Deliberation N°. 2020-046 of April 24, 2020 delivering an opinion on a proposed mobile application called "StopCovid".

(request for opinion N° 20006919)

Courtesy translation - in the event of any inconsistencies between the French adopted version and this English courtesy translation, please note that the French version shall prevail and have legal validity

The French data protection authority (hereafter the "CNIL"),

Entered by the Secretary of State for Digital Affairs a request for an opinion on the terms and conditions of the possible implementation of the "StopCovid" application with regard to French and European rules on the protection of personal data;

Having regard to Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data n° 108;

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 ;

Having regard to the French act n° 78-17 of 6 January 1978, modified, on information technology, data files and civil liberties, in particular its article 8-I-2°e) ;

Considering the decree n° 2019-536 of 29 May 2019 taken in the application of the act n° 78-17 of 6 January 1978 on information technology, data files and civil liberties ;

After hearing Ms. Marie-Laure DENIS, Chairwoman, in her report, and Ms. Nacima BELKACEM, Government Commissioner, in her observations,

Delivers the following opinion:

On 20th 2020, the Secretary of State for Digital Affairs submitted a formal request to the Commission for an opinion on the terms and conditions of the possible implementation of the "StopCovid" application with regard to French and European rules on the protection of personal data, on the basis of Article 8-I-2°-e) of the aforementioned Act No. 78-17 of January 6, 1978 (hereinafter, the "aata protection act").

This submission comes in the context of the public health emergency linked to the COVID-19 epidemic, and more specifically in the context of France's strategy to lift containment measures. The Government plans to develop and launch an application, called "StopCovid", available on 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 close proximity, in the near past, to persons diagnosed positive

for COVID-19 and having the same application, such proximity inducing a risk of transmission of the virus.

It would be a "contact tracing" application, not a tracking application for people exposed or diagnosed positive to the virus, and would rely on the use of Bluetooth proximity communication technology to assess the proximity between two smartphones, without the use of geolocation technology. It would be used only on a voluntary basis and its implementation modalities would aim at minimising any direct or indirect identification of the persons using it. The documents annexed to the submission, which describe a protocol known as the ROBERT protocol, provide initial thoughts 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 as to whether or not, in the event of the implementation of such an application, personal data within the meaning of the aforementionned Regulation (EU) 2016/679 of 27 April 2016 (hereinafter 'the GDPR) and the rench data protection act are being processed, on the identification of the legal basis for such processing, within the meaning of the same provisions, on the compliance of such a system with the rules for the protection of personal data and, where appropriate, on the additional guarantees that should be provided.

The present opinion of the Commission aims to provide some answers to enlighten the Government on the analysis of such an application from the point of view of the law on the protection of personal data, it being specified that the deployment of this application as well as its exact modalities of implementation, from a legal, technical and practical point of view, have not yet been decided at this stage. The Commission asks, after the debate in Parliament and if it is decided to use such a tool , that the matter be referred back to the Commission for an opinionon the final arrangements for implementing the mechanism.

As a preliminary remark, the Commission stresses that it is fully aware of the seriousness of the health situation linked to the COVID-19 epidemic, of the death and suffering it causes, and of the difficulties linked to the confinement of persons 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 plan is part of its action to combat the epidemic and reflects the desire to use every tool available to contain the disease and to manage the lockdown-lifting process as effectiveas possible. In addition, the design of the StopCovid application reflects the concern to protect people's privacy, in particular by preventing a list of people who declare themselves as carriers of the virus centralised on a server.

However, it is also the Commission's duty to point out that this project raises unprecedented questions in terms of the protection of privacy. It certainly does not consist of tracking all the geographical movements of people: it is not a question of tracing individuals on a continuous basis. Nevertheless, it is a question of establishing, through the collection of pseudonymous traces, the list of persons to whom each user of the application has been physically close, for a limited period of time, among all the users of the application. Such a collection, which is intended to apply to the largest possible part of the population, must be envisaged with great caution.

