

Deliberation 2021-103 of September 9, 2021 Commission Nationale de l'Informatique et des Libertés Nature of the

deliberation: Opinion Legal status: In force Date of publication on Légifrance: Saturday October 02, 2021 NOR:

CNIX2129633V Deliberation n° 2021-103 of September 9, 2021 providing an opinion on the draft decree amending decree no. 2021-699 of June 1, 2021 prescribing the general measures necessary for managing the end of the health crisis (request for opinion no. 21015378) The National Commission for Computing and Liberties, Saisie by the Minister of Solidarity and Health of a request for an opinion relating to the draft decree amending decree no. 2021-699 of June 1, 2021 prescribing the general measures necessary for managing the end of the health crisis; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms; Having regard to law n° 2021-689 of May 31, 2021 relating to the management of the end of the health crisis, and in particular its article 1. II.E; Having regard to decree n° 2021-699 of June 1, 2021 prescribing the general measures necessary for the management of the end of the health crisis; After having heard the report of Mrs Valérie PEUGEOT, commissioner, and the observations of Mr Benjamin TOUZANNE, commissioner of the Government, Issues the following opinion: The National Commission for Computing and Liberties (hereinafter the Commission) was seized urgently, on August 25, 2021, by the Minister for Solidarity and Health, then on August 30 2021 by amending referral, of a request for an opinion relating to a draft decree amending decree no. 2021-699 of June 1, 2021 prescribing the general measures necessary for managing the end of the health crisis. sanitary, on August 9, to many activities, some of which relate to daily life (restaurants, drinking establishments, long-distance interregional public transport, etc.) has led to an increase in fraud. The Ministry, in its capacity as controller, intends to implement data processing allowing the revocation of certificates identified as fraudulent so that they can no longer be used in the context of travel and access to places, establishments and events subject to the presentation of the health pass. In addition, in order to respond to the recommendations made by the CNIL in its previous opinions of June 7 and August 6, 2021, the ministry wished to develop a system allowing the generation of a health pass temporary, with a maximum validity of 48 hours, and containing a more limited number of data. Given the seriousness of the health consequences that the use of fraudulent certificates is likely to cause and the growing number of frauds, as well as for the reasons given below, the Commission considers that the changes proposed are legitimate and proportionate. However, with regard to the provisions relating to the fight against fraud, the draft

decree will have to be amended in order to expressly limit the purposes of the processing of personal data envisaged as well as the data entered in the exclusion list, and specify their retention periods. It also insists on the need to inform the holders of the certificates registered in the list at the time of registration, with regard to the impacts that the processing is likely to have on them. Finally, with regard to the temporary generation of a health activity pass, the Commission, which welcomes such a system, invites the Ministry to specify the draft decree on the data processed in this context. sanitary pass The Ministry intends to supplement Article 2-3 of Decree No. 2021-699 of June 1, 2021 referred to above in order to provide for the creation of a referencing database (hereinafter the exclusion list) allowing the storage of a digital fingerprint of certain QR and 2D-DOC code information identified as fraudulent. , to ensure that they can no longer be used as part of the obligation to present the health pass. The ministry clarified that the device must thus make it possible to fight against two types of fraud: the use of a certificate by a third party, as well as the use of a certificate issued illegally by an authorized person. In practice, when a certificate is identified as fraudulent, the information relating to it will be extracted from the information systems of the Ministry of Solidarity and Health so that the digital fingerprint of the certificate can be calculated before the integration of this one within the exclusion list. In order to allow the identification of certificates considered fraudulent, a copy of the exclusion list will be kept locally within the TousAntiCovid and TousAntiCovid Verif applications, as well as on the certificate converter. Therefore, when the persons or services authorized to control a health pass scan a QR-Code, the exclusion list will be queried in order to detect a possible match between the certificate presented and those declared as fraudulent. To this end, the draft decree lays down the principle of automated data processing with the aim of combating fraud, by revoking false or misappropriated health passes. On the procedures for registering certificates identified as fraudulent in the list exclusionThe Commission takes note of the Ministry's clarifications according to which the inclusion, by the Ministry, of a certificate in the exclusion list may be the consequence of the following events: The legitimate holder of the certificate sends a report to the support of TousAntiCovid and the health pass, or files a complaint with the competent authorities, after having noted fraudulent use or breach of confidentiality of his health pass; The certificate is the subject of an ongoing procedure, regardless of whether the latter was initiated following a complaint filed by the Ministry in the context of a whistleblower (for example, a person who reported the sale of certificates on social networks) or directly by the competent authorities. Commission points out that the registration is made at the initiative of the public authorities in the context of a suspicion of fraud and, consequently, without waiting for this to be established by the competent authorities in the matter. The Commission questioned the relevance of the inclusion in the

