**AVIS DU CEPD SUR LE PROJET DE RÈGLES INTERNES DE LA COMMISSION EUROPÉENNE RELATIVES À LA VÉRIFICATION NUMÉRIQUE DES CERTIFICATS COVID-19**

**INTRODUCTION**

* Le présent avis porte sur la demande de consultation formelle présentée au CEPD le 14 octobre 2021 par la Commission européenne (ci-après la «Commission») concernant son projet de règles internes relatives à la vérification numérique des certificats COVID-19.
* Le CEPD émet le présent avis conformément à l’article 58, paragraphe 3, point c), du règlement (UE) 2018/1725[[1]](#footnote-1) (ci-après le «règlement»).
* Le CEPD déplore d’avoir été consulté à ce stade de la procédure. L’évaluation contenue dans le présent avis est le résultat du peu de temps dont il a disposé pour formuler son avis après réception de la demande de consultation.

**CONTEXTE**

Par lettre du 14 octobre 2021, la Commission a consulté le CEPD sur son projet de règles internes (ci-après le «projet de décision») relatives à la vérification numérique des certificats COVID-19 des visiteurs dans les bâtiments de la Commission à Bruxelles et à Luxembourg. Aux fins de la consultation, la Commission a transmis au CEPD le projet de décision de la Commission modifiant la décision C(2020)5973 en ce qui concerne la vérification numérique des certificats COVID-19 et son protocole sur le scannage numérique desdits certificats. Le CEPD a accusé réception de la demande de consultation le jour même.

Selon les informations reçues, la Commission envisage de recourir à l’utilisation d’appareils portables dotés d’une application de lecture de codes QR afin de vérifier les certificats de vaccination, de test ou de rétablissement des visiteurs (ci-après les «certificats COVID-19» ou les «certificats») avant de leur donner accès aux bâtiments de la Commission à Bruxelles et à Luxembourg. Le contrôle des certificats COVID-19 sera réalisé par du personnel non médical (par exemple, des gardes de sécurité), les agents de contrôle des certificats, qui ont suivi une formation appropriée à la méthode de contrôle visuel et automatisé des certificats COVID-19 et au flux de travail correspondant. Les agents de contrôle des certificats utiliseront des applications mobiles spécifiques précisées dans le projet de décision. Ils positionneront l’écran de leur appareil de manière à ce que personne d’autre qu’eux ne puisse voir le résultat du scannage des certificats sur l’écran. Le résultat du contrôle sera soit valide, lorsqu’un signal de contrôle vert apparaît à l’écran, soit non valide, lorsqu’un point d’exclamation rouge apparaît. Lorsqu’il n’est pas possible de contrôler le code QR des certificats, par exemple en cas de problèmes techniques, ou à la demande du visiteur, le contrôle des certificats sera effectué manuellement par les agents de contrôle des certificats[[2]](#footnote-2).

Le contrôle des certificats se déroulera à l’intérieur du bâtiment, mais avant ou au niveau des postes de contrôle de sécurité (zone de transit). À l’entrée de la zone de contrôle, il doit être clairement indiqué que les certificats vont être contrôlés et les informations pertinentes en matière de protection des données doivent être visibles.

Le nom des visiteurs, le contenu du certificat et le résultat de la vérification numérique ne sont ni conservés, ni transférés ni traités d’une autre façon. Lorsqu’un visiteur est en possession d’un certificat non valide, il n’est pas autorisé à pénétrer dans le bâtiment ce jour-là. Le nom du visiteur ou toute autre donnée à caractère personnel ou donnée relative à la santé ne sera ni enregistré, ni stocké ni transféré à un autre service. À la demande d’un visiteur qui s’est vu refuser l’entrée dans le bâtiment, un certificat «Entrée refusée» peut être délivré. Ce certificat ne sera pas personnalisé et indiquera uniquement que l’accès au bâtiment a été refusé à une date spécifique.

**ANALYSE JURIDIQUE ET RECOMMANDATIONS**

**Licéité du traitement**

L’opération de traitement décrite ci-dessus, à savoir la vérification numérique de certificats impliquant le scannage d’un code QR, constitue un traitement au sens de la définition visée à l’article 2, paragraphe 5, du règlement et relève donc du champ d’application du règlement. Le CEPD considère que le traitement en question constitue une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données des individus.

La Commission fonde ce traitement sur l’article 5, paragraphe 1, point a), du règlement et fait valoir qu’il serait nécessaire à l’exécution d’une mission d’intérêt public. Conformément à l’article 5, paragraphe 2, du règlement, le fondement de ce traitement est inscrit dans le droit de l’Union, que le projet de décision fournit. Le traitement en cause peut révéler des données à caractère personnel concernant la santé, telles que les données relatives au statut vaccinal, les résultats de tests ou le rétablissement après une infection à la COVID-19. Les données relatives à la santé sont considérées comme une catégorie particulière de données à caractère personnel, dont le traitement est en principe interdit par l’article 10, paragraphe 1, du règlement. Le traitement de ces données aux fins de la vérification numérique des certificats COVID-19 sur le fondement du projet de décision relève des dérogations à l’article 10, paragraphe 2, points b), g) et i), du règlement. En outre, le traitement repose également sur l’article 1er *sexies*, paragraphe 2, du statut des fonctionnaires, étant donné que la Commission fait fonction de responsable du traitement en matière d’emploi et de sécurité sociale et est tenue de prendre des mesures pour protéger la santé et la sécurité des membres de son personnel. Cette base juridique peut également s’appliquer au traitement par la Commission de données à caractère personnel de personnes qui ne sont pas membres de son personnel.