The protection of privacy is guaranteed by the French Constitution and other sources of law; the collection of lists of persons whom individuals have frequented is a strong infringement of this principle, which can only be justified, if at all, by the need to comply with another constitutional principle, namely the protection of health, which derives from the eleventh preambular paragraph of the 1946 French Constitution. The use of novel forms of data processing may also create a habituation phenomenon among the population which may degrade the level of protection of privacy and must therefore be reserved for certain exceptional situations. Finally, the Commission stresses that compliance with the rules on the protection of personal data, and in particular the proper information of the persons concerned, the respect of their rights and, more generally, of the provisions of the GDPR and of the French data protection act, is likely to promote the confidence of the users of the application and, consequently, the effectiveness of the planned system.

It is in the light of these general principles that the use of the StopCovid application described in the submission should be examined.

The processing of personal data and in particular health data

The system envisaged to date consists, on the one hand, of a mobile application which will be made available on mobile devices (in particular smartphones and tablets) running Android and iOS operating systems and, on the other hand, a central server which will store and transmit a certain amount of data necessary for the overall operation of the system. The Government questions the existence of personal data processed in the context of the device since, on the one hand, the downloading and use of the application would not require the provision of directly identifying data (such as name, telephone number, e-mail address, etc.) and, on the other hand, the downloaded application, and therefore its user, would be identified by the central server only by a *pseudonym,* i.e. data that is not identifying in itself. The protocol described in the submission is thus based on a system associating a permanent random identifier (hereinafter, the permanent pseudonym) with each downloaded application, which then makes it possible to create several temporary random identifiers (hereinafter, the temporary pseudonyms).

Firstly, it should be pointed out 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 attributed, at the time of its installation, to that user's application and those transmitted to the central server by the application of another person which has been diagnosed as positive. The result is that there remains a link between the pseudonyms and the downloaded applications, each application being itself installed on a terminal, which generally corresponds to a specific natural person. As a result of this link, the Commission considers that the device will process personal data within the meaning of the GDPR. Furthermore, the collection of temporary pseudonyms of the persons with whom the user has been in contact could allow the reconstruction of all the relationships the user has had with other users of the application. In the light of these factors, the Commission considers that the planned system is subject to the rules on the protection of personal data, while recognising that the safeguards taken provide a high degree of guarantee to minimise the risk of re-identification of the natural persons associated with the data stored, for a necessarily limited period, by the central server.

Secondly, the central server would have information as to whether or not a user has received notification that he or she has been exposed to the virus. The Commission notes that the entire architecture of the proposed system tends to trasnmitto the central server only the pseudonyms generated by the applications associated with the persons with whom an infected individual has been in contact, and not the pseudonym of the infected individual. It stresses that this procedure minimises the risk of re-identifying the infected person at the origin of an alert, in full compliance with the principles of personal data protection.

Thirdly, the Commission notes that health data will be processed by the scheme. On the one hand, the triggering of an alert by an infected person is directly linked to the health status of that person. On the other hand, the information that a person presents a sufficiently high risk of having contracted a disease, and which leads in particular to him or her being informed by the application, is, according to the Commission's analysis, data concerning health and benefiting from the specific protection regime for such sensitive data provided for by the GDPR, enlightened by its recital 35, by the French data protection act, and even, depending on the uses provided for, by the specific provisions of the public health code 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 minimise the possibility of re-identification of the infected person by the people with whom he or she has been in contact and who have received the alert, this risk, which will depend on the context, and in particular the number of people with whom he or she has been in contact during the period preceding the alert, may remain and must be taken into account.

Nevertheless, the Commission recalls that the presence of personal data does not, as a matter of principle, prevent the implementation of the mechanism. However, it requires appropriate safeguards, which are all the stronger the more intrusive the technologies are, and for which the mitigation of the possibilities of re-identification is an essential measure.

A system based on volunteering

A purpose limited to alerting persons exposed to the risk of contamination

The Commission recalls that the purpose limitation principle, enshrined in article 5(1)(b) of the GDPR, is a key principle of the protection of personal data: personal data should only be used for a precise and predetermined purpose. Any other use of the data is, in principle, prohibited.

In the present case, as stated, the "contact tracing" objective of the application is to be able to inform a user of the application that his smartphone (or other mobile device) has been in close proximity, in the previous days, to that of a person who subsequently tested positive for COVID-19, so that there is a risk that he may have been contaminated in turn.

