVID19

I. Définitions :

« **Responsable du Traitement** » : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du Traitement; lorsque les finalités et les moyens de ce Traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du Traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

En application de l'article 26 du Règlement européen sur la Protection des Données, les agences régionales de santé ci-après dénommées « ARS ») sont **Responsables du Traitement** dans la mesure où elles déterminent les finalités et les moyens du Traitement. Les agences régionales de santé (ARS) sont responsables du traitement faisant l'objet de cet accord de sous-traitance.

« **Sous-Traitant** » : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données Personnelles pour le compte, sur instruction et sous l'autorité du Responsable de Traitement.

La **direction du numérique du Ministère (DNUM)** agit en tant que sous-traitant des ARS dans le cadre du présent accord.

« **Destinataire** » : désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données Personnelles, qu'il s'agisse ou non d'un tiers.

« **Données Personnelles** » ou « Données à caractère personnel » : désigne toute information se rapportant à une personne physique identifiée ou identifiable, 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 ;

« **Finalité** » : désigne les objectifs assignés au Traitement;

« **Personne concernée** » : désigne les personnes physiques identifiables ou identifiées dont les Données Personnelles sont collectées et intégrées dans le Traitement ;

« **Autorité(s) de contrôle** » : désigne l'(les) autorité(s) publique(s) indépendante(s) instituée(s) par chaque État membre chargée(s) de surveiller l'application du Règlement Européen sur la Protection

des Données, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du Traitement et de faciliter le libre flux des Données Personnelles au sein de l'Union européenne. En France il s'agit de la CNIL, Commission nationale de l'informatique et des libertés.

« **Analyse d'impact** » : désigne un processus dont l'objet est de décrire le Traitement de données à caractère personnel, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au Traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face.

« **Traitement de données à caractère personnel** » ou « Traitement » au sens du présent contrat : désigne toute opération ou ensemble d'opérations portant sur des Données Personnelles ayant pour finalité la gestion de la crise sanitaire du Covid-19, quel que soit le procédé utilisé telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

« **Violation** » : désigne une faille de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données Personnelles ;

« **Transfert** » : désigne toute communication, copie ou déplacement de Données Personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne et n'ayant pas un niveau de protection adéquat ou dans une organisation internationale.

« **Règlement européen sur la Protection des Données** » : désigne le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 applicable à compter du 25 mai 2018 ;

« **Contrat** » : désigne l'ensemble des engagements sur la base desquels la Responsabilité du Traitement est mise en place.

« **Délégué** » : désigne le (la) délégué(e) à la protection des Données Personnelles tel que défini par la section 4 du Règlement européen sur la Protection des Données.

II. Objet

Le présent accord a pour objet de définir le rôle confié par les ARS à leur sous-traitant la DNUM, qui se limite aux opérations suivantes :

- Assurer la mise à disposition des ARS des données issues du système d'information « Contact Covid », décrit au chapitre 1er du 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 ;

- Assurer la mise à disposition des ARS des données issues du système d'information « SI-DEP », décrit au chapitre 2 du 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 ;
- Assurer la mise à disposition des ARS de l'application « SORMAS[1] » dans le cadre de l'arrêté pris sur le fondement de l'article 67 de la LIL.

Dans le cadre de leurs relations, les Parties s'engagent à respecter la règlementation en vigueur applicable au Traitement de données à caractère personnel (loi n° 2020-546 du 11 mai 2020 prorogeant l'état d'urgence sanitaire et complétant ses dispositions, décret n° 2020-551 du 12 mai 2020 relatif aux systèmes d'information mentionnés à l'article 11 de la loi) ainsi que le Règlement Européen sur la Protection des Données.

III. Description des conditions techniques de mise à disposition

L'application SORMAS est mise à disposition des ARS au travers d'une plateforme sécurisée composée de serveur (VM), chacun étant installé dans un réseau virtuel VLAN dédié :

- Accès des utilisateurs : filtré sur les adresses IP des ARS, au travers d'un WAF et d'une double authentification par login + mot de passe + code OTP
- Accès des administrateurs : via une interface réseau dédiée de manière forte à un bastion ; une fois connecté à ce bastion, ils peuvent accéder aux équipements via un compte générique avec identifiant et mot de passe.

Les données de ContactCOVID et celles de SI-DEP sont récupérées auprès respectivement de l'assurance maladie et de l'AP-HP via des serveurs SFTP protégés par système bi-clé ; les clés sont partagées via un coffre-fort numérique.