La référence à la base juridique susvisée figure dans les considérants du projet de décision.

**Recommandation nº 1:** Bien que le CEPD considère que le traitement en question soit licite, il recommande que la Commission fasse référence à la base juridique dans le corps du projet de décision, dans le dispositif du texte et pas uniquement dans les considérants.

**Nécessité et proportionnalité du traitement et garanties appropriées**

L’article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la «Charte») dispose que, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à l’exercice des droits et libertés fondamentaux reconnus par celle-ci que si elles sont nécessaires.

Une limitation peut être nécessaire lorsqu’il y a lieu d’adopter des mesures aux fins de l’objectif d’intérêt général poursuivi. La nécessité implique également que les mesures adoptées soient moins intrusives que d’autres options pour atteindre le même objectif. Lorsqu’une mesure est jugée nécessaire, sa proportionnalité doit également être évaluée. On entend par proportionnalité le fait que les avantages résultant de la limitation doivent l’emporter sur les inconvénients que celle-ci entraîne pour l’exercice des droits fondamentaux concernés. Afin de réduire les inconvénients et les risques pour l’exercice des droits au respect de la vie privée et à la protection des données, il importe que les limitations contiennent des garanties adéquates.

En mettant en place le traitement en cause, la Commission a pour objectif de protéger la santé et la sécurité de son personnel à Bruxelles et à Luxembourg, en évitant la poursuite de la propagation de la COVID-19 tout en veillant à la continuité de l’activité. Modifier la finalité des certificats pour l’usage envisagé par la Commission, à savoir l’entrée des visiteurs dans ses bâtiments, devrait clairement avoir pour objectif de réduire le risque de transmission de l’infection et de protéger le personnel contre l’infection. Pour évaluer la nécessité de la mesure proposée, la Commission devrait tenir compte de paramètres tels que la prévalence de l’infection dans la population générale, la dynamique de la transmission dans ses bâtiments et le risque d’exposition du personnel.

Outre l’évaluation figurant dans la décision C(2021)6669 de la Commission, la Commission souligne que l’on constate une augmentation progressive du nombre de faux certificats COVID-19 illicites de grande qualité. S’assurer que les certificats présentés ne sont pas des faux et qu’ils appartiennent aux personnes qui les présentent ne peut se faire efficacement qu’en utilisant un dispositif de scannage pour valider les codes QR affichés sur les certificats. La Commission souligne que des solutions moins intrusives ont été étudiées et rejetées; la collecte des données agrégées relatives au statut vaccinal des visiteurs avant leur arrivée ne permettrait pas d’identifier les individus précis auxquels l’accès aux sites devrait être refusé en raison du risque sanitaire qu’ils pourraient représenter. En outre, le contrôle numérique des certificats est plus fiable et plus efficace qu’un contrôle manuel.

Le CEPD prend note du fait que le projet de décision ne fait pas référence à d’autres méthodes de contrôle moins intrusives, telles que des dispositions organisationnelles destinées à garantir la distanciation physique et les précautions sanitaires.

Conformément au principe de minimisation des données, le projet de décision prévoit un traitement limité à ce qui est nécessaire pour la vérification initiale et n’inclut pas l’enregistrement, la conservation, la transmission ou un autre traitement des données à caractère personnel. La plupart des applications de contrôle des codes QR n’affichent, en effet, qu’un sous-ensemble des données contenues dans le code QR. Toutefois, étant donné que la Commission entend utiliser les applications mobiles CovidScan et CovidCheck.lu pour vérifier les certificats délivrés conformément à l’article 3, paragraphe 1, du règlement (UE) 2021/953, comme l’indiquent les considérants 5 et 13 du projet de décision, les données à caractère personnel traitées sont plus nombreuses que ce qui est actuellement mentionné à l’article 2 *quater*, paragraphe 2.

Il ressort des spécifications du certificat[[3]](#footnote-3) qu’un identifiant unique de certificat, le pays d’administration du vaccin, l’émetteur du certificat et le numéro de série des doses administrées figurent parmi les informations traitées à chaque scannage d’un code QR. Ces métadonnées permettent, par exemple, de déduire le lieu de résidence durant la pandémie ou des informations concernant le fait qu’un visiteur a déjà reçu une dose booster ou fait partie d’un groupe prioritaire de la campagne de vaccination. Par conséquent, les personnes vulnérables pourraient être identifiées comme telles. En outre, l’indication du vaccin précis constitue une information supplémentaire inutile, alors que l’indication que le vaccin administré répond aux exigences prévues par le règlement (UE) 2021/953 aurait été suffisante.