exclusion list of digital fingerprints of certificates corresponding to suspected but not established infringements, given the consequences for the persons concerned. In fact, it is possible that non-fraudulent certificates may thus be revoked, blocking access for the person concerned to places of daily life, or even causing them to lose the use of transport tickets, until they obtain of a new certificate. The Commission notes that such a choice is justified with regard to the objective of protecting public health pursued by the treatment, which requires limiting the risk of contamination by conditioning certain movements as well as access at certain places, establishments and events with the possession of a valid health pass. Furthermore, it notes that the system provides guarantees to ensure a balance between the various interests involved, such as the possibility of generating a new certificate (with a new identifier and a new digital signature) and this, almost instantaneously, following the person's request, either directly online (via the sdep.gouv.fr platform or via the attestation-vaccin.ameli.fr teleservice), or with authorized professionals (health professionals , primary health insurance fund, vaccination centres, etc.), as well as updating the exclusion list according to the outcome of legal proceedings. However, she insists that any suspicion of fraud should not lead to the revocation of a health pass. In this regard, it invites the Ministry to provide details on the nature of these suspicions in the impact assessment relating to data protection (AIPD) linked to the health pass. The Commission also emphasizes that properly informing the persons concerned at the time of registration of the digital fingerprint of their certificate in the exclusion list is a key element in ensuring the effectiveness of some of these guarantees. Under these conditions, and subject to comments made subsequently, the Commission considers that the system envisaged makes it possible to strike a balance between the rights of the persons concerned and the public health objectives pursued. Secondly, with regard to the integration of a digital certificate to the exclusion list following a report made by the legitimate holder of the certificate to the telephone support platform for the TousAntiCovid application and the health pass, the Commission insists on the need to ensure of the identity of said holder before proceeding to the effective integration of the certificate in the list, in order to avoid any malicious registration. Thirdly and lastly, the Commission takes note of the details that the exclusion list will be updated according to the outcome of the legal proceedings initiated, through ad hoc communications with the competent services. It considers, provided that such an update is likely to lead both to the addition of new certificates and to the deletion of those already in the exclusion list and for which the suspected offenses would not ultimately be characterized at the end of the procedure, that the system is such as to allow compliance with the principle of data accuracy, enshrined in Article 5.1.d of Regulation (EU) 2016/679 on the protection of personal data. personal character (GDPR). A purpose limited to the revocation of health passes identified as

fraudulentThe Commission takes note of the clarifications provided by the Ministry according to which the implementation of the processing of personal data envisaged has the sole purpose of allowing the revocation of certificates identified as fraudulent, revocation which will result in prohibiting travel and access to certain activities, subject to the obligation to present the health pass, to people who do not have a valid certificate. The Commission notes, in this respect, that the persons and services empowered to check the health pass will have to confine themselves to prohibiting access to their establishment and to informing the persons concerned of the measures to be taken to obtain a new certificate (in particular by contacting the telephone support platform for the TousAntiCovid application and the health pass). Therefore, the Commission considers that the application of Directive No. 2016/680 of April 27, 2016, known as police-justice, transposed in Title III of Law No. 78-17 of January 6, 1978, should be excluded. amended, when the intended device does not in itself have the purpose of allowing the prevention, investigation, observation or prosecution of criminal offenses or the execution of criminal convictions.

Consequently, it considers that the processing of personal data is subject to the GDPR and invites the ministry to ensure compliance with all the obligations set out in the text, in particular with regard to compliance with the principles provided for in the Article 5 of the GDPR. Moreover, it invites the Ministry to complete the draft decree in order to explicitly limit the purpose pursued by the data processing envisaged to the sole revocation of certificates reported as fraudulent, in order to allow the prohibition of travel and access to activities subject to the obligation to present the health pass to persons without a valid certificate. On the personal data included in the certificate exclusion list The draft decree provides for the integration of the codes associated with the supporting documents in an exclusion list and specifies that this will be made available to the public in order to facilitate the control of the health pass. clarified that the exclusion list will only contain the digital fingerprints generated from certain information of the QR-Codes identified as fraudulent, to the exclusion of any other personal data and in particular personal data as well as those concerning health data subjects. The Commission approves of this process. It considers that this is such as to ensure compliance with the principle of data minimization enshrined in Article 5.1.c of the GDPR and that such a limitation is essential, particularly with regard to the advertising of the list. However, the Commission notes that the wording of V of Article 2-3 as amended by the draft decree subject of this referral, does not allow the processing of data to be restricted solely to the digital fingerprints of the certificates in question: although that in principle the technical and architectural measures for implementing a processing operation do not have to appear in the regulatory act which governs it, it considers it essential in this case that this guarantee, which is essential for the protection of data at personal character,