[1] L'outil SORMAS est un outil de « contact tracing » qui a pour finalité l'enregistrement, l'investigation et le suivi épidémiologique, par les agences régionales de santé (ARS), des cas de COVID-19 et des cas contacts, en vue notamment d'identifier les chaines et cas groupés de contamination et de prendre les mesures destinées à limiter la propagation de l'épidémie.

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé

DNUM DIRECTION DU NUMÉRIQUE

IV. Obligations des Responsables de Traitement et de leur sous-traitant la DNUM

Le tableau ci-dessous synthétise le niveau et les conditions de responsabilité de chacune des parties au cours du Traitement :

Actions	ARS	DNUM
Qui détermine les finalités du traitement ?	X	
Qui élabore les textes relatifs au traitement et formalités auprès de la CNIL ?	X	
Qui définit les données personnelles collectées/traitées ?	X	
Qui détermine les destinataires des données et les catégories de personnes habilitées à accéder à ces données ?	X	
Qui garantit la confidentialité et la sécurité des données traitées ?		X
Qui s'assure de la conformité du traitement aux règles relatives à la protection des données ?	X	X
Qui fournit les moyens techniques pour le traitement ?		X
Qui donne les instructions en matière d'utilisation ? (guide d'utilisation)	X	X
Qui est responsable de la gestion des personnes habilitées à accéder aux données ? (politique de confidentialité/tableau de gestion des habilitations)	X	X
Qui décide des moyens techniques et organisationnels appropriés pour assurer la sécurité des DCP ? (disponibilité, absence de destruction, d'altération ou de perte, chiffrement, pseudonymisation, traçabilité, absence d'accès non autorisés, etc.)	X	X
Qui détermine les évolutions substantielles à apporter au traitement ?	X	
Qui est responsable de la relation avec le(s) sous-traitant(s) et garantit sa conformité aux textes applicables ?	X	X
Qui élabore la procédure de gestion des incidents/violations de données ?	X Pour les remontées	X
Qui réalise la notification des violations de données auprès de l'autorité de contrôle compétente ?	X avec l'aide DNUM	X Aide
Qui est l'autorité d'homologation du traitement ?	X	
Qui élabore la documentation permettant une reprise des données en fin de traitement ?		X

1) Les ARS, en tant que responsables du traitement, s'engagent à :

A compléter

2) La DNUM, en tant que sous-traitant, s'engage à :

a) TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

1. traiter les données pour les seules finalités qui font l'objet du présent accord. Elle s'abstient de tout traitement ultérieur des données traitées pour son propre compte ;

2. traiter les données conformément aux instructions du responsable de traitement dans le présent accord. Si le sous-traitant considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit de l'Union ou du droit Français relatif à la protection des données, il en informe immédiatement les responsables de traitement. En outre, si le sous-traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

En cas de modification du Règlement Européen sur la Protection des Données Personnelles ayant une incidence sur la conformité à la loi du Traitement réalisé dans le cadre du contrat, la DNUM s'engage à y remédier en apportant aux modalités d'exécution du Traitement les adaptations nécessaires au respect des nouvelles dispositions législatives/réglementaires applicables.

Les ARS s'assureront que les Données Personnelles sont traitées uniquement pour la finalité déterminée dans le présent accord.

b) OBLIGATION D'INFORMATION

La DNUM délivre toutes informations utiles aux Responsables du Traitement sur ses activités de Traitement (usage, stockage et pays d'origine des Données Personnelles) et l'assiste afin qu'ils procèdent ensemble aux éventuelles demandes et notifications à la CNIL qui leur incombent en qualité de Responsables du Traitement ;

c) OBLIGATION DE SECURITE

1. La DNUM s'engage à mettre en place et maintenir pendant toute la durée du Traitement toutes les mesures techniques et organisationnelles, adaptées à la nature des Données Personnelles traitées et aux risques présentés par le Traitement (i) pour assurer la

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé

DNUM DIRECTION DU NUMÉRIQUE

confidentialité, la disponibilité, la résilience[2] et l'intégrité constantes des systèmes et des services de Traitement de données à caractère personnel, et (ii) pour rétablir la disponibilité des Données Personnelles et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique (iii) pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.