En conséquence, le CEPD constate que la présente utilisation de codes QR n’est pas totalement conforme aux principes de la protection des données dès la conception et par défaut et de minimisation des données.

Conformément au principe de limitation des finalités, le projet de décision prévoit un traitement uniquement aux fins d’être autorisé à entrer dans un des bâtiments de la Commission.

Conformément au principe de transparence, les informations relatives au traitement devraient être communiquées à la personne avant le début du traitement et celle-ci devrait également y avoir aisément accès pendant le traitement. Le projet de décision prévoit que les informations relatives au traitement «sont communiquées aux personnes concernées au moyen d’une déclaration de confidentialité publiée sur le site web de la Commission ou par d’autres moyens».

Le CEPD prend note du fait que le traitement envisagé prévoit une intervention humaine raisonnable dans le processus de vérification et que les décisions concernant l’accès ou le refus d’accès aux bâtiments ne reposent pas uniquement sur un traitement automatisé.

Le CEPD relève que l’article 2 *quater*, paragraphe 4, du projet de décision prévoit la vérification manuelle des certificats COVID au cas où la vérification au moyen du code QR ne fonctionne pas ou à la demande de la personne concernée. Le CEPD souligne que le scannage des codes QR prévu au septième considérant pour détecter les faux certificats n’est efficace que si les personnes malveillantes ne peuvent pas provoquer le relâchement des normes de sécurité en présentant un code QR délibérément corrompu.

Comme indiqué au treizième considérant du projet de décision, la Commission prévoit d’utiliser les applications nationales de vérification des codes QR. Ces applications traitent des données à caractère personnel, y compris des catégories particulières de données. Nous observons qu’il n’est pas mentionné que la Commission a préalablement évalué si ces applications peuvent traiter des données à caractère personnel de manière licite, en se fondant sur le principe de la protection des données dès la conception et par défaut. Le CEPD observe que le traitement peut relever du champ d’application de ses lignes directrices sur la protection des données à caractère personnel traitées par des applications mobiles fournies par les institutions de l’Union européenne[[4]](#footnote-4). En tout état de cause le CEPD invite la Commission européenne à examiner soigneusement l’attribution des rôles de responsable du traitement et de sous-traitant pour le traitement par l’application mobile et par le système d'exploitation mobile.

Enfin, le CEPD observe que le traitement envisagé a un caractère exceptionnel et temporaire et s’appliquera jusqu’au 31 mars 2022, conformément à la clause de caducité prévue dans la décision C(2021)6669 de la Commission.

**Recommandation nº 2:** La Commission doit évaluer d’autres modalités organisationnelles qui garantiraient la distanciation physique et les précautions sanitaires et documenter le résultat de cette évaluation.

**Recommandation nº 3:** La Commission doit prévoir une procédure de vérification qui ne permette pas aux personnes malveillantes de contourner la vérification du certificat numérique. À défaut, son traitement ne permettra pas d’atteindre l’objectif de faire cesser l’utilisation de faux certificats.

**Recommandation nº 4:** Afin de faciliter l’exercice du droit à l’information des personnes concernées sur le traitement de leurs données à caractère personnel, la Commission doit placer des avis concernant la protection des données dans la zone de transit, là où les certificats des visiteurs seront contrôlés, par exemple au moyen d’affiches apposées sur les murs ou sur toute autre surface où les visiteurs peuvent les voir. Cela leur permettra de savoir comment la vérification se déroulera, quelles seront les données traitées, qui y aura accès et à qui adresser leurs questions ou leurs objectifs concernant le traitement.

**Recommandation nº 5:** S’agissant du traitement des données des applications de vérification, la Commission doit analyser la conformité des applications utilisées avec le règlement, compte tenu de l’obligation de protection des données dès la conception et par défaut, et documenter cette analyse.

**Recommandation nº 6:** La Commission doit inclure dans le projet de décision une référence au fait que la clause de caducité sera soumise à un réexamen périodique et déterminer la fréquence de ce réexamen.

**CONCLUSION**

À la lumière du principe de responsabilité, le CEPD attend de la Commission qu’elle mette en œuvre les recommandations susmentionnées, et décide de **clôturer le dossier**.

Fait à Bruxelles, le 18 octobre 2021

***[signature électronique]***

Wojciech RAFAŁ WIEWIÓROWSKI

1. 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). [↑](#footnote-ref-1)
2. La vérification manuelle des certificats COVID-19 ne relève pas du champ d’application du règlement et ne sera donc pas examinée dans le présent avis. [↑](#footnote-ref-2)
3. <https://ec.europa.eu/health/sites/default/files/ehealth/docs/covid-certificate_ison_specification_en.pdf> [↑](#footnote-ref-3)
4. https://edps.europa.eu/sites/default/files/publication/16-11-[07\_guidelines\_mobile\_apps\_en.pdf](https://edps.europa.eu/sites/default/files/publication/16-11-07_guidelines_mobile_apps_en.pdf) [↑](#footnote-ref-4)