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 submission is not intended to organise contact with the person alerted, to monitor the number of infected persons or to identify the areas to which these persons have 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 users

The Commission notes that the Government's plan is to make the StopCovid application available to the population residing on the national territory, the downloading and use of which would be on a voluntary basis. It therefore considers that the voluntary nature of the use, combined with greater transparency as to how and for what purposes it is used, is a decisive factor in ensuring confidence in the system and encouraging its adoption by a significant proportion of the population. This voluntary nature should be explicitly provided for in the legal texts governing the system and in the information provided to the public.

In this respect, it should be stressed that volunteering should not only result in the choice for the user to download and then implement the application (installation of the application, Bluetooth enabling, or even declaring himself positive to COVID-19 in the application) or the ability to uninstall it. Volunteering also means that there are no negative consequences attached to not downloading or using the application. Thus, access to the tests and healtcare can in no way be conditioned to the installation of the application. The use of an application on a voluntary basis should not condition either the possibility to move around when the lockdown is lifted or access to certain services, such as public transport for example. Nor should users of the application be forced to to carry a Bluetooth-enabled phone on their person at all time. Public institutions or employers or any other person should not make certain rights or access conditional on the use of this application. Moreover, this would, in the rule of law and according to the Commission's analysis, constitute discrimination. Under these conditions, the use of StopCovid could be regarded as genuinely voluntary. Different choices, which would be a matter for the legislator and whose strict necessity would then have to be demonstrated, would infringe the right to protection of personal data and respect for private life to a much greater extent. All the following analysis therefore only applies to a voluntary application project with the above characteristics.

The legal basis of the StopCovid application

Article 6 of the GDPR and Article 5 of the French data protection act stipulate that the processing of personal data is only possible in certain hypotheses and for certain restrictively listed reasons, which constitute the possible "legal basis" for processing. In the present case, the government questions 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 task carried out in the public interest to combat the COVID-19 epidemic.

First of all, the Commission would point out that voluntary use of the application is compatible in law with one or other of these "legal basis".

It recalls that personal data protection law 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 appropriate to the situation and the type of processing. Indeed, each legal basis is subject to specific conditions and has particular legal consequences for the entity carrying out the processing operations as well as for the data subjects. The choice of the legal basis can therefore be a delicate operation,

which does not call for an unequivocal answer. However, if several legal bases may be appropriate for the same processing operation, only one should be chosen, which is ultimately considered to be the most appropriate in the case at issue.

The Commission notes that the fight against the 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 task carried out in the public interest, within the meaning of Articles 6.1(e) of the GDPR and 5.5° of the French data protection act, constitutes the most appropriate legal basis for the development by the public authority of the StopCovid application. It notes that the European Data Protection Committee considered, in its Opinion No. 04/2020 of 21 April 2020, that this legal basis is the most appropriate for this type of application when implemented by public authorities. Moreover, the choice of this legal basis makes it possible to reconcile in full legal certainty the voluntary nature of the use of this application and the possible incentives of public authorities for such use, in order to promote its widest possible use. However, the GDPR requires that the purposes of the processing operation in question are necessary for the task carried out in the public interest which is at stake and that it has a sufficient legal basis in a norm of national law.

With regard to the specific case of processing of health data, the GDPR provides that such data may be processed, as in the present case, for reasons of public interest "*in the area of public health, such as protection against serious cross-border threats to health*", provided that such processing is necessary for those purposes and provided for by Union or national law and that such law provides for "*suitable 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 these data on another exception provided for in Article 9 of the GDPR, the Commission considers that these provisions seem to be the most appropriate in the contexte of the StopCovid application.

In these circumstances, the Commission recommends that the use of a voluntary contact tracing application to manage the current health crisis should have an explicit and precise legal basis in national law. It asks the government, if necessary and whatever the chosen vector, to refer the draft standard governing the implementation of the application in question back to the Commission once the decision has been taken and the project specified.

Finally, it may be noted that the StopCovid application project also involves the storing of information, or the gaining of access to information already stored in the terminal equipment of the user, within the meaning of Article 82 of the French data protection act, i.e. in the mobile device 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 are therefore lawful.