2. Veiller à ce que leurs employés, préposés, mandataires et leurs Sous-Traitants ou toute personne agissant pour leur compte, qui ont accès aux Données Personnelles :
   - soient dûment autorisés ;
   - respectent les obligations précisées dans le présent accord et la confidentialité des données ;
   - soient particulièrement informées et sensibilisées aux règles encadrant la protection des données à caractère personnel et les traitent conformément à ladite annexe ;
   - reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
3. Veiller au respect des exigences de sécurité définies par ailleurs.

d) PROTECTION DES DONNEES PERSONNELLES

La DNUM s'engage à s'assurer de la protection des Données Personnelles dès le début et tout au long du Traitement.

e) RECOURS A LA SOUS-TRAITANCE

La DNUM s'engage à n'avoir recours à la sous-traitance que pour l'hébergement, la sécurisation des infrastructures, la mise en place en place de l'entrepôt permettant d'accueillir les données de SI-DEP et Contact COVID, la gestion des flux d'alimentation de SORMAS et le support de niveau 2 dans les conditions définies ci-après.

La DNUM s'engage à :

- choisir des Sous-Traitants présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences du Règlement Européen sur la Protection des Données et de l'Annexe ;
- signer avec les Sous-Traitants un contrat conforme à la réglementation sur la protection des Données Personnelles.

Sous-traitance par la DNUM

[2] Capacité d'un système ou d'une architecture réseau à continuer de fonctionner en cas de panne

La DNUM s'engage à informer les responsables de traitement en cas de changement de sous-traitant.

Dans le cadre du Traitement, la DNUM aura recours à la sous-traitance des sociétés ITS INTEGRA pour l'hébergement, CERTILIENCE pour la sécurisation des infrastructures, KEYRUS pour la mise en place de l'entrepôt et la gestion des flux d'alimentation de SORMAS et CGI pour le support de niveau 2. La DNUM conclura les conventions prévoyant notamment leurs obligations relatives à la sécurité et à la confidentialité des Données Personnelles afin de satisfaire aux prescriptions du présent point.

La DNUM transmettra à ses sous-traitant les instructions nécessaires à la réalisation du Traitement notamment celles relatives à la sécurité au sein de la DNUM contenues en Annexe 3 du présent accord cadre.

La DNUM contrôlera le respect par ses sous-traitants des règles relatives à la protection des données.

Information des personnes concernées et demandes d'exercice des droits des personnes concernées

Les ARS élaborent les mentions d'information sur le Traitement, le cas échéant avec le concours de la DNUM.

Les ARS diffusent sur leur site une notice d'information complète sur le Traitement.

Les demandes d'information et d'exercice des droits par les Personnes concernées en vertu du RGPD pourront être faites auprès des ARS. Elles seront invitées à exercer leurs droits auprès d'un contact unique par ARS dont les coordonnées (adresse mail et adresse postale) seront précisées sur le site internet de chaque ARS et à solliciter de l'information sur le traitement.

La DNUM n'ayant pas directement accès aux données, les demandes d'information et d'exercice des droits par les personnes concernées seront communiquées et traitées par les ARS dans un délai d'un mois.

f) DUREE DE CONSERVATION

La DNUM s'engage à ne pas conserver les Données à caractère personnel auxquelles elle donne accès.[JO1]

g) REGISTRE DES OPERATIONS DE TRAITEMENT

La DNUM tient un registre de toutes les catégories d'activités de Traitements de Données à caractère personnel effectués conforme à l'article 30 du RGPD.

h) VIOLATION

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé

DNUM DIRECTION DU NUMERIQUE

Les ARS et la DNUM s'engagent à informer sans délai (et au maximum dans un délai de 24h après en avoir pris connaissance) le FSSI et le RSSI des ministères sociaux : ssi@sg.social.gouv.fr de toute violation de données à caractère personnel avérée ou supposée, susceptible d'engendrer un risque pour les personnes concernées.

Cette information du FSSI et du RSSI des ministères sociaux est accompagnée de toutes les documentations utiles permettant de comprendre l'incident, les mesures envisagées et si nécessaire les éléments permettant de notifier à la CNIL dans les 72 heures une violation de données à caractère personnel.

En cas de Violation ou si les Responsables du Traitement ont tout lieu de croire qu'une Violation a eu lieu, ils doivent le notifier sans délai à l'Autorité de contrôle compétente.

