DÉCISION D'EXÉCUTION (UE) 2022/483 DE LA COMMISSION

du 21 mars 2022

modifiant la décision d'exécution (UE) 2021/1073 établissant les spécifications techniques et les règles relatives à la mise en œuvre du cadre de confiance pour le certificat COVID numérique de l'UE établi par le règlement (UE) 2021/953 du Parlement européen et du Conseil

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2021/953 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) afin de faciliter la libre circulation pendant la pandémie de COVID-19 ([1]), et notamment son article 9, paragraphe 1,

considérant ce qui suit:

(1) Le règlement (UE) 2021/953 définit le certificat COVID numérique de l'UE qui prouve qu'une personne a été vaccinée contre la COVID-19, a effectué un test dont le résultat est négatif ou s'est rétablie d'une infection, aux fins de faciliter l'exercice, par son titulaire, de son droit à la libre circulation pendant la pandémie de COVID-19.

(2) Le règlement (UE) 2021/954 du Parlement européen et du Conseil ([2]) prévoit que les États membres doivent appliquer les règles énoncées dans le règlement (UE) 2021/953 aux ressortissants de pays tiers qui ne relèvent pas du champ d'application dudit règlement mais qui séjournent ou résident légalement sur leur territoire et qui ont le droit de se rendre dans d'autres États membres conformément au droit de l'Union.

(3) La recommandation (UE) 2022/290 du Conseil modifiant la recommandation (UE) 2020/912 concernant la restriction temporaire des déplacements non essentiels vers l'UE et la possible levée de cette restriction ([3]) prévoit que les ressortissants de pays tiers désireux d'entreprendre un voyage non essentiel depuis un pays tiers vers l'Union devraient être en possession d'une preuve valable de vaccination ou de rétablissement, telle qu'un certificat COVID numérique de l'UE ou un certificat COVID-19 délivré par un pays tiers visé par un acte d'exécution adopté en vertu de l'article 8, paragraphe 2, du règlement (UE) 2021/953.

(4) Pour que le certificat COVID numérique de l'UE soit opérationnel dans toute l'Union, la Commission a adopté la décision d'exécution (UE) 2021/1073 ([4]), qui établit les spécifications techniques et les règles permettant de compléter et de délivrer et vérifier de manière sécurisée les certificats COVID numériques de l'UE, de garantir la protection des données à caractère personnel, de définir la structure commune de l'identifiant unique du certificat et de délivrer un code-barres valide, sécurisé et interopérable.

(5) Conformément à l'article 4 du règlement (UE) 2021/953, la Commission et les États membres devaient mettre en place et gérer un cadre de confiance pour le certificat COVID numérique de l'UE. Ce cadre est en mesure de soutenir l'échange bilatéral de listes de révocation de certificats qui contiennent les identifiants uniques des certificats révoqués.

([1]) JO L 211 du 15.6.2021, p. 1.

([2]) Règlement (UE) 2021/954 du Parlement européen et du Conseil du 14 juin 2021 relatif à un cadre pour la délivrance, la vérification et l'acceptation de certificats COVID-19 interopérables de vaccination, de test et de rétablissement (certificat COVID numérique de l'UE) destinés aux ressortissants de pays tiers séjournant ou résidant légalement sur le territoire des États membres pendant la pandémie de COVID-19 (JO L 211 du 15.6.2021, p. 24).

([3]) Recommandation (UE) 2022/290 du Conseil du 22 février 2022 modifiant la recommandation (UE) 2020/912 du Conseil concernant la restriction temporaire des déplacements non essentiels vers l'UE et la possible levée de cette restriction (JO L 43 du 24.2.2022, p. 79).

([4]) Décision d'exécution (UE) 2021/1073 de la Commission du 28 juin 2021 établissant les spécifications techniques et les règles relatives à la mise en œuvre du cadre de confiance pour le certificat COVID numérique de l'UE établi par le règlement (UE) 2021/953 du Parlement européen et du Conseil (JO L 230 du 30.6.2021, p. 32).

(6) Le 1er juillet 2021, le service passerelle pour le certificat COVID numérique de l'UE (le «service passerelle»), qui constitue la partie centrale du cadre de confiance et permet l'échange sécurisé et fiable, entre les États membres, des clés publiques servant à vérifier ces certificats COVID, est devenu opérationnel.

(7) Le succès de l'application à grande échelle des certificats COVID numériques de l'UE a fait de ces derniers une cible pour les fraudeurs qui cherchent des moyens de délivrer des certificats frauduleux. Ceux-ci doivent donc être révoqués. En outre, il peut arriver que des États membres révoquent certains certificats COVID numériques de l'UE au niveau national pour des raisons médicales et de santé publique, par exemple lorsqu'un lot de vaccins administrés est ultérieurement jugé défectueux.

(8) Alors que le système de certificat COVID numérique de l'UE a la capacité de révéler immédiatement les certificats falsifiés, les certificats authentiques délivrés de manière illicite sur la base de faux documents, d'un accès non autorisé ou avec une intention frauduleuse ne peuvent pas être détectés dans les autres États membres, à moins que les listes de certificats révoqués générées au niveau national soient échangées entre les États membres. Il en est de même pour les certificats qui ont été révoqués pour des raisons médicales et de santé publique. Le fait que les applications de vérification utilisées par les États membres ne puissent détecter les certificats révoqués par d'autres États membres constitue une menace pour la santé publique et sape la confiance des citoyens dans le système de certificat COVID numérique de l'UE.

(9) Ainsi que le mentionne le considérant 19 du règlement (UE) 2021/953, pour des raisons médicales et de santé publique et dans le cas de certificats délivrés ou obtenus de façon frauduleuse, les États membres devraient pouvoir établir et échanger avec les autres États membres, aux fins dudit règlement, des listes de révocation de certificats dans des cas limités, notamment pour les certificats qui ont été délivrés par erreur, à la suite d'une fraude ou à la suite de la suspension d'un lot de vaccins contre la COVID-19 jugé défectueux. Les États membres ne devraient pas pouvoir révoquer les certificats délivrés par les autres États membres. Les listes de révocation de certificats échangées ne devraient contenir aucune donnée à caractère personnel autre que les identifiants uniques des certificats. En particulier, elles ne devraient pas indiquer la raison pour laquelle un certificat a été révoqué.

(10) Outre une information générale sur la révocation potentielle des certificats et sur les motifs possibles d'une telle mesure, les titulaires des certificats révoqués devraient être rapidement informés, par l'autorité de délivrance compétente, de la révocation de leur certificat et des motifs qui la justifient. Or, dans certains cas, et notamment celui des certificats COVID numériques de l'UE délivrés sur papier, retrouver et informer le titulaire du certificat révoqué peut être impossible ou exiger des efforts disproportionnés. En effet, les États membres ne devraient pas collecter plus de données à caractère personnel qu'il n'est nécessaire au processus de délivrance des certificats, aux seules fins de pouvoir informer les titulaires en cas de révocation.

(11) Il convient donc d'améliorer le cadre de confiance pour le certificat COVID numérique de l'UE, en soutenant l'échange bilatéral des listes de révocation de certificats entre les États membres.

(12) La présente décision ne s'applique pas à la suspension temporaire des certificats dont l'utilisation est imposée dans les cas déterminés au niveau national mais qui ne relèvent pas du champ d'application du règlement relatif au certificat COVID numérique de l'UE, par exemple lorsque le titulaire d'un certificat de vaccination a été testé positif au SARS-CoV-2. Elle est sans préjudice des procédures établies pour vérifier les règles d'entreprise relatives à la validité des certificats.