Admissibility of the invasion of privacy through a contact tracing application

The Commission would point out that the constitutional protection of privacy resulting from Article 2 of the Declaration of the Rights of Man and of the Citizen is subject to conventional protection, based in particular on the Charter of Fundamental Rights of

the European Union and the European Convention on Human Rights, as well as the specific safeguards required by the GDPR, in particular with respect to the processing of health data in the public interest, the government must ensure that the invasion of privacy remains proportionate to the objective pursued. As noted, the protection of health is also an objective of constitutional value.

On the one hand, compliance with the principle of proportionality will result in particular in the collection and retention of data being limited to what is strictly necessary, in order to minimise the invasion of the privacy of individuals. This fundamental guarantee implies in the present case that the collection and processing of data carried out by the application is of a temporary nature, of a duration limited to that of the usefulness of the system in the light of the purposes described above. It also implies that all data must be deleted as soon as the usefulness of the application is no longer proven. In the event that statistical analysis or scientific research is nevertheless necessary, it must be carried out first and foremost on anonymised data or, failing this, in strict compliance with the rules set out in the GDPR and the French data protection act.

On the other hand, it appears to the Commission that the invasion of privacy will be admissible in the present case only if, in the light of the inevitably incomplete and uncertain information at its disposal for dealing with the epidemic, the Government can rely on sufficient evidence to have reasonable assurance that such a measure will be useful in managing the crisis, and in particular in bringing the population out of its confinement, which in itself constitutes a very serious infringement of the freedom of movement. Although this type of system can potentially help public authorities to monitor and contain the COVID pandemic by supplementing the traditional contact tracing methods used to contain the spread of epidemics, it nevertheless has limits, both intrinsic and linked to its integration in a global health policy, which are likely to undermine its effectiveness.

Firstly, its effectiveness depends on certain technical conditions, in particular the possibility for a sufficient proportion of the population to access and use the application under good conditions. This means, in particular, that it would be desirable for the application to be available on a sufficient number of mobile application stores ("*appstores*", "*playstores*", etc.) and compatible with the majority of smartphones and other mobile devices currently in use, both in terms of hardware and software. The Commission also notes that competition from several contact tracing applications, which must in any event comply with the applicable provisions on the protection of personal data and, therefore, are subject to the Commission's supervisory powers, is likely to undermine the effectiveness of the system.

Secondly, the Commission underlines that the effectiveness of the system depends partly on its widespread adoption, while a significant part of the population does not have adequate mobile devices or may have difficulties in installing and using the application. However, some of the people most vulnerable to the disease, as well as younger people without smartphones, who could play a significant role in the spread of the disease, are particularly concerned. In addition, some people who will use the application are likely to contract the disease without showing any symptoms, and therefore may not alert their contacts. However, this must be put into perspective by the fact that the envisaged system could also, due to the possible notification of an alert, encourage such persons to be tested.

Thirdly, the Commission also emphasises that the effectiveness of the planned system depends on the proper calibration of the algorithms used to identify an interaction that may have caused contamination. Furthermore, the Commission recommends that the use of any form of automation of the decision to inform exposed persons should be combined with the possibility for these persons to talk to qualified personnel.

Fourthly, a digital system for individualised monitoring of individuals can only be put in place as a supplementary measure within the framework of a global health response. The Commission considers that the use of contact tracing applications cannot be an autonomous measure and calls for particular vigilance on this point against the temptation of "technological solutionism". Therefore, it is up to the government to evaluate all the various measures to be put in place, such as the mobilisation of health personnel and health investigators, the availability of masks and tests, the organisation of testing, support measures, information and services provided 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 with interest the clarifications provided by the Secretary of State for Digital Affairs, who has indicated that the use of the application is envisaged as part of an integrated approach to the overall health strategy steered in particular by the Ministry of Health and Solidarity.

The Commission emphasises that all these precautions and guarantees are such as to allow public confidence in the system, which is an important factor in 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 enable the public authorities to make an informed decision as to whether or not to maintain it, having regard, in particular, to the principles of proportionality and necessity. The Commission recommends that these analyses should be communicated to it, where appropriate, to enable it to carry out its task of monitoring the conformity of the implementation of the planned arrangements.