Les Responsables du Traitement doivent alors transmettre à l'Autorité de contrôle compétente: (i) la description de la nature de la Violation, y compris si possible, les catégories et le nombre approximatifs de Personnes concernées par la Violation et les catégories et le nombre approximatif d'enregistrements de Données Personnelles concernés ; (ii) le nom et les coordonnées du Délégué ou d'un autre point de contact auprès duquel des informations complémentaires peuvent être obtenues ; (iii) la description des conséquences probables de la Violation; (iv) la description des mesures prises ou que le Responsable du Traitement concerné propose de prendre pour remédier à la Violation, y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. La DNUM s'engage auprès des Responsables de traitement à coopérer pleinement à cette notification de violation de données sans délai notamment en fournissant toutes informations pertinentes.

Si, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, les informations peuvent être communiquées de manière échelonnée sans autre retard indu.

Contrôle de l'autorité de contrôle compétente

Dans le cas où un les Responsables du Traitement feraient l'objet d'un contrôle de la part de l'Autorité de contrôle compétente, la DNUM s'engage à coopérer pleinement et sans délai avec les Responsables du Traitement et l'Autorité de contrôle, notamment en fournissant toutes informations pertinentes et l'accès à tous équipements, logiciels, données, dossiers, systèmes d'information, etc. utilisés pour la réalisation des prestations, et notamment le Traitement, et nécessaires à la réalisation du contrôle par l'Autorité de contrôle.

Les Responsables du Traitement concernés par le contrôle peuvent être contraints de divulguer des Données Personnelles à la demande d'une cour, agence administrative ou autorité gouvernementale, ou en vertu de toute loi, règlementation, citation à comparaître, requête, sommation ou autre processus administratif ou légal, ou par n'importe quelle enquête formelle ou informelle par n'importe quelle agence gouvernementale ou autorité s'engage à utiliser toute option légale pour contester ou s'opposer à une telle demande et, si une telle opposition n'est pas possible ou n'aboutit pas, ne divulguer que les Données Personnelles couvertes par cette demande. La DNUM s'engage à apporter son concours à la transmission des données si nécessaire.

Décision n° 2020-23-0022
Annexe n° 04

MENANT AU 31/05/2020

18 MAI 2020

Le Directeur Général
Docteur Jean-Yves GRALL

Le Directeur Général
de l'Agence Régionale de Santé Auvergne-Rhône-Alpes

Docteur Jean-Yves GRALL

Décision n°2020-23-0022

Portant habilitation des agents de l'Agence et de ses sous-traitants autorisés à enregistrer et à consulter les données du traitement « Contact Covid »

Le Directeur Général de
l'Agence Régionale de Santé Auvergne-Rhône-Alpes
Chevalier de la Légion d'Honneur
Chevalier de l'Ordre National du Mérite

Vu le code de la santé publique, notamment ses articles L. 1431-1 et L. 1431-2 ;

Vu le décret n° 2010-336 du 31 mars 2010 portant création des agences régionales de santé ;

Vu le décret du 6 octobre 2016 portant nomination de Monsieur Jean-Yves GRALL en qualité de directeur général de l'Agence Régionale de Santé Auvergne-Rhône-Alpes ;

Vu 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 ;

Considérant qu'il appartient au Directeur Général, conformément aux dispositions de l'article 3-I 2° du décret 2020-551, d'habiliter les agents de l'Agence et ses sous-traitants à enregistrer l'ensemble des données prévues à l'article 2-II dudit décret et à les consulter dans la limite de leurs besoins respectifs d'en connaître ;

Considérant que l'Agence Régionale de Santé, conformément aux dispositions de l'article 14 du décret 2020-551, doit s'assurer, notamment, que ses sous-traitants présentent des garanties de compétence suffisante pour assurer la mise en œuvre des mesures techniques et organisationnelles appropriées et le respect des règles de confidentialité ;

Considérant la convention de service « accès tiers au télé-service contact covid de la CPAM » et ses 3 annexes ainsi que la charte informatique qui sont annexées à la présente décision [annexes n° 01 et 02] ;

DECIDE

Art. 1 Habilitation de l'ARS

Art. 1.1 – Habilitation des agents de l'ARS

Les personnes nommément désignées en **annexe n° 03 « habilitation des agents de l'ARS – traitement contact covid »** sont habilitées à enregistrer l'ensemble des données prévues à l'article 2-II du décret n° 2020-551 et à les consulter dans la limite de leurs besoins respectifs d'en connaître.

Guillaume Gras - ou en son absence Eric Virard - est désigné pour valider, par sa signature apposée sur l'annexe n° 03 et en la datant, les éventuels ajustements (retrait et ajouts) auxquels il sera procédé postérieurement à la date de signature de la présente décision sur ladite annexe.

