Deliberation 2020-046 of April 24, 2020 National Commission for Computing and Liberties Nature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday February 08, 2022Deliberation n° 2020-046 of April 24, 2020 providing an opinion on a draft mobile application called "StopCovid" (request for opinion no. 20006919) The National Commission for Data Processing and Liberties, Seizure by the Secretary of State for Digital Affairs of a request for an opinion concerning the terms and conditions of the possible implementation of the StopCovid application with regard to French and European rules for the protection of personal data; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automated processing 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 personal data and the free movement of such data, and repealing Directive 95/46/EC; Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms, in particular its article 8 -I-2°e); Considering the decree n° 2019-536 of May 29, 2019 taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; After having heard Mrs Marie-Laure DENIS, President, in her report, and Mrs Nacima BELKACEM, Government Commissioner, in her observations, Issues the following opinion: April 2020, of a request for an opinion relating to the terms and conditions of the possible implementation of the StopCovid application with regard to French and European rules for the protection of personal data, on the basis of Article 8 -I-2°-e) of the aforementioned law n° 78-17 of January 6, 1978 (hereinafter, the Data Protection Act). This referral comes in the context of the state of health emergency linked to the COVID-19 epidemic, and more particularly the so-called deconfinement strategy. In this context, the Government plans to develop and offer an application, called StopCovid, available on ordiphones (smartphones) and other mobile devices. This application would make it possible to inform people who have downloaded it of the fact that they have been in the vicinity, in the near past, of people diagnosed with COVID-19 and having the same application, this proximity inducing a risk of transmission of the virus. virus. It would be an application for tracking contacts (or contact tracing), and not for tracking people exposed or diagnosed positive for the virus, which would be based in particular on the use of Bluetooth proximity communication technology to assess proximity between two smartphones, without using geolocation technology. It would be used solely on a voluntary basis and its implementation methods would aim to minimize any direct or indirect identification of the people who would use it. The documents annexed to the referral, which describe a protocol known as the ROBERT protocol, provide initial elements of reflection on the functional and technical architecture of such an application. In this context

and on the basis of this information, the Government questions the Commission on the existence or not, within the framework of the hypothesis of the implementation of such an application, of a processing of personal data within the meaning of Regulation (EU) 2016/679 of April 27, 2016 referred to above (hereinafter, the GDPR) and the Data Protection Act, on the identification of the legal basis for such processing, within the meaning of the same provisions, on the compliance of such a device with the rules for the protection of personal data and, where applicable, on the additional guarantees that should be provided. This Commission opinion aims to provide these elements of response and to enlighten the Government on the analysis of such an application of the p protection of personal data, it being specified that the deployment of this application as well as its exact methods of implementation, on the legal, technical and practical levels, have not yet been decided at this stage. The Commission asks, after the debate has been held in Parliament and if it has been decided to use such an instrument, that it be called upon again to decide on the final terms of implementation of the system. Commission emphasizes that it is fully aware of the seriousness of the health situation linked to the COVID-19 epidemic, the deaths and suffering it causes, as well as the difficulties linked to the confinement of people residing on national territory. The country is facing a health crisis of exceptional magnitude and the government has a duty to take the necessary measures to protect the population. The government's project is part of its action to fight the epidemic and reflects the desire not to leave aside any tool to contain the disease and to better manage the period of deconfinement. In addition, the design of the StopCovid application demonstrates the concern to protect people's privacy, in particular by preventing a list of people who declare themselves to be sick from being centralized in a server. However, it is also the duty of the Commission to point out that this project raises unprecedented questions in terms of the protection of privacy. Admittedly, it does not consist in following all the geographical movements of people: it is not a question of tracing individuals continuously. Nevertheless, it is a question of establishing, by collecting pseudonymous traces, the list of people to whom each holder of the application has been physically close, for a limited period, among all the holders of the application. Such collection, which is intended to apply to as wide a section of the population as possible, should be approached with great caution. The protection of privacy is guaranteed by the Constitution and other sources of law; the fact of collecting the lists of people that individuals have frequented strongly undermines them, which can only, if necessary, be justified by the need to respond to another constitutional principle, namely the protection of health, which stems from the eleventh paragraph of the preamble to the 1946 Constitution. The use of new forms of data processing may also create a phenomenon of habituation among the population that is likely to degrade the level of protection