(13) Si, d'un point de vue technique, plusieurs architectures sont envisageables pour l'échange des listes de révocation, l'échange de ces listes via le service passerelle est l'option la plus appropriée, car elle limite les échanges de données au cadre de confiance déjà établi et elle réduit le nombre des éventuels points d'échec et le nombre des échanges entre les États membres par rapport à un autre système de pair à pair.

(14) Le service passerelle pour le certificat COVID numérique de l'UE devrait dès lors être amélioré afin de permettre l'échange sécurisé desdits certificats révoqués, en vue de leur vérification sécurisée par le service passerelle. À cet égard, il conviendrait d'appliquer des mesures de sécurité appropriées pour protéger les données à caractère personnel traitées dans le service passerelle. Afin de garantir un niveau élevé de protection, les États membres devraient pseudonymiser les attributs des certificats, au moyen d'un hachage irréversible à intégrer dans les listes de révocation. L'identifiant unique devrait ainsi être considéré comme une donnée pseudonymisée pour les opérations de traitement effectuées dans le cadre du service passerelle.

(15) Il convient en outre d'établir des dispositions relatives au rôle des États membres et de la Commission dans l'échange des listes de révocation de certificats.

(16) Le traitement des données à caractère personnel des titulaires des certificats, auquel il est procédé sous la responsabilité des États membres ou d'autres organisations publiques ou organismes officiels des États membres, devrait être effectué conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil ([5]). Le traitement des données à caractère personnel sous la responsabilité de la Commission en vue de gérer le service passerelle pour le certificat COVID numérique de l'UE et de garantir sa sécurité devrait respecter le règlement (UE) 2018/1725 du Parlement européen et du Conseil ([6]).

(17) Les États membres, représentés par les autorités nationales ou les organismes officiels désigné(e)s, définissent ensemble la finalité et les moyens du traitement des données à caractère personnel par l'intermédiaire du service passerelle pour le certificat COVID numérique de l'UE et sont, par conséquent, les responsables conjoints de ce traitement. L'article 26 du règlement (UE) 2016/679 impose aux responsables conjoints du traitement des données à caractère personnel l'obligation de définir, de manière transparente, leurs obligations respectives aux fins d'assurer le respect des exigences dudit règlement. Cet article prévoit également la possibilité que ces responsabilités soient définies par le droit de l'Union ou par le droit de l'État membre auquel les responsables du traitement sont soumis. L'accord visé à l'article 26 devrait être inclus dans l'annexe III de la présente décision.

(18) Le règlement (UE) 2021/953 confie à la Commission la tâche de soutenir ces échanges. La façon la plus appropriée de s'acquitter de cette tâche est de compiler, pour le compte des États membres, les listes de révocation de certificats soumises. La Commission devrait, par conséquent, se voir confier un rôle de sous-traitant, pour soutenir ces échanges en facilitant l'échange des listes via le service passerelle pour le certificat COVID numérique de l'UE pour le compte des États membres.

(19) La Commission, en qualité de fournisseur de solutions techniques et organisationnelles destinées au service passerelle pour le certificat COVID numérique de l'UE, traite, dans le service passerelle, les données à caractère personnel figurant dans les listes de révocation, pour le compte des États membres qui sont les responsables conjoints du traitement. Elle agit donc en tant que leur sous-traitant. Conformément à l'article 28 du règlement (UE) 2016/679 et à l'article 29 du règlement (UE) 2018/1725, le traitement par un sous-traitant doit être régi par un contrat ou un acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit le traitement. Il convient par conséquent de définir les règles régissant le traitement des données par la Commission en qualité de sous-traitant.

(20) La tâche de soutien de la Commission n'implique pas la création d'une base de données centrale telle que visée au considérant 52 du règlement (UE) 2021/953. Cette interdiction vise à éviter la création d'un registre central de tous les certificats COVID numériques de l'UE délivrés et n'empêche pas les États membres d'échanger des listes de révocation, ce qui est expressément prévu à l'article 4, paragraphe 2, du règlement (UE) 2021/953.

(21) Lorsqu'elle traite des données à caractère personnel dans le service passerelle pour le certificat COVID numérique de l'UE, la Commission est liée par la décision (UE, Euratom) 2017/46 de la Commission ([7]).

(22) L'article 3, paragraphe 10, du règlement (UE) 2021/953 autorise la Commission à adopter des actes d'exécution établissant que les certificats COVID-19 délivrés par un pays tiers avec lequel l'Union et les États membres ont conclu un accord sur la libre circulation des personnes autorisant les parties contractantes à restreindre cette libre circulation pour des motifs de santé publique de manière non discriminatoire et ne contenant pas de mécanisme d'intégration des actes juridiques de l'Union sont équivalents à ceux délivrés conformément audit règlement. Sur ce fondement, la Commission a adopté, le 8 juillet 2021, la décision d'exécution (UE) 2021/1126 ([8]) établissant l'équivalence des certificats COVID-19 délivrés par la Suisse.

([5]) 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 (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([6]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

([7]) La Commission publie des informations complémentaires sur les normes de sécurité applicables à tous les systèmes d'information de la Commission européenne sur la page https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en

([8]) Décision d'exécution (UE) 2021/1126 de la Commission du 8 juillet 2021 établissant l'équivalence des certificats COVID-19 délivrés par la Suisse avec les certificats délivrés conformément au règlement (UE) 2021/953 du Parlement européen et du Conseil (JO L 243 du 9.7.2021, p. 49).

(23) L'article 8, paragraphe 2, du règlement (UE) 2021/953 autorise la Commission à adopter des actes d'exécution établissant que les certificats COVID-19 délivrés par un pays tiers conformément à des normes et à des systèmes technologiques qui sont interopérables avec le cadre de confiance pour le certificat COVID numérique de l'UE et qui permettent de vérifier l'authenticité, la validité et l'intégrité du certificat, et qui contiennent les données figurant en annexe, doivent être considérés comme équivalents aux certificats COVID numériques de l'UE, aux fins de faciliter l'exercice, par les titulaires, de leur droit à la libre circulation au sein de l'Union. Ainsi que le mentionne le considérant 28 du règlement (UE) 2021/953, l'article 8, paragraphe 2, de ce dernier concerne l'acceptation des certificats délivrés par des pays tiers aux citoyens de l'Union et aux membres de leur famille. La Commission a déjà adopté plusieurs de ces actes d'exécution.

(24) Afin d'éviter les failles dans la détection des certificats révoqués qui relèvent de ces actes d'exécution, il devrait également être possible aux pays tiers dont les certificats COVID-19 ont été jugés équivalents en vertu de l'article 3, paragraphe 10, et de l'article 8, paragraphe 2, du règlement (UE) 2021/953, de communiquer les listes de révocation de certificats correspondantes au service passerelle pour le certificat COVID numérique de l'UE.