Art. 2.1 – Habilitation des sous-traitants et de leurs collaborateurs

Les prestataires et leur personnel nommément désignés en **annexe n° 04 « habilitation des sous-traitants et de leurs collaborateurs – traitement contact covid »** sont habilités à enregistrer l'ensemble des données prévues à l'article 2-II du décret n° 2020-551 et à les consulter dans la limite de leurs besoins respectifs d'en connaître.

Il appartient au(x) sous-traitant(s) d'apporter les garanties mentionnées à l'article 14 du décret n° 2020-551.

Guillaume Gras - ou en son absence Eric Virard - est désigné pour valider, par sa signature apposée sur l'annexe n° 04 et en la datant, les éventuels ajustements (retrait et ajouts) auxquels il sera procédé postérieurement à la date de signature de la présente décision sur ladite annexe.

Art. 2.3 – Spécimen de signature

Un spécimen de signature des agents, désignés aux articles 2.1 et 2.2, est apposé ci-dessous :

Nom et prénom	Signature	Paraphe
GRAS Guillaume Directeur Délégué Système d'Information, Affaires Immobilières et Logistiques		
VIRARD Eric Secrétaire Général		

Art. 2 Modalités d'enregistrement des données et d'accès au traitement « Contact covid »

Art. 2.1 – Modalités d'enregistrement des données

Conformément à l'article 4-I du décret n° 2020-551, les personnes et sous-traitants mentionnées aux annexes n° 03 et n° 04 enregistrent, sans délai, les données relatives aux personnes infectées et aux personnes évaluées comme contacts à risque de contamination.

Art. 2.2 – Modalités d'accès au traitement « contact covid »

Conformément à l'article 4-II-3° du décret n° 2020-551, le traitement « contact covid » est accessible par les moyens d'identification et d'authentification selon des modalités fixées par la Caisse Nationale d'Assurance Maladie décrites dans la convention de service annexée (annexe n° 01) et la charte informatique (annexe n° 02).

Art. 3 Traitement automatisé des données

L'ARS Auvergne-Rhône-Alpes procède à un traitement de données personnelles sur le fondement de l'article 6 1. e) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) pour la permettre la désignation et d'habilitation des personnes autorisées à accéder à CONTACT-COVID.

Les données enregistrées sont conservées pendant la durée de l'habilitation précitée et ne peuvent être communiquées qu'aux destinataires suivants : personnels de l'ARS ARA et agents des sous-traitants.

Conformément au RGPD et à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les personnes disposent d'un droit d'accès, de rectification, d'effacement et de portabilité des données les concernant. Ils peuvent également demander la limitation du traitement de leurs données ou s'opposer, pour des raisons tenant à leur situation particulière, au traitement des données les concernant.

Ils peuvent exercer ces droits, en adressant au délégué à la protection des données de l'ARS par courrier (241 rue Garibaldi – 69003 Lyon) ou par courriel à l'adresse ars-ara-dpd@ars.sante.fr. Ils peuvent d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés s'ils considèrent que le traitement de données à caractère personnel les concernant constitue une violation du règlement général sur la protection des données et de la loi informatique et libertés

Art. 4 Date de prise d'effet

La présente décision, comprenant quatre annexes, prend effet au mardi 13 mai 2020.

Lyon le **18 MAI 2020**

Le Directeur Général
Docteur Jean-Yves GRALL

Décision n°2020-23-0023

Portant habilitation des agents de l'Agence et de ses sous-traitants autorisés à être destinataires des données du traitement « SI-DEP »

Le Directeur Général de
l'Agence Régionale de Santé Auvergne-Rhône-Alpes
Chevalier de la Légion d'Honneur
Chevalier de l'Ordre National du Mérite

Vu le code de la santé publique, notamment ses articles L. 1431-1 et L. 1431-2 ;

Vu le décret n° 2010-336 du 31 mars 2010 portant création des agences régionales de santé ;

Vu le décret du 6 octobre 2016 portant nomination de Monsieur Jean-Yves GRALL en qualité de directeur général de l'Agence Régionale de Santé Auvergne-Rhône-Alpes ;

Vu 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 ;

Considérant qu'il appartient au Directeur Général d'habiliter les agents de l'Agence et ses sous-traitants à être destinataire des données enregistrées dans le traitement (article 10-II-2° du décret 2020-551) et des seules données relatives aux personnes infectées et aux personnes ayant été en contact avec ces personnes ayant fait l'objet de mesures adéquates de pseudonymisation permettant d'assurer la confidentialité de l'identité des personnes (article 10-III-1° du décret 2020-551)