of privacy and must therefore be reserved to certain exceptional situations, Finally, the Commission stresses that compliance with the rules for the protection of personal data, and in particular the proper information of the persons concerned, respect for their rights and, more generally, the provisions of the GDPR and the law Informatique et Libertés, is likely to promote the confidence of users of the application and, consequently, the effectiveness of the planned device. It is in the light of these general principles that the use of the Stopcovid application described in the referral should be studied. The existence of processing of personal data and in particular health data The device envisaged to date consists, on the one hand, of a mobile application which will be made available on mobile equipment (in particular smart phones and tablets) operating under the Android and iOS operating systems and, on the other hand, of a central server which will ensure the storage and the transmission of a certain amount of data necessary for the overall operation of the device. The government wonders about the existence of personal data processed within the framework of the system since, on the one hand, the downloading and use of the application would not require the provision of directly identifying data (such name, telephone number, e-mail address, etc.) and, on the other hand, that the downloaded application, and therefore its user, would only be identified by the central server by a pseudonym, i.e. non-identifying data by itself. The protocol described in the referral is thus based on a system associating with each downloaded application a permanent random identifier (hereinafter, the permanent pseudonym) then allowing the creation of several temporary random identifiers (hereinafter, the temporary pseudonyms). First of all, it should be emphasized that in order to be able to inform a user of a possible exposure to the virus, the central server must check whether there is a match between the pseudonyms assigned, during its installation, to the application of this user and those having been transmitted to the central server by the application of another person recognized as positive. As a result, a link remains between the pseudonyms and the downloaded applications, each application being itself installed on a terminal, which generally corresponds to a determined natural person. Because of this link, the Commission considers that the device will process personal data within the meaning of the GDPR. In addition, the collection of the temporary pseudonyms of the people with whom the user has been in contact could make it possible to reconstruct all the relationships he has had with other users of the application. In view of these elements, the Commission considers that the planned system is subject to the rules of protection of personal data, while recognizing that the protections taken provide a high degree of guarantee to minimize the risk of re-identification of the natural persons associated to the data stored, for a necessarily limited period, by the central server. Secondly, the central server would have the information according to which a user will or will not have received a

notification indicating that he has been exposed to the virus. The Commission notes that the entire architecture of the device envisaged tends to send back to the central server only the pseudonyms generated by the applications associated with the people with whom an infected individual has been in contact, and not the pseudonym of the latter. It emphasizes that this process minimizes the risk of re-identification of the infected person who is the source of an alert, in full compliance with the principles of protection of personal data.Thirdly, the Commission observes that data concerning health will be processed by the device. On the one hand, the triggering of an alert by an infected person is directly linked to the latter's state of health. On the other hand, the information that a person presents a sufficiently high risk of having contracted a disease, and leading in particular to him being informed of this by the application, is, according to the Commission's analysis, data concerning health and benefiting from the specific protection regime for this sensitive data provided for by the GDPR, informed by its recital 35, by the Data Protection Act, or even, depending on the intended uses, by the specific provisions of the Data Protection Code. public health relating in particular to the sharing and hosting of data. This information will be present in the central server. In addition, if technical precautions are taken to minimize the possibility of re-identification of the infected person by the people they have been in contact with and who have received the alert, this risk, which will depend on the context, and in particular on the number of people contacted during the period preceding the alert, may persist and should be taken into account. Nevertheless, the Commission points out that the presence of personal data does not, in principle, prevent the implementation of the system. However, it imposes the provision of appropriate safeguards, which are all the stronger as the technologies are intrusive, safeguards under which the attenuation of the possibilities of re-identification constitutes an essential measure. A system based on voluntary action A purpose limited to alerting persons exposed to the risk of contaminationThe Commission recalls that the principle of purpose limitation, enshrined in Article 5(1) (b) of the GDPR, is a cardinal principle of the protection of personal data: these must only be used only for a specific objective determined in advance. Any other use of the data is in principle prohibited. mobile equipment) has been in the vicinity, during the previous days, of that of a person who has subsequently been diagnosed with COVID-19, so that there is a risk that it in turn has been contaminated. The StopCovid application is not intended to monitor compliance with containment measures or other health obligations. The Commission also notes that the processing described in the referral is not intended to organize contact with the person alerted, to monitor the number of people infected or to identify the areas in which these people moved. An enrichment of the purposes of the application would require taking into account the right balance between these new objectives and the protection of privacy.An