(25) Il peut arriver que certains ressortissants de pays tiers qui sont titulaires d'un certificat COVID-19 révoqué, délivré par un pays tiers dont les certificats COVID-19 ont été jugés équivalents en vertu du règlement (UE) 2021/953, ne relèvent pas de ce règlement ou du règlement (UE) 2021/954 au moment où le pays tiers concerné génère une liste de révocation comprenant leurs certificats respectifs. Or, il n'est pas possible de savoir, au moment où un pays tiers génère une liste de révocation de certificats, si tous ses ressortissants titulaires des certificats révoqués relèvent de l'un de ces deux règlements. Il n'est donc pas envisageable d'exclure les personnes qui ne relèvent du champ d'application d'aucun de ces deux règlements au moment où les listes de révocation de certificats de ces pays sont générées, et toute tentative à cet effet aurait pour résultat que les États membres ne pourraient pas détecter les certificats révoqués détenus par les ressortissants de pays tiers se rendant pour la première fois dans l'Union. Cependant, même les certificats révoqués de ces ressortissants de pays tiers seraient vérifiés par les États membres lorsque leurs titulaires entreraient sur le territoire de l'Union, et ensuite, lorsqu'ils voyageraient à l'intérieur de l'Union. Les pays tiers dont les certificats ont été jugés équivalents en vertu du règlement (UE) 2021/953 ne participent pas à la gouvernance du service passerelle et ne peuvent donc pas être des responsables conjoints du traitement.

(26) En outre, le système de certificat COVID numérique de l'UE s'est avéré être le seul système de certificat COVID-19 à être opérationnel à grande échelle au niveau international. En conséquence, le certificat COVID numérique de l'UE a gagné en importance au niveau mondial et a contribué à lutter contre la pandémie sur le plan international, en facilitant les voyages internationaux en toute sécurité et la reprise mondiale. Lors de l'adoption d'autres actes d'exécution au titre de l'article 8, paragraphe 2, du règlement (UE) 2021/953, de nouveaux besoins sont apparus en ce qui concerne la manière de compléter le certificat COVID numérique de l'UE. D'après les règles énoncées dans la décision d'exécution (UE) 2021/1073, le nom de famille est un champ obligatoire dans le contenu technique du certificat. Il est nécessaire de modifier cette exigence afin de favoriser l'inclusion et l'interopérabilité avec d'autres systèmes, étant donné que, dans certains pays tiers, il existe des personnes sans nom de famille. Dans les cas où le nom du titulaire du certificat ne peut être divisé en deux parties, le nom devrait être placé dans le même champ (nom ou prénom) du certificat COVID numérique de l'UE que celui du document de voyage ou d'identité du titulaire. Cette modification permettrait également de mieux harmoniser le contenu technique des certificats avec les spécifications actuellement en vigueur pour les documents de voyage lisibles par machine, publiées par l'Organisation de l'aviation civile internationale.

(27) Il convient donc de modifier la décision d'exécution (UE) 2021/1073 en conséquence.

(28) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 et a rendu un avis le 11 mars 2022.

(29) Afin de laisser aux États membres et à la Commission suffisamment de temps pour mettre en œuvre les modifications nécessaires pour permettre l'échange des listes de révocation de certificats via le service passerelle pour le certificat COVID numérique de l'UE, la présente décision devrait commencer à s'appliquer quatre semaines après son entrée en vigueur.

(30) Les dispositions prévues par la présente décision sont conformes à l'avis du comité institué en vertu de l'article 14 du règlement (UE) 2021/953,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

La décision d'exécution (UE) 2021/1073 est modifiée comme suit:

1) Les articles 5 *bis*, 5 *ter* et 5 *quater* suivants sont ajoutés:

«*Article 5 bis*

Échange de listes de révocation de certificats

1. Le cadre de confiance pour le certificat COVID numérique de l'UE permet l'échange de listes de révocation de certificats via le service passerelle central pour le certificat COVID numérique de l'UE (le «service passerelle») conformément aux spécifications techniques figurant à l'annexe I.

2. Lorsque les États membres révoquent des certificats COVID numériques de l'UE, ils peuvent communiquer des listes de révocation de certificats au service passerelle.

3. Lorsque les États membres communiquent des listes de révocation de certificats, les autorités de délivrance conservent une liste des certificats révoqués.

4. Lorsque des données à caractère personnel sont échangées via le service passerelle, le traitement est limité à la finalité consistant à soutenir l'échange d'informations relatives à la révocation. Ces données à caractère personnel ne sont utilisées qu'aux fins de vérifier le statut de révocation des certificats COVID numériques de l'UE délivrés dans le cadre du règlement (UE) 2021/953.

5. Les informations communiquées au service passerelle comprennent les données suivantes, conformément aux spécifications techniques figurant à l'annexe I:

a) les identifiants uniques pseudonymisés des certificats révoqués;

b) la date d'expiration de la liste de révocation de certificats qui a été communiquée.

6. Lorsqu'une autorité de délivrance révoque des certificats COVID numériques de l'UE qu'elle a délivrés en vertu du règlement (UE) 2021/953 ou du règlement (UE) 2021/954 et qu'elle a l'intention d'échanger les informations à ce sujet via le service passerelle, elle lui transmet les informations visées au paragraphe 5 sous la forme de listes de révocation de certificats, dans un format sécurisé, conformément aux spécifications techniques figurant à l'annexe I.

7. Les autorités de délivrance fournissent, dans la mesure du possible, une solution pour informer les titulaires des certificats révoqués de la révocation de leur certificat et du motif de cette mesure au moment où celle-ci est appliquée.

8. Le service passerelle rassemble les listes de révocation de certificats reçues. Il fournit des outils permettant de diffuser les listes aux États membres. Il supprime automatiquement les listes conformément aux dates d'expiration indiquées pour chaque liste communiquée par l'autorité concernée.

9. Les autorités nationales ou les organismes officiels désigné(e)s des États membres qui traitent des données à caractère personnel dans le service passerelle sont les responsables conjoints du traitement des données. Les responsabilités respectives des responsables conjoints du traitement sont réparties conformément à l'annexe VI.

10. La Commission est le sous-traitant des données à caractère personnel traitées dans le cadre du service passerelle. En sa qualité de sous-traitant pour le compte des États membres, la Commission veille à la sécurité de la transmission et de l'hébergement des données à caractère personnel au sein du service passerelle et respecte les obligations du sous-traitant énoncées à l'annexe VII.

11. L'efficacité des mesures techniques et organisationnelles destinées à assurer la sécurité du traitement des données à caractère personnel au sein du service passerelle est testée, analysée et évaluée régulièrement par la Commission et par les responsables conjoints du traitement.

Article 5 ter

Communication de listes de révocation de certificats par des pays tiers

Les pays tiers délivrant des certificats COVID-19 pour lesquels la Commission a adopté un acte d'exécution en vertu de l'article 3, paragraphe 10, ou de l'article 8, paragraphe 2, du règlement (UE) 2021/953 peuvent communiquer des listes de certificats COVID-19 révoqués relevant de cet acte d'exécution, que la Commission traitera, pour le compte des responsables conjoints du traitement, dans le service passerelle visé à l'article 5 *bis*, conformément aux spécifications techniques énoncées à l'annexe I.

Article 5 quater

Gouvernance du traitement des données à caractère personnel dans le service passerelle central pour le certificat COVID numérique de l'UE

1. Le processus décisionnel des responsables conjoints du traitement est encadré par un groupe de travail établi au sein du comité visé à l'article 14 du règlement (UE) 2021/953.

2. Les autorités nationales ou les organismes officiels désigné(e)s des États membres qui traitent des données à caractère personnel dans le service passerelle en qualité de responsables conjoints du traitement désignent des représentants pour siéger au sein de ce groupe.».

2) L'annexe I est modifiée conformément à l'annexe I de la présente décision.

3) l'annexe V est modifiée conformément à l'annexe II de la présente décision.

4) le texte de l'annexe III de la présente décision est ajouté en tant qu'annexe VI.

5) le texte de l'annexe IV de la présente décision est ajouté en tant qu'annexe VII.