Considérant que l'Agence Régionale de Santé, conformément aux dispositions de l'article 14 du décret 2020-551, doit s'assurer, notamment, que ses sous-traitants présentent des garanties de compétence suffisante pour assurer la mise en œuvre des mesures techniques et organisationnelles appropriées et le respect des règles de confidentialité ;

DECIDE

Art. 1 Habilitation de l'ARS

Art. 1.1 – Habilitation des agents de l'ARS

Les personnes nommément désignées en **annexe n° 01 « habilitation des agents de l'ARS – traitement SI-DEP »** sont habilitées, pour les données listées à l'article 9 du décret n° 2020-551, à être destinataire :

- ✓ des données enregistrées dans le traitement (art. 10-II dudit décret) ;
- ✓ des données ayant fait l'objet d'une pseudonymisation (art. 10-III dudit décret) ;

Guillaume Gras - ou en son absence Eric Virard - est désigné pour valider, par sa signature apposée sur l'annexe n° 01 et en la datant, les éventuels ajustements (retrait et ajouts) auxquels il sera procédé postérieurement à la date de signature de la présente décision sur ladite annexe.

Art. 2.1 – Habilitation des sous-traitants et de leurs collaborateurs

Les prestataires et leur personnel nommément désignés en **annexe n° 02 « habilitation des sous-traitants et de leurs collaborateurs – traitement SI-DEP »** sont habilités, pour les données listées à l'article 9 du décret n° 2020-551, à être destinataire :

- ✓ des données enregistrées dans le traitement (art. 10-II dudit décret) ;
- ✓ des données ayant fait l'objet d'une pseudonymisation (art. 10-III dudit décret) ;

Il appartient au(x) sous-traitant(s) d'apporter les garanties mentionnées à l'article 14 du décret n° 2020-551.

Guillaume Gras - ou en son absence Eric Virard - est désigné pour valider, par sa signature apposée sur l'annexe n° 02 et en la datant, les éventuels ajustements (retrait et ajouts) auxquels il sera procédé postérieurement à la date de signature de la présente décision sur ladite annexe.

Art. 2.3 – Spécimen de signature

Un spécimen de signature des agents, désignés aux articles 2.1 et 2.2, est apposé ci-dessous :

Nom et prénom	Signature	Paraphe
GRAS Guillaume Directeur Délégué Système d'Information, Affaires Immobilières et Logistiques		
VIRARD Eric Secrétaire Général		

Art. 2 Modalités d'enregistrement des données et d'accès au traitement « SI-DEP »

Art. 2.1 – Modalités d'enregistrement des données

Conformément à l'article 10-I du décret susvisé, seuls les médecins ou les professionnels placés sous la responsabilité des services ou des laboratoires de biologie médicale sont habilités à renseigner les résultats de leurs examens, ce à quoi ne sont pas autorisés les personnes mentionnées aux annexes n° 01 et n° 02.

Art. 2.2 – Modalités d'accès au traitement « SI-DEP »

Les opérations de consultation du traitement « SI-DEP » font l'objet d'un enregistrement comportant l'identification de l'utilisateur ainsi que les données de traçabilité (notamment la date, l'heure et la nature de l'intervention dans le traitement), conformément à l'article 11-II du décret n° 2020-551. Pour ce faire, les personnes mentionnées aux annexes n° 01 et n° 02 sont signataires de la charte informatique « SI-DEP » dont le modèle est annexé (annexe n° 03).

Art. 3 Traitement automatisé des données

L'ARS Auvergne-Rhône-Alpes procède à un traitement de données personnelles sur le fondement de l'article 6 1. e) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) pour la permettre la désignation et d'habilitation des personnes autorisées à accéder à CONTACT-COVID.

Les données enregistrées sont conservées pendant la durée de l'habilitation précitée et ne peuvent être communiquées qu'aux destinataires suivants : personnels de l'ARS ARA et agents des sous-traitants.

Conformément au RGPD et à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les personnes disposent d'un droit d'accès, de rectification, d'effacement et de portabilité des données les concernant. Ils peuvent également demander la limitation du traitement de leurs données ou s'opposer, pour des raisons tenant à leur situation particulière, au traitement des données les concernant.

