Deliberation 2020-135 of December 17, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday February 16, 2021NOR: CNIX2105104VDeliberation n° 2020-135 of December 17, 2020 providing an opinion on a draft decree amending decree no. 2020-650 of May 29, 2020 relating to the processing of data called "StopCovid" (request for opinion no. 20020446) The National Commission for Computing and Liberties, Seized by the Minister for Solidarity and health of a request for an opinion concerning a draft decree amending decree no. 2020-650 of May 29, 2020 relating to the processing of data called StopCovid; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data; 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; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 6-III; Having regard to Law No. 2020-1379 of November 14, 2020 authorizing the extension of the state of health emergency and laying down various measures for managing the health crisis; Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to Decree No. 2020-650 of May 29, 2020 relating to the processing of data called StopCovid; After having heard Mrs. Marie-Laure DENIS, President, in her report, and Mr. Benjamin TOUZANNE, Government Commissioner, in his observations; Issues the following opinion:The Commission has received an urgent request from the Minister for Solidarity and Health for an opinion relating to a draft decree amending decree no. 2020-650 of 29 May 2020 relating to data processing called StopCovid. The draft decree aims to change the conditions for implementing the data processing necessary for the operation of the application now called TousAntiCovid, in particular with a view to a new deconfinement and the reopening of certain establishments open to the public (ERP ). The changes envisaged are mainly aimed at introducing into the TousAntiCovid application a digital device for recording visits to such places, in order to facilitate the alert of people who have visited them over a time slot similar to that of one or more people. subsequently tested or diagnosed positive for COVID-19. The draft decree is also intended to allow the collection and processing of new data necessary for the fight against the epidemic and to integrate the successive evolutions of the application since the deployment of its version 2.0 last October. Taken as a whole , these modifications have the effect of changing the application towards a portal comprising several functionalities based, where applicable, on data processing pursuing distinct purposes and whose

implementation methods are specific to each of them. The Ministry wishes, for reasons of transparency, to regulate all the data processing likely to occur in the context of the use of the application, and not the only processing of health data which has made it necessary to take a decree in Conseil d'Etat taken after consulting the Commission. In addition to the fact that it seems that the decree could gain in readability, this referral calls for the following observations.As regards the device relating to the QR codes used in certain placesThis new device available in the TousAntiCovid application is intended to alert people users that they have been present in a closed place (hereinafter referred to as a contact place) allowing the gathering or meeting of several people and over a period during which they could have been contaminated by one or more people subsequently diagnosed or tested positive for COVID-19. It is based on a protocol called TAC-WARNING (hereinafter TAC-W), distinct from the ROBERT protocol and the contact tracking functionality. In practice, it is based on the provision, by ERP managers, of codes -QR that people are invited to scan, at the entrance or inside these premises, with the TousAntiCovid application. These QR codes and the time slot concerned are saved in the application. When a user reports himself as positive for the virus, the application sends the TAC-W central server the list of scanned QR codes, which therefore represents the list of ERPs he has visited. This list of contact locations is saved on the server. In addition, the application of each user regularly queries this central server by sending it the list of QR codes scanned by it and, when the TAC-W server identifies a match between one of the places reassembled and a contact place already registered , it notifies the user that he may have been exposed in one of the places he has frequented. The nature of the notification received may vary depending on the risk of contamination incurred, calculated by the TAC-W server on the basis of forthcoming recommendations from health authorities. Thus, people who visited a place during the same time slot as one or more people declared positive will be notified as a moderate risk contact. Beyond a certain threshold allowing the presence of a cluster to be identified, users may be notified as a high-risk contact as in the ROBERT protocol. On the necessity and proportionality of the device The introduction of such a feature should contribute to enhancing the health usefulness of the application by allowing a greater number of users to be informed of the risky contacts they have encountered. It is thus intended to complete the contact tracking functionality based on the use of Bluetooth proximity communication technology to assess the proximity between two smartphones, so as to take into account the particular risks of contamination linked to the frequentation of public buildings and other places hosting several people. In accordance with the recommendations of Public Health France, these places are in fact likely to present a high risk of exposure to the virus, when the people who frequent them are not able to ensure compliance with the gestures barriers (sports