application based on the voluntary participation of usersThe Commission notes that the government's plan consists of provision of the StopCovid application to the population residing in the national territory, the downloading and use of which would be based on a voluntary approach. In this regard, it considers that the voluntary nature of use, combined with increased transparency as to the mode of operation and the purposes of processing, is a decisive factor in ensuring confidence in the system and encouraging its adoption by a significant part of population. This volunteering should be explicitly provided for in the legal texts governing this device and in public information. In this respect, it should be emphasized that volunteering should not only result in the user choosing to download and then to implement the application (installation of the application, activation of communication by Bluetooth, or even declaring oneself positive for COVID-19 in the application) or the ability to uninstall it. Voluntary service also means that no negative consequences are attached to not downloading or using the application. Thus, access to tests and care can in no way be conditioned on the installation of the application. The use of an application on a voluntary basis should not condition either the possibility of moving around, in the context of the lifting of confinement, or access to certain services, such as for example public transport. The users of the application should not be forced to leave in possession of their mobile devices either. Public institutions or employers or any other person should not subordinate certain rights or access to the use of this application. This would also constitute, in the state of the law and according to the analysis of the Commission, discrimination. Under these conditions, the use of StopCovid may be regarded as truly voluntary. Different choices, which would be left to the legislator and whose strict necessity would then have to be demonstrated, would have a much greater effect on the right to the protection of personal data and to respect for private life. All the following analysis therefore only applies to a voluntary use application project meeting the aforementioned characteristics. The legal basis of the StopCovid application Article 6 of the GDPR and Article 5 of the Data Protection Act et Libertés provide that the processing of personal data is only possible in certain cases and for certain reasons exhaustively listed, which constitute the possible legal bases of the processing. In this case, the government wonders about the possibility of basing the StopCovid application on the legal basis of the consent of its users or, failing that, on the existence of a public interest mission to fight against COVID-19 outbreak. As a preliminary point, the Commission recalls that voluntary use of the application is compatible in law with one or other of these legal bases. It recalls that the law on the protection of personal data does not establish any hierarchy between the different legal bases and that the appropriate legal basis must be determined only on a case-by-case basis, in a manner adapted to the situation and the type of processing. Each legal basis is subject to specific conditions and has specific legal

consequences for the organization implementing the processing and for the persons concerned by it. The choice of the legal basis can therefore be a delicate operation, which does not call for a clear answer. However, if several legal bases may prove to be appropriate for the same processing, only one should be retained, considered in fine to be the most appropriate in the case in point. The Commission notes that the fight against he COVID-19 epidemic is a mission of general interest, the pursuit of which is primarily the responsibility of the public authorities. Consequently, it considers that the mission of public interest, within the meaning of Articles 6.1.e) of the GDPR and 5.5° of the Data Protection Act, constitutes the most appropriate legal basis for the development by the public authority of the StopCovid app. It notes that the European Data Protection Board considered, in its opinion No. 04/2020 of April 21, 2020, that this legal basis is the most appropriate for this type of application implemented by public authorities. The choice of this legal basis also makes it possible to reconcile in complete legal certainty the voluntary nature of the use of this application and the possible incentives of the public authorities for such use, in order to promote its use as widely as possible. The GDPR nevertheless requires that the purposes of the processing in question be necessary for the task of public interest in question and that it has a sufficient legal basis in a standard of national law. With regard to the specific case of the processing of data relating to the health of the persons concerned, the GDPR provides that the processing of such data may in particular take place, as in the present case, for reasons of public interest in the field of public health, such as protection against threats serious cross-border incidents affecting health , where such processing is necessary for those purposes and provided for by Union or national law and where that law provides for appropriate and specific measures to safeguard the rights and freedoms of the data subject (article 9-2-i of the GDPR). Without prejudice to the legal possibility of basing the processing of this data on another exception provided for in Article 9 of the GDPR, the Commission considers that these provisions seem the most appropriate to the situation of the StopCovid application. Under these conditions, the Commission recommends that the use of a voluntary contact tracing scheme to manage the current health crisis has an explicit and precise legal basis in national law. It asks the government, if necessary and regardless of the vector chosen, to refer it again to the draft standard governing the implementation of the application in question when the decision has been taken and the project clarified. Finally, it It may be noted that the StopCovid application project also involves access to stored information and the recording of information in the electronic communications terminal equipment of the persons concerned, within the meaning of Article 82 of the Data Protection Act. , namely in the mobile equipment of the persons implementing the application. In this respect, the Commission considers that these operations are strictly necessary