appears in the decree. The Commission takes note of the Ministry's commitment to modify the text on this point. Furthermore, the Commission notes that the draft decree intends to modify paragraph 3 of Article 2-3-III of Decree No. 2021- 699 of June 1, 2021 referred to above, in order to add the technical fingerprint of the certificate to the list of data that the persons and services authorized to check the supporting documents required pursuant to 2° of A of II of Article 1 of the amended law of 31 May 2021 can read, insofar as such reading is essential to identify a possible match with the digital fingerprints present in the exclusion list. It draws the Ministry's attention to the fact that, as the project is being drafted, the reading of this new data is not planned for the checks of supporting documents linked to the travel health pass . Finally, if the draft text is not intended to modify the decree governing the TousAntiCovid application, which provides for the performance of statistical analyses, the Commission invites the Ministry not to collect additional usage data linked to this new treatment, i.e. concerning fraud and the related exclusion list. In any case and in general, it reminds the ministry that the decree governing the TousAntiCovid application only allows statistical analyzes to be carried out from anonymous data. On the information of the persons concerned The Commission notes that the information of the persons concerned will be issued through several communication channels made available to the public since the beginning of the health crisis. These are, in this case, institutional websites, the confidentiality policy of the TousAntiCovid application, as well as the addition of a statement on the paper receipts. On this last point, the Commission considers that the integration of information relating at least to the purpose of the system and the procedures for exercising rights and remedies (in particular, the telephone number of the support platform) directly on paper supporting documents (with a reference to more complete information online) is essential, since it ensures the transparency of the system for the entire population, including for people whose ability to access and use of digital tools remains limited. In addition, the ministry specified that the legitimate holder of the certificate will not necessarily be informed of the registration of the latter on the exclusion list at the time of the effective integration of the thumbprint in the list. However, while the Commission welcomes the fact that the user of the certificate in question, whether or not he is the legitimate holder of the medical pass, will be alerted after inclusion in the exclusion list (at the time of importing the certificate into the Carnet functionality of the TousAntiCovid application or when the user goes to this functionality as well as during a certificate check), it considers that the ministry should provide for the implementation of a procedure allowing the information of the legitimate holder at the time of the integration of his certificate in the exclusion list. Firstly, it considers that such information is essential with regard to the impact that such a device is likely to have on people and in particular on the legitimate holders of the health pass for whom integration in the

exclusion list would result neither from a complaint nor from a report on their initiative or who have not rec bear to the Notebook functionality of the TousAntiCovid application. In concrete terms, such a lack of information could, for example, lead a person to be refused access to a health establishment to which they must go for scheduled care (except in an emergency situation which does not require presentation of the health pass) or even that an employee cannot temporarily access his place of work, or when boarding a means of transport. The provision of a procedure allowing data subjects to generate, almost instantly, a new certificate (with a new unique identifier and a new signature) does not, according to the Commission, sufficiently limit the impact for people and, more particularly, those for whom the ability to access and use digital tools remains limited. Secondly, the Commission notes that the importance of such information also emerges from the spirit of the European legislator which specifies, for the attention of the Member States which implement such an exclusion list, that the holders of revoked certificates should be quickly informed of the revocation of their certificates and of the reasons for the revocation (recital 19 of the regulation relating to the European Covid digital certificate). Finally, the Commission notes that it will be up to the Ministry to identify the methods by which the information can be delivered, whether this is automated or requires human intervention, and in particular the procedure which will make it possible to retrieve the contact details of people to contact. In this respect, it recalls that, in the event that informing people involves accessing and reusing the contact information of the person concerned via the national screening information system (SI-DEP) and the information for the implementation, monitoring and management of vaccination campaigns against covid-19 (SI VACCINE COVID), the ministry must ensure the legality of such a system with regard to the texts governing these treatments, particularly with regard to the purposes pursued as well as the persons authorized to access the data. On the rights of the persons concerned The Commission recalls that the information delivered to the persons (at the different stages of the processing, as recalled above) must specify available to it with regard to the processing envisaged, as well as the procedures for exercising these rights. Furthermore, the clarifications provided by the Ministry on the exercise of certain rights guaranteed by the GDPR call for the following observations. Firstly, with regard to the right to object, the Commission takes note of the clarifications provided by the Ministry according to which the right of opposition, enshrined in Article 21.1 of the GDPR, remains applicable to the data processing envisaged. The Commission wonders about the benefit of providing, in this case, for a right of opposition with regard to the aims pursued, since this right cannot be justified when the fraud is serious, especially since, when it turns out that it is not, the fingerprints of the certificates must be erased in application of the principle of data accuracy (article 5.1.d of the GDPR) and the right to