Article 2

La présente décision entre en vigueur le troisième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Elle est applicable quatre semaines après son entrée en vigueur.

Fait à Bruxelles, le 21 mars 2022.

Par la Commission
La présidente
Ursula VON DER LEYEN

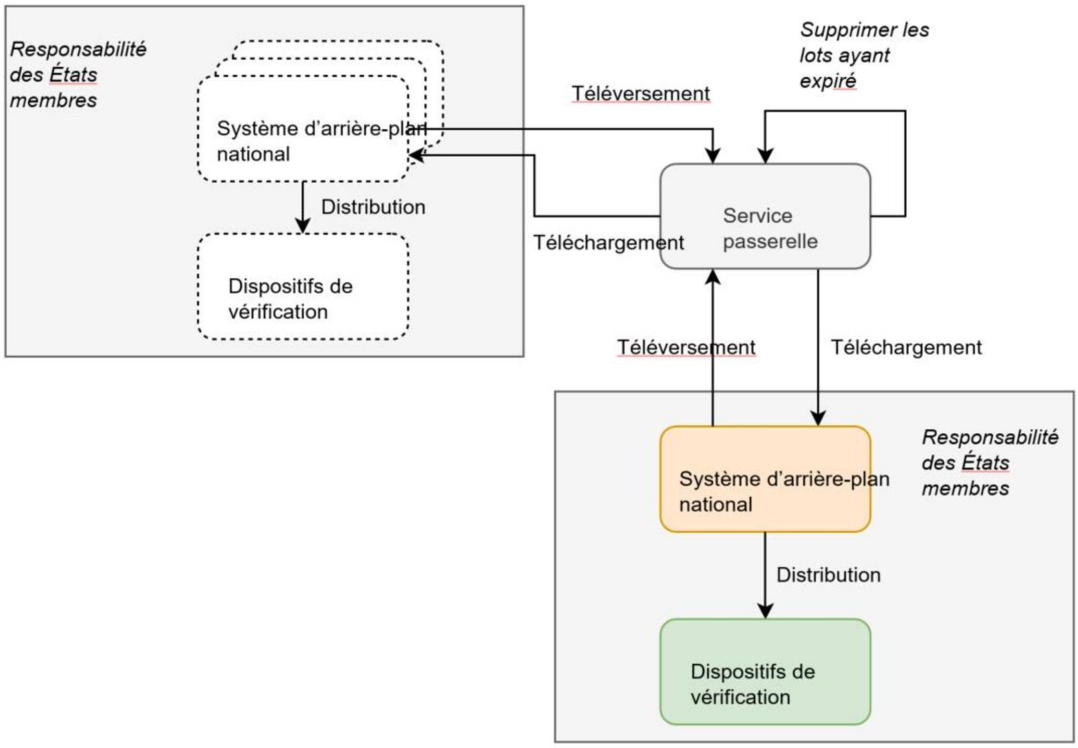
ANNEXE I

À l'annexe I de la décision d'exécution (UE) 2021/1073, la section 9 suivante est ajoutée:

«9. **SOLUTION DE RÉVOCATION**

9.1. **Établissement des listes de révocation de DCC (*DCC Revocation List* — DRL)**

Le service passerelle fournit des points de terminaison (*endpoints*) et une fonctionnalité pour conserver et gérer les listes de révocation:



9.2. **Modèle de confiance**

Toutes les connexions sont établies par le modèle de confiance type du DCCG par les certificats NB_{TLS} et NB_{UP} (voir gouvernance des certificats). Toutes les informations sont assemblées en paquet et chargées par messages CMS afin que leur intégrité soit garantie.

9.3. **Construction des lots**

9.3.1. *Lot (Batch)*

Chaque liste de révocation contient une ou plusieurs entrées et est assemblée en paquet par lots contenant un ensemble de hachages (*hashes*) et leurs métadonnées. Un lot est immuable (*immutable*) et définit une date d'expiration qui indique à quel moment le lot peut être supprimé. La date d'expiration de tous les éléments du lot doit être exactement la même, ce qui signifie que les lots doivent être regroupés par date d'expiration et par DSC signataire. Chaque lot contient au maximum 1 000 entrées. Si la liste de révocation comporte plus de 1 000 entrées, des lots multiples sont créés. Une entrée ne peut apparaître que dans un seul lot au maximum. Le lot est empaqueté dans une structure CMS et signé par le certificat NB_{UP} du pays de chargement.

9.3.2. *Index des lots (Batch Index)*

Lorsqu'un lot (*batch*) est créé, il se voit attribuer un ID unique par le service passerelle et est automatiquement ajouté dans l'index. L'index des lots indique les dates modifiées, par ordre chronologique ascendant.

9.3.3. *Comportement du service passerelle*

Le service passerelle traite les lots de révocation sans aucune modification: il ne peut ni mettre à jour, ni supprimer les lots, ni y ajouter aucune information. Les lots sont transmis à tous les pays autorisés (voir chapitre 9.6).

Le service passerelle surveille activement les dates d'expiration des lots et supprime les lots ayant expiré. Une fois le lot supprimé, le service passerelle renvoie une réponse «HTTP 410 Gone» pour l'URL du lot supprimé. De ce fait, le lot apparaît dans l'index des lots comme étant «supprimé».

9.4. **Types de hachage (*Hash Types*)**

La liste de révocation contient des hachages qui peuvent représenter différents attributs/types de révocation. Ces types ou attributs sont indiqués lors de l'établissement des listes de révocation. Les types actuels sont les suivants:

Type	Attribut	Calcul du hachage
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Seuls les 128 bits initiaux des hachages encodés en chaînes base64 (*base64 strings*) sont placés dans les lots et utilisés pour identifier le DCC révoqué ([1]).

9.4.1. *Type de hachage: SHA256 (Signature DCC)*

Dans ce cas, le hachage est calculé sur les octets (*bytes*) de la signature COSE_SIGN1 venant du CWT. Pour les signatures RSA, la signature entière sera utilisée comme entrée. Pour les certificats signés EC-DSA, la formule utilise la valeur r comme entrée:

SHA256(r)

[nécessaire pour toutes les nouvelles mises en œuvre]

9.4.2. *Type de hachage: SHA256(UCI)*

Dans ce cas, le hachage est calculé sur la chaîne UCI (*UCI string*) encodée en UTF-8 et convertie en un *byte array*.

[déconseillé ([2]), mais supporté pour des raisons de rétrocompatibilité]

9.4.3. *Type de hachage: SHA256(Issuing CountryCode+UCI)*

Dans ce cas, CountryCode encodé en une chaîne UTF-8 (*UTF-8 string*) concaténé avec l'UCI encodé avec une chaîne UTF-8. Il est ensuite converti en un *byte array* et utilisé comme entrée pour la fonction de hachage.

[déconseillé[2], mais supporté pour des raisons de rétrocompatibilité]

9.5. **Structure de l'API**

9.5.1. *API fournissant les entrées de révocation*

9.5.1.1. Objectif

L'API fournit les entrées des listes de révocation par lots et comporte un index des lots.

9.5.1.2. Points de terminaison (*endpoints*)

([1]) Veuillez également consulter, le point 9.5.1.2 pour les descriptions détaillées de l'API

([2]) Cela signifie que cette fonctionnalité ne doit pas être envisagée pour de nouvelles mises en œuvre, mais doit être supportée pour les mises en œuvre existantes pendant une période bien définie.