halls, restaurants, bars, etc.), or a moderate risk when these barrier measures must be implemented but a breach of this protection is possible (public transport, cultural places, places of worship, etc. .). In the light of these elements, the Commission considers that the usefulness, at the current stage of the fight against the epidemic, of an additional system for identifying contacts at risk of contamination has been sufficiently demonstrated. rights to respect for private life and to the protection of personal data must not only be necessary for the pursuit of a general interest, as is the case here, but also be proportionate to that objective. It also stresses that the recording of the places frequented by individuals reveals information relating to their private life, or even sensitive data benefiting from a specific protection regime provided for by the General Data Protection Regulation (GDPR) in certain cases, such as when visiting places of worship. The processing of this information, and in this case by the public authorities, must therefore be subject to the greatest vigilance. In this respect, the Commission notes that the technical and functional architecture of the system provides several substantial guarantees, such as to ensure proportionality. In particular, the device does not use geolocation technology or involve the tracking of the movements of the users of the application. It is based on the sole storage in the TAC-W central server of the list of contact locations, without linking to any user identifier, thus minimizing the risk of linking all the locations frequented to the user and thus being able to reconstitute a history of some of his movements. In addition, if the interrogation of the central server requires that the application of a user transmit to him the list of the places he has visited associated with a timestamp, this interrogation does not involve , according to the elements provided by the ministry, the identifier of the application, the person or their terminal. The Commission also notes that the procedures for storing and comparing places frequented are subject to measures aimed at limiting the risks of identification of these places by third parties. Finally, the collection and processing of data carried out for this functionality is temporary and this data is strictly separated from that processed within the framework of the ROBERT protocol (no common identifier and separate central servers for the two functions). The Ministry has thus chosen an architecture in which the application queries the server by regularly sending the history of the places frequented and recorded by the application, and not that of an architecture in which the QR codes of the places contacts would be broadcast by the server to all users, allowing local comparison of contact locations on each application. Nevertheless, in the light of all the elements, the Commission considers that the proposed system is likely to reduce the risks posed by the processing of data to the fundamental rights and freedoms of the persons concerned and make the interference proportionate to the estimated usefulness of the device in the context of the current health crisis. It notes, however, that the extent of the collection and

processing of data to which users of the application will be subject is conditioned on certain choices which have not brought to its attention, on the precise list of ERP concerned, on the mandatory nature or not, for these establishments, to provide a QR code, or on the obligation imposed on the persons concerned to register their visits so that they can be alerted in the event of a risk of contamination. The Commission is therefore not fully in a position to assess the proportionality of the collection envisaged. It nevertheless takes note of the Ministry's clarifications according to which, in the event that the recording of visits constitutes an obligation for the persons concerned (customers , visitors, employees, etc.), two devices, one digital (QR codes), the other non-digital (a reminder book, for example), would be made available to them by the managers of the establishments concerned. It recalls that this is an essential guarantee, insofar as the use of an application on a voluntary basis cannot by nature condition access to certain places, in particular with regard to establishments which may receive the public (public transport, sports halls, restaurants, bars, etc.). In addition, it draws the Ministry's attention to the need to ensure that any non-digital alternative device complies with accessibility standards, in order to allow people with disabilities who do not use the application to access to the places concerned. It also notes that the precise perimeter of the system will soon be the subject of arbitration by the competent health authorities. In order to minimize the infringement of the right to the protection of personal data, the Commission recommends that the mandatory nature of the system be, where appropriate, limited to only ERPs presenting a high risk. It also calls for the greatest vigilance with regard to places whose frequentation is likely to reveal data subject to special protection, such as places of worship or trade union or political meeting places. It recommends that the system not be made compulsory in these places and that appropriate health measures, complementary to the system of health investigations under common law, be planned in order to sufficiently limit the risk of contamination. Finally, the Commission invites the Ministry to provide for new guarantees likely to further minimize the risks of user tracking, such as a limitation of the validity period of QR codes or even the use of single-use codes. On the provisions of the draft decree The integration of the aforementioned device of QR-codes in the TousAntiCovid application implies the modification of Decree No. 2020-650 of May 29, 2020 referred to above on several points and calls for the following observations from the Commission. Firstly, the Commission invites the Ministry to modify the second paragraph of article 1-I of the aforementioned decree n° 2020-650 in order to specify that the device is based on two distinct central servers. place, it is planned to add, to the draft article 1-II-7° of the said decree, a purpose reporting on the QR-code system as presented above. The Commission notes that the proposed wording is very close to the purpose of alerting pre-existing contact cases of the TousAntiCovid processing provided for in 1° of