for the provision of the online communication service expressly requested by the person concerned and that they are therefore lawful. The admissibility of the invasion of privacy by a device contact tracingThe Commission recalls that by virtue of the constitutional protection of privacy, which results from Article 2 of the Declaration of the Rights of Man and of the Citizen, conventional protections, based in particular on the Charter of Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as well as the specific safeguards required by the GDPR, in particular with regard to the processing of health data in the context of a mission of public interest, the government must ensure that the invasion of privacy remains proportionate to the objective pursued. As has been indicated, the protection of health also constitutes an objective with constitutional value. On the one hand, compliance with the principle of proportionality will result in particular in the collection and storage of data limited to what is strictly necessary, in order to minimize the invasion of individuals' privacy. This fundamental guarantee implies in this case that the collection and processing of data carried out by the application is temporary, for a period limited to that of the usefulness of the device with regard to the purposes described above. It also implies that all data is deleted as soon as the usefulness of the application is no longer proven. In the event that statistical analysis or for scientific research purposes nevertheless proves necessary, this must be carried out as a priority on anonymized data or, failing that, in strict compliance with the rules set by the GDPR and the law. Computing and Freedom . On the other hand, it appears to the Commission that the invasion of privacy will only be admissible in this case if, given the inevitably incomplete and uncertain information at its disposal to deal with the epidemic, the government can rely on sufficient elements to have reasonable assurance that such a system will be useful in managing the crisis, and in particular in ending the confinement of the population, which in itself has a very strong impact on the freedom to come and go. However, while this type of device can potentially help public authorities monitor and contain the COVID-19 pandemic, by complementing the traditional methods of contact tracing used to contain the spread of epidemics, it nevertheless has limits, both intrinsic and linked to its insertion in an overall health policy, which are likely to affect its effectiveness. Firstly, its effectiveness depends on certain technical conditions, in particular the possibility for a sufficient proportion of the population to access to the application and to use it under good conditions. This means in particular that it would be desirable for this application to be available on enough mobile application stores (appstores , playstore , etc.) and compatible with the majority of telephones and other mobile equipment currently in circulation, both from a both hardware and software. The Commission also notes that the competition of several contact tracing applications, which must in any case

comply with the applicable provisions on the protection of personal data and are, as such, subject to the powers of control of the Commission, is likely to harm the effectiveness of the system.Secondly, the Commission underlines that the effectiveness of the system depends in part on its wide adoption, whereas a significant part of the population does not have suitable mobile equipment or may have difficulty installing and using the application. However, some of the people most vulnerable to the disease, as well as the youngest people who do not have a telephone, who could play a significant role in the spread of it, are particularly concerned. In addition, some people who will use the application are likely to contract the disease without showing symptoms, and therefore may not trigger the alert of their contacts. However, this element must be put into perspective by the fact that the system envisaged could also, because of the possible notification of an alert, encourage these people to be subject to a screening measure.Thirdly, the Commission also emphasizes that the effectiveness of the system envisaged depends on the correct calibration of the algorithms making it possible to identify an interaction likely to have generated contamination. Furthermore, the Commission recommends that the use of any form of automation of the decision to inform exposed persons be associated with the possibility for these persons to discuss with qualified personnel.Fourthly, a digital system for individualized monitoring of people can only be put in place as a complementary measure as part of an overall health response. In this sense, the Commission considers that the use of contact tracing applications cannot be an autonomous measure and calls, on this point, for particular vigilance against the temptation of technological solutionism. Also, it is up to the government to assess all the different actions to be put in place, such as the mobilization of health personnel and health investigators, the availability of masks and tests, the organization of screenings, the measures of support, information and service delivered to people who have received the alert, the ability to isolate them in suitable places, etc. This deployment must be part of an overall plan. On this point, the Commission welcomes the clarifications provided by the Secretary of State in charge of digital, who told it that the use of the application is envisaged in an integrated approach to the overall health strategy led in particular by the Ministry of Health and Solidarity. its effectiveness. Finally, it recommends that the impact of the system on the overall health strategy be studied and documented on a regular basis, so that its effectiveness over time can be assessed. This will allow the public authorities to decide in an informed manner whether or not to maintain it with regard, in particular, to the principles of proportionality and necessity. The Commission recommends that these analyzes be communicated to it, if necessary, in order to enable it to carry out its mission of monitoring compliance with the implementation of the planned system.Configuration of the applicationThe Commission points out that it does not only decides on the principle