erasure (article 17 of the GDPR) . It reminds the Ministry that Article 23 of the GDPR makes it possible to set aside this right and, where applicable, draws its attention to the need to ensure compliance with Article 23.2 of the GDPR. Secondly, the Ministry has clarified that the right of access may be exercised by taking cognizance of the exclusion list, publicly accessible, and underlines that the information on whether or not the certificate is in the processing in question will also be present within the Notebook functionality of the TousAntiCovid application. The Commission draws attention to the fact that these elements cannot constitute valid methods of responding to the exercise of the right of access by data subjects since: on the one hand, the reference to the exclusion list, publicly accessible, does not allow data subjects to know whether their personal data is present in the file, which only contains the digital fingerprints of the certificates, which are unreadable for the general public; on the other hand, the information provided via the Carnet functionality, if it makes it possible to know that the person's personal data is or is not in the file, only concerns people using the Carnet functionality of the TousAntiCovid application; moreover, it does not make it possible to obtain a copy within the meaning of Article 15.3 of the GDPR. on the possible remedies, once they have been informed of the inclusion of the digital fingerprint of their certificate in the exclusion list. Indeed, the persons concerned must be clearly informed of the procedures allowing them to generate a new certificate including a new unique identifier and a new digital signature. On the retention period The Commission notes that the decree remains silent on the retention period of the data (digital fingerprints of certificates) within the exclusion list. concerning travel abroad, should at least continue until 31 December 2021. In this respect, the Commission invites the Ministry to complete the draft decree in order either to indicate a precise date from which the data must be deleted, or to specify the criteria used to determine this duration. In any event, the Commission recalls that the digital fingerprints of the certificates for which the suspected infringements would not ultimately be established at the end of the procedure must be removed from the exclusion list, in application in particular of the principle of accuracy data provided for in Article 5.1.d of the GDPR. On the temporary generation of a health activity pass Article 1 provides for the addition of a 4° to Article 2-2 of Decree No. 2021-699 of the 1st June 2021 prescribing the general measures necessary for managing the end of the health crisis in order to integrate, into the certificates provided for by the texts, a so-called activity pass valid for a maximum period of 48 hours, on presentation of one of the certificates making up the health pass. This activity pass makes it possible, on the one hand, to considerably limit the personal data present in the QR code, these being restricted to the surname, first names, date of birth as well as the date and time to end of validity of the activity pass and, on the other hand, to restrict the duration during which the pass can be used. several

times in the context of its previous opinions, by contributing to the strengthening of the guarantees provided by the health pass in terms of the protection of personal data. Indeed, the minimization of data and the temporary nature of the pass make it possible to considerably reduce the risk that people, whether authorized or not to check the health pass, may have access to personal data of which they should not be aware (in particular data concerning the health of individuals) given the lack of encryption of the information stored in the QR code of the receipts. More specifically, the activity pass makes it possible in particular to respond to the observations made by the Commission, in its deliberation of August 6, 2021, on the need to identify technical and functional solutions to minimize the risks induced by the use of the application. TousAntiCovid instead of the health pass reading application called TousAntiCovid Verif. However, it draws the Ministry's attention to the need to ensure that the user journey is as simple as possible in order to ensure that the system is understood and accessible to as many people as possible. in its deliberation of June 12, 2021, that when the processing of personal data, implemented by a public authority, is specifically governed by a regulatory act, the list of data processed should, in principle, appear in the act . She then invited the ministry to complete the draft decree on this point, especially since the regulation relating to the European Covid digital certificate, which listed the data present in the European health pass and to which the ministry referred in its writings, was not intended to regulate the presentation of supporting documents for national uses such as the regulation of access to certain places, establishments or events. Similarly, the Commission considers that the draft decree, the subject of this referral, should be supplemented in order to specify the data present in this new activity pass. Finally, the Commission notes that the generation of this activity pass is only accessible via the TousAntiCovid application. Insofar as it provides additional guarantees in terms of personal data protection, it wonders about the possibility of developing a similar device for people who do not wish or cannot use the above application. mentioned, for example by allowing the generation of an activity pass within the sidep.gouv.fr platform or via the attestation-vaccin.ameli.fr teleservice. various devices impacted by the modifications of this draft decree (sanitary pass, TousAntiCovid application) must be updated prior to the implementation of the changes provided for by this draft decree and takes note of the ministry's commitment on this point . In particular, they must include a detailed assessment of the risks to the fundamental rights and freedoms of individuals generated by the creation of data processing relating to the fight against fraud in the health pass. The Commission recalls that the measures taken to guarantee the security of the data processed within the framework of the exclusion lists and to inform the persons whose digital fingerprint of the certificates is registered in the list as to the action to be taken, must also be applied to the alternative

pass reading devices to the TousAntiCovid Verif application. It suggests, in this respect, that the precise procedures for managing these lists appear explicitly in the decree mentioned in Article 2-3-III of Decree No. 2021-699 of 1 June 2021 referred to above. Finally, the Commission recalls to the Ministry that the technical methods for generating the digital fingerprints of the certificates must comply with the general security reference system (RGS) and noted refer to its appendix relating to cryptographic mechanisms. Marie-Laure DENIS