the same provisions, which it does not appear absolutely necessary to modify on this point. It further notes that the specifications of the TAC-W protocol indicate that the specific objective of the solution also consists in allowing the identification of potential clusters in closed places gathering the public. It therefore requests the modification of the draft decree on these two points.Secondly, draft article 2-I-12° of decree no. frequenting a closed place allowing the gathering or meeting of several people obtained by a QR-code made available inside or in front of this place and specifies that this information is stored on the central server in order to inform the user that he has been in contact with a person diagnosed or tested positive for the covid-19 virus and having visited the same place during the same time slot. In this respect, the Commission considers that the draft decree defines the data collected in this context too broadly and therefore does not include the legal guarantees likely to ensure compliance with the principle of minimizing the data processed established by Article 5.1. c of the GDPR even though, in accordance with the elements transmitted by the ministry, these data appear effectively limited to what is necessary with regard to the purpose. It thus invites the Ministry to modify the draft decree in order to specify the categories of data collected for this new purpose and notes, in this respect, the absence of processing of the identifier of the application specific to each user. In addition, the current wording of the draft decree leaves open the possibility of general and undifferentiated storage, within the central server, of information relating to all the places frequented by all the users of the application. The Commission considers that the draft decree should be amended in order to specify, in accordance with the information provided by the Ministry, that only information relating to the places frequented by users who have declared themselves positive in the application are subject to a storage within the central server. This element indeed constitutes, in its eyes, a substantial guarantee. Thirdly, the draft decree specifies that the data are kept on the central server for fifteen days from their recording by the application of the mobile equipment the person concerned. If this duration does not call for any observation on the part of the Commission, it invites the Ministry to also specify in the draft decree the retention period of the data stored locally, as well as the possibility offered to the user of the application to delete, at any time, a place visited from his history, directly from his terminal. On the information of the people concerning the device relating to the QR codes It is planned that the persons concerned are informed of the device on place, via a display in the places concerned, as well as online within the TousAntiCovid application and on the website dedicated to the application. It specifies that information, including ible by the greatest number, must be placed at the place of the QR-code so that people are able to understand what it is related to. Finally, the Commission recommends, in order to ensure the homogeneity and compliance of these information measures with

Articles 12 and 13 of the GDPR, that standardized display models adapted to the different use cases be made available. of the establishments concerned within the platform used to generate the QR codes. On security measures As a preliminary point, the Commission underlines the effective consideration of the principles of data protection and security from the design of the system, which appear as constant concerns of the designers of the application. However, given the very tight deadlines in which it was called upon to make a decision, its analysis focused particularly on the device envisaged in the short term, even if the evolution of TAC-W towards a protocol qualified as dynamic will offer better guarantees. in terms of data protection and security, subject to its effective implementation conditions. comments from the scientific community will allow the continuous improvement of the device and the correction of any vulnerabilities, aimed at guaranteeing data security. It therefore invites the Ministry to continue and expand the openness approach governing the initial implementation of StopCovid. The Commission considers that such a system must, in particular, prevent any misuse of the epidemiological purpose and any abuse of the infrastructure considered. Thus, given the key role played by the central servers for tracking contacts and managing contact locations, it considers it necessary that suitable organizational and technical security measures be put in place in order to prevent any malicious act on this environment. .The Commission notes that the two protocols ROBERT and TAC-W operate independently, with in particular a logical separation of flows and respective servers, so that the data of each of the protocols cannot be linked, and to avoid any risk of inference of information. It notes that the protocol envisaged does not provide for the central server to know precisely the places frequented by the people declared positive. However, the server collects the unique and random identifiers contained in the QR codes returned when a user declares himself positive in the application. Although the correspondence table between this random identifier and the name or location of the establishment does not seem to be known by the server, this information exists elsewhere and could therefore be linked to the data stored on the server, which would be likely to weaken the overall level of security of the processing. In this respect, the Commission notes that when reporting the history of places frequented by a user who declares himself positive, the server applies a hash function to the identifier of the place contact, using the SHA256 algorithm and associating it with different values of a parameter, similar to a salt, without this implementation corresponding to the state of the art in the field to avoid comparisons . Although the Commission understands from this practice that it aims to limit the possibilities for third parties to re-identify the places frequented by users, it invites the Ministry to put in place, without delay, even more effective measures, such as the use of dynamic QR codes, the use of which is already planned by the ministry and which could substantially improve the security of

