RÉPUBLIQUE FRANÇAISE

_____

Ministère des solidarités et de la santé

_____

Arrêté du … août 2021
pris en application du III de l'article 2-3 du décret n° 2021-699 du 1er juin 2021 prescrivant les mesures générales nécessaires à la gestion de sortie de crise sanitaire

NOR :

Le ministre des solidarités et de la santé et le secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et de la ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques,

Vu la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, et notamment la notification n° … ;

Vu la loi n° 2021-689 du 31 mai 2021 modifiée relative à la gestion de la sortie de la crise sanitaire, notamment le II de son article 1er ;

Vu le décret n° 2021-699 du 1er juin 2021 modifié prescrivant les mesures générales nécessaires à la gestion de sortie de crise sanitaire, notamment le III de son article 2-3,

Arrêtent :

Article 1

Pour être autorisée à se connecter aux dispositifs techniques développés par le ministère permettant le contrôle des justificatifs mentionnés à l'article 2-2 du décret du 1er juin 2021 susvisé, la personne qui propose un dispositif de lecture des justificatifs, autre que l'application mobile dénommée « TousAntiCovid Verif », adresse au directeur général de la santé un dossier de présentation permettant de vérifier que le dispositif proposé satisfait aux conditions fixées par la charte annexée au présent arrêté, ainsi que la charte signée.

Le directeur général de la santé autorise la connexion aux dispositifs techniques développés par le ministère permettant le contrôle des justificatifs des dispositifs conformes à la charte

annexée au présent arrêté. Cette autorisation consiste en une notification à la personne et la mise en place de la connexion.

En cas de constat de non-conformité d'un dispositif dont la connexion a été autorisée, l'accès aux dispositifs techniques développés par le ministère permettant le contrôle des justificatifs est suspendu sans délai. La personne est notifiée par le directeur général de la santé des raisons de cette suspension afin qu'elle puisse lui adresser un dossier de présentation mis à jour permettant de vérifier que le dispositif proposé satisfait de nouveau aux conditions fixées par la charte annexée au présent arrêté.

Article 2

Le présent arrêté sera publié au Journal officiel de la République française.

Fait le … août 2021.

Le ministre des solidarités et de la santé,

Olivier VERAN

Le secrétaire d'État auprès du ministre de l'économie, des finances et de la relance et de la ministre de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques,

Cédric O

ANNEXE

Charte applicable aux dispositifs de lecture des justificatifs mentionnés à l'article 2-2 du décret n° 2021-699 du 1er juin 2021 modifié prescrivant les mesures générales nécessaires à la gestion de sortie de crise sanitaire, autres que l'application mobile dénommé « TousAntiCovid Verif »

Définitions

Utilisateur : Est entendu dans la suite du document par le terme « utilisateur », tout personnel ou service chargé d'opérer un système de vérification

Usager : Est entendu dans la suite du document par le terme « usager », toute personne présentant son passe sanitaire pour le contrôle d'accès à un lieu/activité/service

Traitement du passe sanitaire : Est entendu dans la suite du document par le terme « traitement du passe sanitaire », tout traitement des données brutes présentes sur le passe sanitaire pour :

- contrôle de l'authenticité de la preuve via la vérification cryptographique de la signature électronique ;
- décompression du contenu du passe sanitaire ;
- vérification de la conformité des données aux règles sanitaires en vigueur pour l'activité concernée.

Respect des droits des usagers

Les systèmes tiers mettant en œuvre un service de vérification du passe sanitaire s'engagent à mettre en place et à respecter des mesures protectrices des droits des usagers (notamment les droits d'accès, de rectification et de limitation, articles 15, 16 et 18 du RGPD) et à informer les usagers à propos du traitement réalisé sur leurs données d'une manière simple et accessible (article 14 du RGPD).

Protection des données personnelles

1. Les passes sanitaires (2DDOC et DCC) au format QR Code, DataMatrix, ou texte, ainsi que les données qui y sont encodées, constituent des données de santé ne pouvant être stockées sur un système non habilité HDS.

2. Les données à caractère personnel présentes sur le DCC ne peuvent être transférées ou traitées pour d'autres finalités que le contrôle des règles sanitaires pour un accès à un lieu

ou une activité soumis à la présentation d'un passe sanitaire, tel que prévu par la loi n° 2021-689 du 31 mai 2021 modifiée relative à la gestion de la sortie de la crise sanitaire.

3. Les systèmes tiers mettant en œuvre un service de vérification de passe sanitaire s'engagent à :
    a. respecter l'ensemble des conditions posées par la loi n° 2021-689 du 31 mai 2021 modifiée relative à la gestion de la sortie de la crise sanitaire, notamment le II de son article 1er, et le décret n° 2021-699 du 1er juin 2021 modifié prescrivant les mesures générales nécessaires à la gestion de sortie de crise sanitaire, notamment le III de son article 2-3, relatifs à la mise en œuvre de la vérification du passe sanitaire par des systèmes et application tiers ;
    b. justifier du niveau de sécurité au regard des exigences de l'article 32 du RGPD ;
    c. justifier de l'absence de transfert illicite de données en application du chapitre V du RGPD ;
    d. ne pas conserver les données des passes sanitaires, ne pas les transmettre à des tiers ou les modifier ;
    e. mettre en œuvre des mesures de sécurité conformes à l'article 32 du RGPD, notamment le recours à des algorithmes de chiffrement robustes et à l'état de l'art ;
    f. ne pas transférer des données du passe sanitaire ou le résultat de son traitement en dehors de l'Union européenne, ou à défaut, justifier ces transferts et expliquer l'encadrement juridique et technique qui en garantie la licéité.