9.5.1.2.1. Point de terminaison pour le téléchargement des listes de lots

Les points de terminaison suivent une conception simple et renvoient une liste de lots avec un petit *wrapper* fournissant des métadonnées (*metadata*). Les lots sont triés par *date*, par *ordre (chronologique) ascendant*:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Remarque: Le résultat est limité par défaut à 1 000. Si le drapeau «more» est paramétré sur «true», la réponse indique qu'il est possible de télécharger davantage de lots. Pour télécharger davantage d'éléments, le client doit régler l'en-tête (*header*) If-Modified-Since sur une date qui ne doit pas être antérieure à la dernière entrée reçue.

La réponse contient un *JSON array* dont la structure est la suivante:

Champ	Définition
more	Drapeau booléen qui indique qu'il y a davantage de lots.
batches	*Array* avec les lots existants.
batchId	https://fr.wikipedia.org/wiki/Universally_unique_identifier
country	Code pays ISO 3166
date	ISO 8601 Date UTC. Date à laquelle le lot a été ajouté ou supprimé.
deleted	boolean. «True» si supprimé. Lorsque le drapeau «supprimé» est sélectionné, l'entrée peut être finalement retirée des résultats de la requête après 7 jours.

9.5.1.2.1.1. *Codes* de réponse

Code	Description
200	Tout OK.
204	Pas de contenu, si l'en-tête (*header*) «If-Modified-Since» n'a pas de correspondance.

En-tête de requête (Request Header)

En-tête	Obligatoire	Description
If-Modified-Since	Oui	Cet en-tête contient la dernière date téléchargée afin de n'obtenir que les résultats les plus récents. Lors de l'appel initial, l'en-tête devrait être réglé sur '2021-06-01T00:00:00Z'.

9.5.1.2.2. Point de terminaison pour le téléchargement des lots

Les lots contiennent une liste d'identifiants de certificats:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

La réponse contient un CMS comportant une signature qui doit correspondre au certificat NB_{UP} du pays. Tous les éléments du *JSON array* contiennent la structure suivante:

Champ	Obligatoire	Type	Définition
expires	Oui	String	Date à laquelle l'élément peut être retiré. ISO8601 Date/heure UTC
country	Oui	String	Code pays ISO 3166
hashType	Oui	String	Type de hachage des entrées fournies (voir Types de hachage)
entries	Oui	JSON Object Array	Voir tableau Entrées
kid	Oui	String	KID encodé en base64 du DSC utilisé pour signer le DCC. Si le KID n'est pas connu, la chaîne `UNKNOWN_KID` (à l'exclusion des `) peut être utilisée.

Remarques:

— Les lots sont regroupés par date d'expiration et par DSC — tous les éléments expirent en même temps et ont été signés par la même clé.

— L'heure d'expiration est une date/heure en UTC parce que l'EUDCC est un système mondial et que nous devons utiliser une heure dépourvue d'ambiguïté.

— La date d'expiration d'un DCC définitivement révoqué est fixée à la date d'expiration du DSC correspondant utilisé pour signer le DCC ou à l'heure d'expiration du DCC révoqué (auquel cas les heures *NumericDate/epoch* utilisées sont considérées comme se trouvant dans le fuseau horaire UTC).

— Le système d'arrière-plan national (*National Backend — NB:*) supprime des éléments de leur liste de révocation lorsque la date d'**expiration** est atteinte.

— Le *NB:* peut retirer des éléments de leur liste de révocation si le **kid** utilisé pour signer le DCC est révoqué.

9.5.1.2.2.1. Entrées

Champ	Obligatoire	Type	Définition
hash	Oui	String	128 bits initiaux du hachage SHA256 encodés en une chaîne base64 (*base64 string*)

Remarque: L'objet des entrées ne contient actuellement qu'un hachage, mais c'est un objet qui a été choisi, plutôt qu'un *JSON array*, pour permettre la compatibilité avec les modifications à venir.

9.5.1.2.2.2. Codes de réponse

Code	Description
200	Tout OK.
410	*Batch gone*. Le lot peut être supprimé dans le système d'arrière-plan national.

9.5.1.2.2.3. En-têtes de réponse

En-tête	Description
ETag	ID du lot

9.5.1.2.3. Point de terminaison pour le chargement des lots

Le chargement est effectué sur le même point de terminaison au moyen du verbe (*Verb*) POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Le lot est signé en utilisant le certificat NB_{UP}. Le service passerelle vérifie que la signature a été réglée par le NB_{UP} pour le *pays* concerné. Si la vérification de la signature échoue, le chargement échoue.

REMARQUE: Chaque lot est immuable (*immutable*) et ne peut pas être modifié après le chargement. Il peut toutefois être supprimé. L'ID de chaque lot supprimé est stocké, et tout chargement d'un nouveau lot portant le même ID est rejeté.

9.5.1.2.4. Point de terminaison pour la suppression des lots

Un lot peut être supprimé sur le même point de terminaison au moyen du verbe (*Verb*) DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

ou, pour des raisons de compatibilité, au point de terminaison suivant au moyen du verbe (*Verb*) POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6. **Protection de l'API/RGPD**

La présente section précise les mesures garantissant que la mise en œuvre respecte les dispositions du règlement (UE) 2021/953 en ce qui concerne le traitement des données à caractère personnel.

9.6.1. *Authentification existante*

Le service passerelle utilise actuellement le certificat NB_{TLS} pour authentifier les pays qui s'y connectent. Cette authentification peut être utilisée pour déterminer l'identité du pays connecté au service passerelle. Cette identité peut ensuite être utilisée pour mettre en œuvre le contrôle d'accès.

9.6.2. *Contrôle d'accès*

Pour pouvoir traiter légalement des données à caractère personnel, le service passerelle met en œuvre un mécanisme de contrôle de l'accès.

Le système passerelle met en œuvre une liste de contrôle d'accès (*Access Control List*) combinée à une sécurité fondée sur les rôles (*Role Based Security*). Ce système implique de tenir deux tableaux, l'un indiquant quels rôles peuvent appliquer quelles opérations à quelles ressources, l'autre indiquant quels rôles sont attribués à quels utilisateurs.

La mise en œuvre des contrôles requis par le présent document nécessite les trois rôles suivants:

RevocationListReader

RevocationUploader

RevocationDeleter

Les points de terminaison (*endpoints*) suivants vérifient si l'utilisateur (*User*) dispose du rôle (*Role*) de RevocationListReader; s'ils effectuent la vérification, l'accès est accordé et, si ce n'est pas le cas, le système passerelle renvoie un HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

Les points de terminaison suivants vérifient si l'utilisateur dispose du rôle de RevocationUploader; s'ils effectuent la vérification, l'accès est accordé et, si ce n'est pas le cas, le système passerelle renvoie un HTTP 403 Forbidden:

POST/revocation-list

Les points de terminaison suivants vérifient si l'utilisateur dispose du rôle de RevocationDeleter; s'ils effectuent la vérification, l'accès est accordé et, si ce n'est pas le cas, le système passerelle renvoie un HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Le service passerelle fournit également une méthode fiable permettant aux administrateurs de gérer les rôles liés aux utilisateurs de manière à réduire les risques d'erreurs humaines sans pour autant occasionner de charge pour les administrateurs fonctionnels.»

ANNEXE II

La section 3 de l'annexe V de la décision d'exécution (UE) 2021/1073 est remplacée par le texte suivant:

«3 ***Structures communes et exigences générales***

Le certificat COVID numérique de l'UE n'est pas délivré si, en raison de l'absence d'informations, tous les champs de données ne peuvent pas être correctement complétés conformément à la présente spécification. **Cela ne doit pas être interprété comme remettant en cause l'obligation des États membres de délivrer des certificats COVID numériques de l'UE.**

Dans tous les champs, il est possible d'indiquer les informations au moyen de la série complète de caractères UNICODE 13.0 encodés en UTF-8, sauf en cas de restriction spécifique à des ensembles de valeurs ou à des ensembles de caractères plus réduits.