the data processed. example by implementing state-of-the-art cryptographic algorithms, and that it must be carried out in a robust way so that the simple observation of the communication does not allow to infer information on the users of the app. The Commission also recommends that the data stored on the server and that stored on the user's terminal be encrypted using a state-of-the-art cryptographic algorithm. It recalls in this respect that the encryption keys must be of sufficient size and must be managed under conditions ensuring their confidentiality. Finally, in order to prevent access to the history of locally registered places by persons other than the user of the application, the Commission recommends the implementation in the mobile application of adequate access restriction mechanisms. the prioritization of contact cases in access to examinations or screening tests Draft article 1-II-4° of decree no. 2020-650 of May 29, 2020 intends to allow users of the application with the status of contacts at risk of contamination to benefit from an examination or a screening test under priority conditions. In this respect, the Commission recalls that the fact of downloading and using the TousAntiCovid application does not imply, fact o, the possibility of benefiting from priority access to these examinations, only users notified as contacts at risk being concerned by this priority. It also notes that the proposed modification of the decree is part of the prioritization doctrine put in place by the Ministry in recent months, to deal with the increase in the number of people presenting themselves in the laboratories. of medical biology to be screened, prioritizing the screening of contact cases. Since this priority access will not be reserved for users of the application, but open to all contact cases, the Commission considers that this system cannot call into question the voluntary nature of the use of the application. It is nevertheless necessary that the information provided, in particular in the application itself, be unambiguous on the fact that the priority is attached to the quality of case-contact and not to the use of the application by itself. same.With regard to the expansion of the functionalities offered by the applicationThe draft articles 1-II-6° and 1-II-8° of decree n° 2020-650 of May 29, 2020 make it possible to broaden the purposes data processing in order to integrate the new functionalities of the TousAntiCovid application successively implemented since the deployment of version 2.0. They thus provide that the processing of data has the following purposes in particular: to inform users about the circulation of the virus at national and local level (when the user enters a postal code in the latter case), about promotional measures or actions , prevention and health education as well as on the application's usage data and to direct them towards other digital tools implemented for the management of the epidemic; to allow people using the application to store personal data on their smartphone in order to generate supporting documents required by public authorities. To do this, data such as surname, first name and address are recorded on the terminal so as not to have to be entered each time a new proof is generated. such

processing by decree. On the one hand, the administration has already implemented them within the framework of the TousAntiCovid application and certain administration websites also offer similar functionalities (in particular to allow the generation of supporting documents), without being for provided for by regulatory texts. On the other hand, personal data being stored and processed only locally, at the discretion and on behalf of the user alone, it does not appear that the public authorities are responsible for this processing, the mere provision of software to the public not constituting the implementation of personal data processing. In this sense, it should be noted that the provisions of the decree relating to this processing do not comply with the requirements of the Commission (duration of storage, list of recipients, etc.) but that it does not seem appropriate to regulate these aspects which, within the framework of the operation of the software in question, must remain at the discretion of the individual who uses the application. The Commission takes note of the fact that the Government wishes to make the provision of these tools to the public an obligation for the administration, enacted by the draft decree. It notes the guarantees provided by the Ministry with regard to these purposes, in a logic of data minimization and data protection from the design stage and by default. Thus, the data likely to be collected both for obtaining health information relating to a place of interest (identified by the postal code) and for the generation of derogatory travel certificates will be stored on the smartphone of the user and will not be processed on the central server. In addition, in accordance with the principle of limiting data retention, the postal code entered to obtain local information on the health situation will not be retained and the QR-code allowing you to have a derogatory travel certificate cannot be retained. more than twenty-four hours from its date of validity. The data provided by the user on the sites and applications referenced within TousAntiCovid are not subject to any data processing within the framework of the application. On the performance of statistical analyzes The draft article 1-II -5° of Decree No. 2020-650 of May 29, 2020 aims to specify the statistical purpose attributed to the processing by mentioning the performance of statistical analyzes from anonymous data from the application in order to adapt the necessary management measures to deal with the epidemic. According to the information provided by the Ministry, these statistical analyzes do not constitute processing for the purposes of research, studies and evaluation in the field of health, nor processing aimed at adapting the management measures necessary to the fight against the epidemic. Insofar as their sole purpose is to improve the performance of the application, the Commission requests that the draft decree be clarified on this point and on the data actually processed for this purpose.In the event that the development such statistics would require the implementation of read or write operations on the user's terminal, the Commission recalls that these may be exempted from consent provided that