Application settings

The Commission emphasizes that it is only giving its opinion on the principle of deploying an application such as the one described in the submission, the precise details of which could, if necessary, change. However, it wishes to provide the Government with the following clarifications.

Responsibility for processing

The 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 of Health and Solidarity or any other health authority involved in the management of the health crisis can assume responsibility for the processing.

On the need for a data protection impact assessment

The Commission draws the government's attention to the fact that, as with any processing likely to result in a high risk (health data, large-scale use, systematic monitoring, use of a new technological solution), a data protection impact assessment (DPIA) will have to be carried out before any such measure is implemented. The publication of the DPIA is recommended for transparency purposes and in view of the current context.

On data accuracy

The Commission notes that the technical protocol forwarded to it envisages the possibility of introducing false positives in notifications sent to individuals in order to limit the risk of re-identification in certain types of attack. It considers that this measure cannot and should not be implemented, since it would result in false alerts to persons who have not been at risk and who would therefore be encouraged to submit to voluntary containment measures consisting of a self-imposed restriction of their individual freedoms. It emphasises that maintaining the accuracy of data is a mandatory legal obligation under the GDPR and the French data protection act and that such a measure is not conceivable, under penalty of calling into question the conformity of the processing operation with the applicable texts.

On data security

The security of personal data is an indispensable guarantee, given the sensitivity of this system. This security requires considering the entirety of the conditions of implementation of data processing and a continuous improvement of the techniques, procedures and protocols implemented. Faced with the challenge of meeting these requirements in a very short time, the Commission draws the Ministry's attention to this point.

The Commission stresses that this opinion is based on the documentation sent to it, that it does not cover all the characteristics of the data processing and that the proposed protocol is constantly evolving. Nevertheless, it considers it necessary to draw the Government's attention to the following four points at this stage.

Firstly, the Commission notes that the planned system includes a server responsible for centralising the identifiers of exposed persons. In order to provide the highest guarantees possible against any misuse of purpose linked to this choice, it considers it necessary to put in place very high-level organisational and technical security measures, in accordance with an appropriate security model that takes into account any malicious act. In this respect, 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.

Secondly, the Commission considers it necessary to implement measures both in the central server and in the application to avoid the possibility of recreating a link between these temporary pseudonyms and specific device information related to the Bluetooth technology (such as the name of the mobile equipment or its MAC address) which could identify users.

Thirdly, the Commission reminds that only state-of-the-art cryptographic algorithms should be used in order to ensure the integrity and confidentiality of exchanges. On this matter, 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 baseline published by the National Cybersecurity Agency of France (ANSSI), this algorithm should in principle no longer be used.

Finally, the Commission notes that the envisaged system does not provide a mechanism for the persons signing up when the application is used for the first time, which allows limiting the personal data collected. However, this could result in an increased risk of attack, which is acceptable only insofar as such a mechanism for signing up would question the logic of pseudonymity of the data processing. It therefore calls on the Ministry to put in place appropriate measures to mitigate this risk.

Furthermore, the Commission welcomes the fact that elements of technical documentation have already been made public. In this respect, it stresses the importance of ensuring free access to the protocols used and to the source code of the application, the central server and their settings. The aim is both to enable the scientific community to contribute to the constant improvement of the system and the correction of any vulnerabilities and to guarantee complete transparency for all citizens. It also recommends, in order to maximise the quality of the application, that the comments and debates of the scientific community be taken into account.

On the respect of the rights of individuals with regard to their personal data

Data subjects' control over their data is an essential safeguard to ensure public confidence in the measures taken to manage the COVD-19 crisis. Appropriate information should therefore be provided to users, in compliance with Articles 12 to 14 of the GDPR. Since a significant part of the population is likely to be affected by the measures, the Commission stresses in particular the need to provide information that is comprehensible to the greatest possible number of people, using clear and plain language.

The Commission recalls that situations such as the current outbreak of COVID- 19 do not suspend or restrict, as a matter of principle, the possibility for data subjects to exercise their rights with regard to their personal data in accordance with the provisions of Articles 12 to 22 of the GDPR. Appropriate modalities for the exercise of the rights will also need to be defined if the application is deployed.

The Chairwoman

Marie-Laure DENIS