La structure commune est la suivante:

"JSON":{

"ver":<information sur la version>,

"nam":{

<informations sur le nom de la personne>

},

"dob":<date de naissance>,

"v" ou "t" ou "r":[

{<informations sur la dose de vaccin ou sur le test de dépistage ou de rétablissement, une seule entrée>}

]

}

Des informations détaillées sur les différents groupes et champs sont fournies dans les points ci-après.

Lorsque les règles indiquent qu'un champ doit être ignoré, cela signifie que son contenu doit être vide et que ni le nom ni la valeur du champ ne sont autorisés dans le contenu.

3.1. ***Version***

Il y a lieu de fournir des informations sur la version. La gestion des versions s'effectue selon Semantic Versioning (semver: https://semver.org). En production, il s'agit de l'une des versions officiellement publiées (en cours ou officiellement publiées antérieurement). Pour plus de détails, voir le point Emplacement du schéma JSON.

Identifiant du champ	Nom du champ	Instructions
ver	Version de schéma	Correspond à l'identifiant de la version du schéma utilisée pour produire l'EUDCC. Exemple: "ver":"1.3.0"

3.2. ***Nom et date de naissance de la personne***

Le nom de la personne est le nom officiel complet de la personne, correspondant au nom indiqué sur les documents de voyage. L'identifiant de la structure est *nam*. Exactement 1 (un) nom de personne est indiqué.

Identifiant du champ	Nom du champ	Instructions
nam/fn	Nom(s)	Nom(s) du titulaire Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, tous les noms y étant inclus. S'il y a plusieurs noms, ils sont séparés par une espace. Les noms composés comprenant des traits d'union ou des caractères similaires ne doivent toutefois pas être modifiés.

		Exemples: "fn":"Musterfrau-Gößinger" "fn":"Musterfrau-Gößinger Müller"
nam/fnt	Nom(s) normalisé(s)	Nom(s) du titulaire translitteré(s) suivant la même convention que celle utilisée pour les documents de voyage lisibles par machine du titulaire (par exemple, les règles définies dans le document ICAO 9303, partie 3). Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, comportant uniquement les caractères A-Z et <. Longueur maximale: 80 caractères (selon la spécification du document ICAO 9303). Exemples: "fnt":"MUSTERFRAU<GOESSINGER" "fnt":"MUSTERFRAU<GOESSINGER<MUELLER"
nam/gn	Prénom(s)	Prénom(s) du titulaire. Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, tous les prénoms y étant inclus. S'il y a plusieurs prénoms, ils sont séparés par une espace. Exemple: "gn":"Isolde Erika"
nam/gnt	Prénom(s) normalisé(s)	Prénom(s) du titulaire translitteré(s) suivant la même convention que celle utilisée pour les documents de voyage lisibles par machine du titulaire (par exemple, les règles définies dans le document ICAO 9303, partie 3). Si le titulaire n'a pas de noms et a un prénom, le champ est ignoré. Dans tous les autres cas, exactement 1 (un) champ non vide, comportant uniquement les caractères A-Z et <. Longueur maximale: 80 caractères Exemple: "gnt":"ISOLDE<ERIKA"
dob	Date de naissance	Date de naissance du titulaire du DCC Date complète ou partielle sans heure, plage limitée à la période comprise entre le 1900-01-01 et le 2099-12-31. Exactement 1 (un) champ non vide si la date de naissance totale ou partielle est connue. Si la date de naissance n'est pas connue, même partiellement, le champ est une chaîne vide «». Les informations devraient correspondre à celles qui figurent sur les documents de voyage. Si des informations sur la date de naissance sont disponibles, l'un des formats ISO 8601 suivants est utilisé. Aucune autre option n'est supportée. YYYY-MM-DD YYYY-MM YYYY (Pour les parties manquantes de la date de naissance, l'application de vérification peut faire appel à la convention XX utilisée dans les documents de voyage lisibles par machine, par exemple 1990-XX-XX.) Exemples: "dob":"1979-04-14" "dob":"1901-08" "dob":"1939" "dob":""

3.3. ***Groupes pour les informations spécifiques au type de certificat***

Le schéma JSON supporte trois groupes d'entrées comprenant des informations spécifiques au type de certificat. Chaque EUDCC contient exactement 1 (un) groupe. Les groupes vides ne sont pas autorisés.

Identifiant du groupe	**Nom du groupe**	**Entrées**
v	Groupe Vaccination	Si ce groupe est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (une) dose de vaccin (une dose).
t	Groupe Test	Si ce groupe est présent, il contient exactement 1 (une) entrée décrivant exactement 1 (un) résultat de test.
r	Groupe Rétablissement	Si ce groupe est présent, il contient exactement 1 (une) entrée décrivant 1 (une) déclaration de rétablissement.»

ANNEXE III

«*ANNEXE VI*

RESPONSABILITÉS DES ÉTATS MEMBRES EN QUALITÉ DE RESPONSABLES CONJOINTS DU TRAITEMENT À L'ÉGARD DU SERVICE PASSERELLE POUR LE CERTIFICAT COVID NUMÉRIQUE DE L'UE AUX FINS DE L'ÉCHANGE DE LISTES DE RÉVOCATION D'EUDCC

SECTION 1

Sous-section 1

Répartition des responsabilités

(1) Les responsables conjoints du traitement traitent les données à caractère personnel par l'intermédiaire du service passerelle du cadre de confiance conformément aux spécifications techniques décrites à l'annexe I.

(2) Les autorités de délivrance des États membres demeurent l'unique responsable de la collecte, de l'utilisation, de la divulgation et de tout autre traitement d'informations relatives à la révocation qui ont lieu en dehors du service passerelle, y compris en ce qui concerne la procédure conduisant à la révocation d'un certificat.

(3) Il incombe à chaque responsable du traitement de traiter les données à caractère personnel au sein du service passerelle du cadre de confiance conformément aux articles 5, 24 et 26 du règlement général sur la protection des données.

(4) Chaque responsable du traitement met en place un point de contact doté d'une boîte aux lettres fonctionnelle qui servira à la communication entre les responsables conjoints du traitement, ainsi qu'entre ces derniers et le sous-traitant.

(5) Un groupe de travail institué par le comité visé à l'article 14 du règlement (UE) 2021/953 est mandaté pour trancher toute question relative à l'échange de listes de révocation et à la responsabilité conjointe du traitement de données à caractère personnel correspondant, ainsi que pour faciliter la communication d'instructions coordonnées à la Commission en qualité de sous-traitant. Le processus décisionnel des responsables conjoints du traitement est encadré par ce groupe de travail et régi par le règlement intérieur que ledit groupe doit adopter. À titre de règle de base, la non-participation de l'un des responsables conjoints du traitement à une réunion de ce groupe de travail qui a été annoncée au moins sept (7) jours avant sa convocation par écrit emporte approbation tacite des conclusions de cette réunion du groupe de travail. Tout responsable conjoint du traitement peut convoquer une réunion de ce groupe de travail.