these operations comply with Article 5 Commission guidelines on cookies and other trackers. Failing this, consent must be obtained, in accordance with article 82 of the law of January 6, 1978 as amended. In addition, the draft article 2-I-6° bis of decree n° 2020-650 of May 29, 2020 provides that the date of the reporting of the proximity history of contacts at risk of contamination by the covid-19 virus, the date of the last notification of the contact status at risk of contamination and, if applicable, the date of appearance of the first symptom and the date of the positive sample. First of all, the Commission takes note of the clarifications provided by the Ministry according to which such data will only be used in the context of carrying out the statistical analyzes mentioned above. In this regard, it recommends to the Ministry that the draft decree be clarified on this point. The Commission notes that these data, transmitted to the central server when the proximity history of contacts at risk of contamination are not linked to the identifiers of the people actually infected, which appears to be a protective minimization measure for the privacy of the people concerned. On the collection of new data for the contact tracking functionality via Bluetooth technology The draft decree intends to allow the collection new data as part of the contact tracing feature via Bluetooth technology. The draft article 2-I-7° of decree n° 2020-650 of May 29, 2020 authorizes the processing of the date of last contact of users with one of the people diagnosed or tested positive for COVID-19 or a approximation of the latter to more or less one day. According to the ministry, the processing of this data, inferred from the contacts reported by the application, is intended to improve the accuracy of the recommendations made to the notified user with regard to, on the one hand, the period to be respected to be tested following the last contact and, on the other hand, the period during which the latter must remain isolated. Indeed, to date, the recommended date is that of the notification which remains dependent on the time taken by the index case to be tested and declare positive in the application. The Commission therefore considers this data to be relevant with regard to the purpose of the processing. On the introduction of a push notification system The Commission notes that the DPIA transmitted mentions that devices running the iOS operating system now have use of a push notification system. Indeed, the ministry indicates that the proper functioning of the application on these devices requires, due to the technical limitations imposed by Apple, that it be reactivated periodically, failing which the regular interrogations of the central server to check the status of user's virus exposure could not occur. Technically, this system results in the sending of a notification which involves the sending of additional data to the central server as well as to the notification server of Apple, and in particular a unique identifier specific to the terminal and the application. Therefore, it invites the Ministry to complete the draft decree in order to mention, under the processed data, the technical data necessary for these push notifications. Furthermore, the

Commission recognizes the benefit of using this functionality, which is also common to most applications developed on iOS (in particular to notify the user of an update), in the context of the health crisis, as soon as when it wakes up the application for the purpose of querying the central server. However, it draws the ministry's attention to the fact that this functionality could lead to data transfers to the United States necessary for the proper technical operation of the application. It invites the ministry to approach the Apple company to have confirmation that this functionality does not involve a transfer or to try, if necessary and as far as possible, to avoid them. In any case, the information for users of the application must be clarified accordingly. On the duration of implementation of the application The Commission notes that the duration of implementation is consistent with that provided for processing Contact Covid and SI-DEP, the application only being useful in connection with the more general framework for conducting health investigations. On the impact analysis on data protection The Commission draws the attention of the Ministry to the need to regularly update the data protection impact assessment (DPIA) before implementing successive changes to the application. If the Commission notes that the ministry has initiated a management process risks including a privacy section, it regrets that the AIPD dedicated to the device relating to QR codes made available in certain places, in progress, was not sent to it in support of the referral. The Commission asks that this be sent to it and recalls in any case that the residual risks must be reduced to an acceptable level. Finally, it reiterates its call for transparency on this point and recommends that this DPIA be made public. PresidentMarie-Laure DENIS