Ils peuvent exercer ces droits, en adressant au délégué à la protection des données de l'ARS par courrier (241 rue Garibaldi – 69003 Lyon) ou par courriel à l'adresse ars-ara-dpd@ars.sante.fr. Ils peuvent d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés s'ils considèrent que le traitement de données à caractère personnel les concernant constitue une violation du règlement général sur la protection des données et de la loi informatique et libertés

Art. 4 Date de prise d'effet

La présente décision, comprenant trois annexes, prend effet au mardi 13 mai 2020.

Lyon le 18 MAI 2020

Le Directeur Général
Docteur Jean-Yves GRALL

Décision n°2020-23-0024

Portant habilitation des agents de l'Agence et de ses sous-traitants autorisés à consulter et à enregistrer les données du traitement « SORMAS »

Le Directeur Général de
l'Agence Régionale de Santé Auvergne-Rhône-Alpes
Chevalier de la Légion d'Honneur
Chevalier de l'Ordre National du Mérite

Vu le code de la santé publique, notamment ses articles L. 1431-1 et L. 1431-2 ;

Vu le décret n° 2010-336 du 31 mars 2010 portant création des agences régionales de santé ;

Vu le décret du 6 octobre 2016 portant nomination de Monsieur Jean-Yves GRALL en qualité de directeur général de l'Agence Régionale de Santé Auvergne-Rhône-Alpes ;

Vu 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 ;

Vu la Loi Informatique et Liberté n° 78-17 du 6 janvier 1978, notamment son article 67 permettant une dérogation à l'article 66 ;

Vu 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, et abrogeant la directive 95/46/CE ;

Vu le contrat de sous-traitance passée entre l'ARS Auvergne-Rhône-Alpes et le Groupement de Coopération Sanitaire « SARA » portant sur la mise en œuvre du traitement « SORMAS » qui permet l'exploitation des données mentionnées aux articles 2 et 9 du décret n° 2020-551 (annexe n° 04) ;

Considérant que les finalités, décrites ci-après, de ce traitement mis en œuvre par l'ARS entrent dans le cadre de sa mission d'intérêt public (article 6-1-e du règlement (UE) 2016/679) et pour les motifs d'intérêt public (article 9-2-i du règlement (UE) 2016/679)

Considérant que le traitement mis en œuvre - comportant des données à caractère personnel dans le domaine de la santé - qui a pour seule finalité de répondre, en cas de situation d'urgence, à une alerte sanitaire et d'en gérer les suites, est soumis aux seules dispositions de la section 3 du chapitre IV du règlement (UE) 2016/679 du 27 avril 2016

Considérant qu'il appartient au Directeur Général d'habiliter spécialement les agents de l'Agence et ses sous-traitants, pour les données contenues dans le traitement « SORMAS », à être destinataire des données et à traiter certaines de ces données pour des finalités limitativement énumérées

Considérant que l'Agence Régionale de Santé, conformément aux dispositions de l'article 14 du décret 2020-551, doit s'assurer, notamment, que ses sous-traitants présentent des garanties de compétence suffisante pour assurer la mise en œuvre des mesures techniques et organisationnelles appropriées et le respect des règles de confidentialité ;

DECIDE

Art. 1 Finalité du traitement

L'outil SORMAS est un outil de « contact tracing » qui a pour finalité l'enregistrement, l'investigation et le suivi épidémiologique, par les agences régionales de santé (ARS), des cas de COVID-19 et des cas contacts, en vue notamment d'identifier les chaînes et cas groupés de contamination et de prendre les mesures destinées à limiter la propagation de l'épidémie.

Art. 2 Habilitation de l'ARS

Les habilitations décrites ci-dessous cesseront de produire leur effet six (6) mois après la fin de l'état d'urgence tel qu'il a été fixé par la Loi n° 2020-546 du 11 mai 2020 dans son article 1-I.

Art. 2.1 – Habilitation des agents de l'ARS

Les personnes nommément désignées en **annexe n° 01 « habilitation des agents de l'ARS – traitement SORMAS »**, pour les données listées à l'article 9 du décret n° 2020-551, sont habilitées à être destinataire :

- ⇨ des données enregistrées dans le traitement (art. 10-II dudit décret) ;
- ⇨ des données ayant fait l'objet d'une pseudonymisation (art. 10-III dudit décret).

Dans ce cadre, ils sont habilités à traiter ces données dans le cadre de la finalité décrite à l'article 1.

Guillaume Gras - ou en son absence Eric Virard – est désigné pour valider, par leur signature apposée sur l'annexe n° 01 et en les datant, les éventuels ajustements (retrait et ajouts) auxquels il sera procédé postérieurement à la date de signature de la présente décision sur ladite annexe.