(6) Les instructions à l'intention du sous-traitant sont envoyées par le point de contact de l'un des responsables conjoints du traitement, en accord avec les autres responsables conjoints du traitement, conformément au processus décisionnel du groupe de travail exposé au point 5 ci-dessus. Le responsable conjoint du traitement qui transmet les instructions devrait les communiquer par écrit au sous-traitant et en informer tous les autres responsables conjoints du traitement. Si la question en cause est urgente au point de ne pas permettre la tenue d'une réunion du groupe de travail visé au point (5) ci-dessus, une instruction peut néanmoins être fournie, mais peut être annulée par le groupe de travail. Il conviendrait de communiquer cette instruction par écrit, et tous les autres responsables conjoints du traitement devraient en être informés au moment de sa communication.

(7) The working group as set up per (5) above does not preclude any of the joint controllers' individual competence to inform their competent supervisory authority in accordance with article 33 and 24 of the General Data Protection Regulation. Une telle notification ne nécessite le consentement d'aucun des autres responsables conjoints du traitement.

(8) Dans le service passerelle du cadre de confiance, seules les personnes autorisées par les autorités nationales ou les organismes officiels désigné(e)s peuvent avoir accès aux données à caractère personnel échangées.

(9) Chaque autorité de délivrance tient un registre des activités de traitement effectuées sous sa responsabilité. La responsabilité conjointe du traitement peut être indiquée dans le registre.

Sous-section 2

Responsabilités et rôles en matière de traitement des demandes et d'information des personnes concernées

(1) Chaque responsable du traitement, en sa qualité d'autorité de délivrance, fournit aux personnes physiques dont il a révoqué le ou les certificats (les «personnes concernées») des informations sur ladite révocation et sur le traitement de leurs données à caractère personnel dans le service passerelle pour le certificat COVID numérique de l'UE aux fins de permettre l'échange de listes de révocation, conformément à l'article 14 du règlement général sur la protection des données, sauf si la fourniture de ces informations se révèle impossible ou exige des efforts disproportionnés.

(2) Chaque responsable du traitement fait office de point de contact pour les personnes physiques dont il a révoqué le certificat, et traite les demandes présentées par les personnes concernées, ou par leurs représentants respectifs, dans l'exercice de leurs droits conformément au règlement général sur la protection des données. Si un responsable conjoint du traitement reçoit une demande d'une personne concernée qui se rapporte à un certificat délivré par un autre responsable conjoint du traitement, il informe la personne concernée de l'identité et des coordonnées de ce dernier. Sur demande d'un autre responsable conjoint du traitement, les responsables conjoints du traitement se prêtent mutuellement assistance pour le traitement des demandes des personnes concernées et se répondent dans les meilleurs délais, et au plus tard dans un délai d'un mois à compter de la réception d'une demande d'assistance. Si une demande se rapporte à des données communiquées par un pays tiers, le responsable du traitement qui reçoit la demande la traite et informe la personne concernée de l'identité et des coordonnées de l'autorité de délivrance dans le pays tiers.

(3) Chaque responsable du traitement porte à la connaissance des personnes concernées le contenu de la présente annexe, notamment les modalités prévues aux points 1) et 2).

SECTION 2

Gestion des incidents de sécurité, notamment des violations de données à caractère personnel

(1) Les responsables conjoints du traitement se prêtent mutuellement assistance pour la détection et la gestion des incidents de sécurité, notamment des violations de données à caractère personnel, en lien avec le traitement de données dans le service passerelle pour le certificat COVID numérique de l'UE.

(2) En particulier, les responsables conjoints du traitement s'informent mutuellement des éléments suivants:

a) tout risque potentiel ou avéré pour la disponibilité, la confidentialité et/ou l'intégrité des données à caractère personnel faisant l'objet d'un traitement dans le service passerelle du cadre de confiance;

b) toute violation de données à caractère personnel, les conséquences probables de ladite violation et l'évaluation du risque pour les droits et libertés des personnes physiques, ainsi que toute mesure prise pour remédier à la violation de données à caractère personnel et pour atténuer le risque pour les droits et libertés des personnes physiques;

c) toute atteinte aux garanties techniques et/ou organisationnelles du processus de traitement au sein du service passerelle du cadre de confiance.

(3) Les responsables conjoints du traitement communiquent toute violation de données à caractère personnel relative au processus de traitement au sein du service passerelle du cadre de confiance à la Commission, aux autorités de contrôle compétentes et, lorsqu'ils y sont tenus, aux personnes concernées, conformément aux articles 33 et 34 du règlement général sur la protection des données, ou à la suite d'une notification par la Commission.

4) Chaque autorité de délivrance met en œuvre des mesures techniques et organisationnelles appropriées, destinées à:

a) garantir et préserver la sécurité, l'intégrité et la confidentialité des données à caractère personnel traitées de manière conjointe;

b) se prémunir contre le traitement, la perte, l'utilisation, la divulgation, l'acquisition non autorisés ou illégaux de toute donnée à caractère personnel en sa possession ou contre l'accès non autorisé ou illégal à ces données;

c) garantir que les données à caractère personnel ne sont ni divulguées ni rendues accessibles à des personnes autres que les destinataires ou les sous-traitants.

SECTION 3

Analyse d'impact relative à la protection des données

(1) Si, afin de s'acquitter des obligations qui lui incombent en application des articles 35 et 36 du règlement (UE) 2016/679, un responsable du traitement a besoin de s'informer auprès d'un autre responsable du traitement, il adresse une demande spécifique à la boîte fonctionnelle visée à la section 1, sous-section 1, point 4). L'autre responsable du traitement met tout en œuvre pour fournir les informations demandées.»

ANNEXE IV

«*ANNEXE VII*

RESPONSABILITÉS DE LA COMMISSION EN QUALITÉ DE SOUS-TRAITANT DES DONNÉES À L'ÉGARD DU SERVICE PASSERELLE POUR LE CERTIFICAT COVID NUMÉRIQUE DE L'UE EN VUE DE SOUTENIR L'ÉCHANGE DE LISTES DE RÉVOCATION D'EUDCC

La Commission:

(1) met en place et garantit une infrastructure de communication sécurisée et fiable pour le compte des États membres, qui prend en charge l'échange de listes de révocation communiquées au service passerelle pour le certificat COVID numérique.

(2) Afin de s'acquitter de ses obligations en qualité de sous-traitant des données du service passerelle du cadre de confiance pour les États membres, la Commission peut faire appel à des tiers comme sous-traitants ultérieurs; la Commission informe les responsables conjoints du traitement de toute modification envisagée concernant l'ajout ou le remplacement d'autres sous-traitants ultérieurs, donnant ainsi aux responsables du traitement la possibilité de s'opposer conjointement aux modifications de cette nature. La Commission veille à ce que les mêmes obligations en matière de protection des données que celles énoncées dans la présente décision s'appliquent à ces sous-traitants ultérieurs.

(3) La Commission ne traite les données à caractère personnel que sur instruction documentée des responsables du traitement, à moins qu'elle ne soit tenue d'y procéder en application du droit de l'Union ou du droit d'un État membre; dans ce cas, la Commission informe les responsables conjoints du traitement de cette obligation juridique avant de poursuivre l'activité de traitement, sauf si le droit concerné interdit la communication d'une telle information pour des motifs importants d'intérêt public.