4. Conformément au décret n° 2021-699 du 1er juin 2021 modifié prescrivant les mesures générales nécessaires à la gestion de sortie de crise sanitaire, notamment le III de son article 2-3, l'affichage des données du passe sanitaire et des résultats de son traitement doit respecter les restrictions en vigueur pour les activités soumises au contrôle du passe sanitaire :
    a. Les systèmes tiers mettant en œuvre un service de vérification de passe sanitaire dans le cadre du passe « activités » s'engagent à restreindre tout affichage des données du passe sanitaire au strict minimum pour opérer le contrôle (Noms, Prénoms, Date de naissance, Résultat de la vérification) ;
    b. Les systèmes tiers mettant en œuvre un service de vérification de passe sanitaire pour un opérateur de transport, s'engagent à restreindre tout affichage des données du passe sanitaire au strict minimum (Noms, Prénoms, Date de naissance, Résultat de la vérification) dans tous les cas de déplacements pour lesquels les règles sanitaires spécifiques prévues par le décret du 1er juin 2021 modifié sont automatiquement appliquées à destination ou en provenance du territoire hexagonal, de la Corse ou des Outre-mer dans un premier temps, et certains pays d'Europe à moyen terme. L'utilisateur doit dans tous les cas se référer aux règles sanitaires en vigueur adaptées au déplacement donnant lieu à vérification.

5. Les personnes accédant aux résultats du traitement ou à toute information personnelle issue du passe sanitaire, doivent être identifiées, habilitées, et référencées dans un registre spécifique qui doit pouvoir être mis à disposition des autorités en cas de contrôle.

6. Les systèmes de vérification tiers s'engagent à ne conserver que temporairement le résultat d'un traitement d'un passe sanitaire, pour la durée d'un seul et même contrôle

d'un déplacement ou d'un accès à un lieu, établissement ou service visés par l'obligation de présentation du passe sanitaire.

a. Le résultat de la vérification du passe sanitaire est assorti d'une date/heure de fin de validité, calculée en fonction de la règle sanitaire, et d'un maximum de 72h. (Durée de vie du résultat = minimum(t+durée de vie passe sanitaire selon la règle, t+72h))
b. Ce résultat peut être conservé jusqu'à son utilisation pour le déplacement ou l'accès à un lieu, et au maximum jusqu'à son terme.
c. Les informations relatives à la nature et attributs de l'acte médical concerné par la preuve (vaccination, dépistage, rétablissement) ne peuvent être conservées sans habilitation HDS des systèmes concernés et en aucun cas dans le cadre du passe « activités », outre-mer et Corse.

Sécurité des systèmes d'information

Les systèmes tiers mettant en œuvre un service de vérification du passe sanitaire s'engagent à mettre en œuvre les mesures de sécurité nécessaires à la protection des mécanismes de vérification du passe sanitaire, en conformité avec le Référentiel général de sécurité[1] (RGS), les guides et recueils de bonnes pratiques de l'ANSSI[2], les recommandations de la CNIL[3] et notamment :

- Tout transfert ou traitement des données, dans le cadre de ces finalités, doit respecter les directives RGPD en termes d'hébergement ;
- Assurer la sécurité de l'exploitation des systèmes de transfert ou de traitement des données (veille vulnérabilités, application régulière des correctifs, etc.) ;
- Mettre en place les mesures de sécurisation des canaux informatiques et la surveillance du réseau hébergeant les systèmes de transfert et de traitement (firewalls, veille sécurité, etc.) ;
- Assurer la sécurité des postes d'administration et des serveurs d'hébergement des systèmes de transfert et de traitement contre les logiciels malveillants (cloisonnement réseau, filtrage des accès, antivirus si applicable, etc.) ;
- Assurer la sécurité physique et le contrôle d'accès physique aux équipements (systèmes informatiques, terminaux d'accès et d'administration, etc.) ;
- Mettre en place des politiques de protection de la vie privée et des libertés et en informer ses collaborateurs, et assurer la gestion et l'enregistrement des incidents de sécurité. Les personnels intervenants sur les systèmes de transfert et de traitement sont formés aux RGPD et aux obligations de protection de données.
- Le code source des systèmes tiers doit être publiquement accessible, à l'exception des secrets cryptographiques et des éléments de configuration des systèmes assurant la sécurité des systèmes informatiques utilisés.

[1] https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

[2] https://www.ssi.gouv.fr/administration/bonnes-pratiques/

[3] https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles

Sous-traitance

Toutes les relations de sous-traitance dans le cadre d'un traitement de données relatif au passe sanitaire font l'objet d'une contractualisation (article 28.3 du RGPD), qui porte notamment sur :

- l'objet et la durée du traitement ;
- la nature et la finalité du traitement ;
- le type de données et les catégories de personnes concernées ;
- les obligations et droits du responsable de traitement ;
- les obligations et missions d'assistance du sous-traitant ;
- le sort des données à l'issue du traitement ;
- les conditions de sous-traitance de 2nd rang ;
- et le cas échéant, les conditions de transfert des données du passe sanitaire ou le résultat de son traitement en dehors de l'Union européenne, en justifiant ces transferts et en expliquant l'encadrement juridique et technique qui en garantie la licéité.

Dossier type à transmettre à tousanticovid-rgpd@sante.gouv.fr

- La documentation des traitements et la cartographie des flux de données lors de la vérification ;
- L'architecture dans laquelle le système est mis en œuvre (DAT) ;
- L'architecture de sécurité et les mécanismes déployés pour répondre aux exigences de la charte en terme de SSI et de protection des données personnelles ;
- Le code source composant logiciel intégré aux services IN Groupe et de toute fonction manipulant les données du passe sanitaire ou le résultat de sa vérification (ce code source ne sera utilisé qu'à des fins de vérification a priori par la Direction Générale de la Santé).