of deploying an application such as that described in the referral, the precise terms and conditions of which could, if necessary, change. However, it wishes to provide the Government with the following clarifications as of now.Responsibility for processingThe identification of the data controller makes it possible to establish who is responsible for compliance with the rules on the protection of personal data. Given the sensitivity of the data collected, the Commission is of the opinion that the system should be designed in such a way that the ministry responsible for health or any other health authority involved in the management of the health crisis can assume responsibility for processing .On the need to carry out a data protection impact assessmentThe Commission draws the government's attention to the fact that, like any processing likely to present high risks (health data, large-scale use, systematic monitoring, use of a new technological solution), a data protection impact analysis (DPIA) must be carried out before any implementation of such a system. Publication of the DPIA is recommended for the purposes of transparency and in view of the current context. On the accuracy of the data The Commission notes that, in the technical protocol sent to it, it is envisaged that we could introduce false positives in the notifications sent to people in order to limit the risks of re-identification in certain types of attacks. It considers that this measure cannot and should not be implemented, since it would have the effect of falsely alerting people who have not had contact at risk, and who would therefore be encouraged to submit to voluntary confinement measures consisting of a self-imposed restriction of their individual freedoms. It emphasizes that maintaining the accuracy of the data is an overriding legal obligation under the GDPR and the Data Protection Act and that such a measure is not possible, under penalty of calling into question the compliance of the processing with regard to the applicable texts. On data security The security of personal data is an essential guarantee, given the sensitivity of this device. This security requires an exhaustive consideration of the conditions of implementation of the processing and a continuous improvement of the techniques, procedures and protocols put in place. Faced with the challenge of taking these requirements into account in a very short time, the Commission draws the Ministry's attention to this point. that it does not cover all the characteristics of the treatment and that the proposed protocol is still constantly evolving. It nevertheless considers it necessary to immediately draw the Government's attention to the following four points. Firstly, the Commission notes that the system envisaged includes a server responsible for centralizing the identifiers of exposed persons. In order to provide the highest possible guarantees against any misuse of purpose related to this choice, it considers it necessary that very high-level organizational and technical security measures be put in place, in accordance with an appropriate security model taking into account any malicious act. As such, it draws attention to the encryption keys allowing

access to the identifiers of the persons concerned, which could for example be protected via hardware security modules, as well as independent trusted third parties. Commission considers it necessary that measures be implemented both in the central server and in the application to avoid being able to recreate a link between these temporary pseudonyms and information specific to the terminal linked to Bluetooth technology (such as the name of the mobile equipment or its MAC address) enabling users to be identified.Thirdly, the Commission points out that only state-of-the-art cryptographic algorithms must be implemented, in order to ensure the confidentiality of exchanges. In this respect, it notes the use of the 3DES algorithm, envisaged at this stage, and draws the Ministry's attention to the fact that, in accordance with the general security reference system published by the National Agency for the Security of Information Systems this algorithm should in principle no longer be used.Finally, fourthly, the Commission notes that the system envisaged does not provide for a mechanism for enrolling people when using the application for the first time, which makes it possible to limit the data personal data collected. However, this could result in an increased risk of attack which is only acceptable insofar as such a mechanism for enrolling people would call into question the logic of pseudonymization of the processing. It therefore calls on the Ministry to put in place appropriate measures to combat this risk. Furthermore, the Commission welcomes the fact that elements of the technical documentation have already been made public. In this regard, it emphasizes the importance of ensuring free access to the protocols used as well as to the source code of the application, the central server and their configuration. This is both to allow the scientific community to contribute to the constant improvement of the system and to the correction of any vulnerabilities as well as to guarantee perfect transparency vis-à-vis all citizens. It also recommends, in order to maximize the quality of the solution, that the comments and debates of the scientific community be taken into account. On respect for the rights of individuals over their personal data The control of their data by the persons concerned is an essential guarantee to ensure public confidence in the measures taken for the purpose of managing the COVID-19 crisis. Appropriate information must therefore be provided to users, in compliance with Articles 12 to 14 of the GDPR. Insofar as a large part of the population is likely to be affected by the system, the Commission insists in particular on the need to provide information that can be understood by as many people as possible, in clear and simple terms. The Commission points out that situations such as the current COVID-19 epidemic do not suspend or restrict, in principle, the possibility for data subjects to exercise their rights over their personal data in accordance with the provisions of Articles 12 to 22 of the GDPR. appropriate for the exercise of rights must also be defined if the application is deployed. The President Marie-Laure DENIS