Le traitement par la Commission comporte les éléments suivants:

a) l'authentification des serveurs d'arrière-plan nationaux, fondée sur les certificats des serveurs d'arrière-plan nationaux;

b) la réception des données visées à l'article 5 *bis*, paragraphe 3, de la décision téléchargées par les serveurs d'arrière-plan nationaux à l'aide d'une interface de programmation d'application mise à disposition, qui permet aux serveurs d'arrière-plan nationaux de télécharger les données pertinentes;

c) le stockage des données dans le service passerelle pour le certificat COVID numérique de l'UE;

d) la mise à disposition des données aux fins de leur téléchargement par les serveurs d'arrière-plan nationaux;

e) la suppression des données à leur date d'expiration ou sur instruction du responsable du traitement qui les a communiquées;

f) après la fin de la prestation de service, la suppression de toutes les données restantes, à moins que le stockage des données à caractère personnel ne soit exigé au titre du droit de l'Union ou du droit d'un État membre.

(4) La Commission prend toutes les mesures de sécurité à la pointe de la technique nécessaires sur les plans organisationnel, physique et logique pour préserver le service passerelle pour le certificat COVID numérique de l'UE. À cette fin, elle:

a) désigne une entité responsable de la gestion de la sécurité au niveau du service passerelle pour le certificat COVID numérique de l'UE, communique ses coordonnées aux responsables conjoints du traitement et veille à sa disponibilité pour réagir aux menaces pour la sécurité;

b) est chargée d'assurer la sécurité du service passerelle pour le certificat COVID numérique de l'UE, notamment en procédant régulièrement à des essais, des analyses et des évaluations des mesures de sécurité;

c) veille à ce que toutes les personnes auxquelles est accordé l'accès au service passerelle pour le certificat COVID numérique de l'UE soient soumises à une obligation contractuelle, professionnelle ou légale de confidentialité.

(5) La Commission prend toutes les mesures de sécurité nécessaires pour éviter de compromettre le bon fonctionnement opérationnel des serveurs d'arrière-plan nationaux. À cette fin, elle met en place des procédures particulières relatives à la connexion à partir des serveurs d'arrière-plan au service passerelle pour le certificat COVID numérique de l'UE. Il s'agit notamment:

a) d'une procédure d'évaluation des risques, afin d'identifier et d'estimer les menaces potentielles pour le système;

b) d'une procédure d'audit et de contrôle destinée:

i. à vérifier la correspondance entre les mesures de sécurité mises en œuvre et la politique de sécurité applicable;

ii. à contrôler régulièrement l'intégrité des fichiers système, les paramètres de sécurité et les autorisations accordées;

iii. à assurer une surveillance afin de détecter les atteintes à la sécurité et les intrusions;

iv. à appliquer des modifications afin de corriger les failles existantes en matière de sécurité;

v. à définir les conditions dans lesquelles il convient d'autoriser, notamment à la demande des responsables du traitement, la réalisation d'audits indépendants, y compris des inspections, et d'examens des mesures de sécurité, ainsi que de contribuer à ces opérations, sous réserve de conditions qui respectent le protocole n° 7 du TFUE sur les privilèges et immunités de l'Union européenne;

c) d'une modification de la procédure de contrôle afin de documenter et de mesurer l'incidence des modifications avant leur mise en œuvre et de tenir les responsables conjoints du traitement informés de toute modification susceptible d'affecter la communication avec leurs infrastructures et/ou la sécurité de celles-ci;

d) d'une procédure de maintenance et de réparation afin de préciser les règles et les conditions à respecter lors de la maintenance et/ou de la réparation des équipements;

e) d'une procédure relative aux incidents de sécurité afin de définir le système de signalement et d'escalade, d'informer sans délai les responsables du traitement concernés, d'informer sans délai les responsables du traitement afin qu'ils avertissent les autorités nationales de contrôle de la protection des données, de toute violation de données à caractère personnel et de définir une procédure disciplinaire pour traiter les atteintes à la sécurité.

(6) La Commission prend des mesures de sécurité physiques et/ou logiques à la pointe de la technique pour les installations hébergeant l'équipement du service passerelle pour le certificat COVID numérique de l'UE ainsi que pour les contrôles d'accès de sécurité et les contrôles d'accès aux données logiques. À cette fin, la Commission:

a) assure la sécurité physique, afin de mettre en place des périmètres de sécurité distincts et de permettre la détection des atteintes;

b) contrôle l'accès aux installations et tient un registre des visiteurs à des fins de suivi;

c) veille à ce que les personnes extérieures auxquelles l'accès est accordé soient accompagnées par du personnel dûment autorisé;

d) veille à ce que des équipements ne puissent être ajoutés, remplacés ou retirés sans autorisation préalable des organismes compétents désignés;

e) contrôle l'accès au service passerelle du cadre de confiance depuis les serveurs d'arrière-plan nationaux et l'accès depuis ledit service à ces derniers;

f) veille à ce que les personnes qui ont accès au service passerelle pour le certificat COVID numérique de l'UE soient identifiées et authentifiées;

g) réexamine les droits d'autorisation liés à l'accès au service passerelle pour le certificat COVID numérique de l'UE en cas d'atteinte à la sécurité touchant cette infrastructure;

h) préserve l'intégrité des informations transmises par l'intermédiaire du service passerelle pour le certificat COVID numérique de l'UE;

i) met en œuvre des mesures de sécurité d'ordre technique et organisationnel afin d'empêcher l'accès non autorisé aux données à caractère personnel;

j) met en œuvre, en tant que de besoin, des mesures visant à empêcher tout accès non autorisé au service passerelle pour le certificat COVID numérique de l'UE depuis le domaine des autorités de délivrance (c'est-à-dire: blocage d'une localisation/d'une adresse IP).

(7) La Commission prend des mesures pour protéger son domaine, y compris la rupture des connexions, en cas d'écart important par rapport aux principes et concepts de qualité ou de sécurité.

(8) La Commission tient à jour un plan de gestion des risques relatif à son domaine de compétence.

(9) La Commission surveille – en temps réel – la performance de tous les composants de service des prestations au sein du service passerelle du cadre de confiance, produit régulièrement des statistiques et tient des registres.

(10) Pour toutes les prestations du service passerelle du cadre de confiance, la Commission fournit un soutien en anglais, 24 heures sur 24 et 7 jours sur 7, par téléphone, courrier électronique ou portail web, et accepte les appels émanant des appelants autorisés: les coordonnateurs du service passerelle pour le certificat COVID numérique de l'UE et leurs services d'assistance respectifs, les responsables de projets et les personnes désignées de la Commission.

(11) La Commission aide les responsables conjoints du traitement au moyen de mesures techniques et organisationnelles appropriées, dans la mesure du possible, conformément à l'article 12 du règlement (UE) 2018/1725, à s'acquitter de l'obligation qui leur incombe de répondre aux demandes d'exercice des droits de la personne concernée prévus au chapitre III du règlement général sur la protection des données.

(12) La Commission soutient les responsables conjoints du traitement en fournissant des informations relatives au service passerelle pour le certificat COVID numérique de l'UE, dans le but de mettre en application les obligations énoncées aux articles 32, 33, 34, 35 et 36 du règlement général sur la protection des données.

(13) La Commission veille à ce que les données traitées au sein du service passerelle pour le certificat COVID numérique de l'UE soient incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès.

(14) La Commission prend toutes les mesures appropriées pour empêcher que les opérateurs du service passerelle pour le certificat COVID numérique de l'UE disposent d'un accès non autorisé aux données transmises.

(15) La Commission prend des mesures pour faciliter l'interopérabilité et la communication entre les responsables du traitement désignés du service passerelle pour le certificat COVID numérique de l'UE.

(16) La Commission tient, conformément à l'article 31, paragraphe 2, du règlement (UE) 2018/1725, un registre des activités de traitement effectuées pour le compte des responsables conjoints du traitement.»