Art. 2.2 – Habilitation des sous-traitants et de leurs collaborateurs

Les personnes nommément désignées en **annexe n° 02 « habilitation des sous-traitants de l'ARS et de leurs collaborateurs – traitement SORMAS »**, pour les données listées à l'article 9 du décret n° 2020-551, sont habilitées à être destinataire :

- ⇨ des données enregistrées dans le traitement (art. 10-II dudit décret) ;
- ⇨ des données ayant fait l'objet d'une pseudonymisation (art. 10-III dudit décret).

Dans ce cadre, ils sont habilités à traiter ces données dans le cadre de la finalité décrite à l'article 1.

Il appartient au(x) sous-traitant(s) d'apporter les garanties mentionnées à l'article 14 du décret n° 2020-551.

Guillaume Gras - ou en son absence Eric Virard – est désigné pour valider, par leur signature apposée sur l'annexe n° 02 et en les datant, les éventuels ajustements (retrait et ajouts) auxquels il sera procédé postérieurement à la date de signature de la présente décision sur ladite annexe.

Art. 2.3 – Spécimen de signature

Un spécimen de signature des agents, désignés aux articles 2.1 et 2.2, est apposé ci-dessous :

Nom et prénom	Signature	Paraphe
GRAS Guillaume Directeur Délégué Système d'Information, Affaires Immobilières et Logistiques		
VIRARD Eric Secrétaire Général		

Art. 3 Modalités d'enregistrement des données et d'accès au traitement « SORMAS »

Art. 3.1 – Modalités d'enregistrement des données

Les personnes et sous-traitants mentionnées aux annexes n° 01 et n° 02 enregistrent, concomitamment aux traitements mentionnés aux articles 1.1 et 2.1, les réponses formulées par les personnes appelées au questionnaire relatif à leur situation (patient zéro ou cas contact selon la définition des articles 1-II-1° et 1-II-2° du décret n° 2020-551).

Art. 3.2 – Modalités d'accès au traitement « SORMAS »

Ces modalités sont décrites dans le contrat de sous-traitance.

Pour ce faire, les personnes mentionnées aux annexes n° 01 et n° 02, dès lors qu'elles accèdent à l'application, sont réputées avoir accepté la « *Charte de Sécurité des données de contact tracing* » annexé à la présente (annexe n° 03).

Art. 4 Traitement automatisé des données

L'ARS Auvergne-Rhône-Alpes procède à un traitement de données personnelles sur le fondement de l'article 6 1. e) du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (RGPD) pour la permettre la désignation et d'habilitation des personnes autorisées à accéder à CONTACT-COVID.

Les données enregistrées sont conservées pendant la durée de l'habilitation précitée et ne peuvent être communiquées qu'aux destinataires suivants : personnels de l'ARS ARA et agents des sous-traitants.

Conformément au RGPD et à la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les personnes disposent d'un droit d'accès, de rectification, d'effacement et de portabilité des données les concernant. Ils peuvent également demander la limitation du traitement de leurs données ou s'opposer, pour des raisons tenant à leur situation particulière, au traitement des données les concernant.

Ils peuvent exercer ces droits, en adressant au délégué à la protection des données de l'ARS par courrier (241 rue Garibaldi – 69003 Lyon) ou par courriel à l'adresse ars-ara-dpd@ars.sante.fr. Ils peuvent d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés s'ils considèrent que le traitement de données à caractère personnel les concernant constitue une violation du règlement général sur la protection des données et de la loi informatique et libertés

Art. 5 Secret professionnel

Conformément à l'article 11-III de la loi du 11 mai 2020 susvisée, les personnes habilitées dans le cadre de la présente décision sont soumises au secret professionnel. En cas de révélation d'une information issue des données collectées dans les systèmes d'information pour lesquels elles sont habilitées, elles encourent les peines prévues à l'article 226-13 du code pénal.

Art. 6 Délais et voies de recours

La présente décision peut faire l'objet d'un recours contentieux auprès du tribunal administratif territorialement compétent dans le délai de deux mois à compter de sa notification.

La notification prend la forme de la transmission, sur leur adresse mail professionnelle, de la présente décision aux agents mentionnées aux annexes n° 01 et 02.

Art. 7 Date de prise d'effet

La présente décision, comportant trois annexes, prend effet au mardi 19 mai 2020.

Lyon le **26 MAI 2020**

Le Directeur Général
Docteur Jean-Yves GRALL