Deliberation 2020-056 of May 25, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Wednesday June 03, 2020NOR: CNIX2012957Deliberation n° 2020-056 of May 25, 2020 providing an opinion on a draft decree relating to the mobile application called "StopCovid" (request for opinion no. 20008032)

The National Commission for Computing and Liberties,

Seizure by the Minister of Solidarity and Health of a request for an opinion concerning a draft decree relating to the mobile application 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 emergency law n° 2020-290 of March 23, 2020 to deal with the covid-19 epidemic, in particular its article 4;

Having regard to Law No. 2020-546 of May 11, 2020 extending the state of health emergency and supplementing its provisions;

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 n° 2020-551 of May 12, 2020 relating to the information systems mentioned in article 11 of law n° 2020-546 of May 11, 2020 extending the state of health emergency and supplementing its provisions, in particular its article 9;

Having regard to CNIL deliberation no. 2020-046 of April 24, 2020 providing an opinion on a mobile application project called StopCovid;

Having regard to deliberation no. 2020-051 of May 8, 2020 providing an opinion on a draft decree relating to the information systems mentioned in article 6 of the bill extending the state of health emergency;

After having heard Mrs. Marie-Laure DENIS, President, in her report, and Mrs. Nacima BELKACEM, Government

Commissioner, in her observations;

Gives the following opinion:

The National Commission for Computing and Liberties (hereinafter the Commission) was urgently seized by the Minister for Solidarity and Health (hereinafter the Ministry), on May 15, 2020, of a request for opinion concerning a draft decree relating to the mobile application called StopCovid, in application of the provisions of III of article 6 of the aforementioned law n ° 78-17 of January 6, 1978 (hereinafter the Data Protection Act). In accordance with these provisions, this notice must be published with the corresponding decree.

This referral comes in the context of the covid-19 epidemic, and more particularly of the so-called deconfinement strategy. In this context, the Government plans to implement an application, called StopCovid, available on ordiphones (smartphones) and, if necessary, on other mobile devices. It aims to inform users that they have been close to people diagnosed with covid-19 and using the same application, this proximity inducing a risk of transmission of the SARS-CoV-2 virus.

The Commission ruled, in its opinion of April 24, 2020, on the general compliance with the personal data protection rules of a contact tracking system as then envisaged by the Government. This referral to a draft decree relating to the application called StopCovid, accompanied by the data protection impact analysis (hereinafter AIPD) relating to the planned system, specifies the projected conditions of implementation of the contact tracing app. This processing of personal data, which must comply with the applicable provisions of the aforementioned Regulation (EU) 2016/679 of April 15, 2016 (hereinafter the GDPR) and the Data Protection Act, calls for the following observations from of the Commission.

On the necessity and proportionality of the device

The Commission emphasizes first of all that it is fully aware of the seriousness of the crisis linked to the health situation created by the covid-19 epidemic, which is of exceptional magnitude. The implementation of the StopCovid treatment is part of the Government's action to fight against the epidemic and reflects the desire not to leave aside any tool to fight against the epidemic, and in particular to better manage the deconfinement period.

The fight against this epidemic, which falls within the constitutional objective of protecting health, is a major imperative that can justify, under certain conditions, temporary infringements of the right to protection of privacy and data personal character. It thus justified the authorization, by the law of May 11, 2020 referred to above, of systems based on the processing of personal data, of a particular sensitivity and of national scope. The Contact Covid and SI-DEP treatments, which aim to identify the

chains of contamination of the SARS-CoV-2 virus and to ensure the monitoring and support of the persons concerned, have been authorized in this respect by the decree of May 12, 2020 referred to above, taken after the opinion of the Commission dated May 8, 2020.

The Commission nevertheless recalls that the constitutional and conventional protections of the right to respect for private life and the protection of personal data, based in particular on the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of rights and fundamental freedoms, require that the infringements of these rights by the public authorities not only be justified by a reason of general interest, as is the case here, but also be necessary and proportionate to the achievement of this objective.

In addition, it recalls the sensitive nature, by nature, of the implementation of a system for automatically monitoring the contacts of users of a mobile application made available by the public authorities. Although the Commission recognizes that the planned application respects the concept of data protection by design, such collection, which is intended to apply to as large a part of the population as possible, must in any case be considered with caution. It refers on this point to its opinion of 24 April 2020.

Secondly, with regard to the usefulness of the StopCovid treatment, the Commission had recalled, in its opinion of April 24, 2020, that the planned device would only be admissible if the Government had sufficient elements to establish its usefulness. for crisis management, particularly in the context of deconfinement. In particular, she had insisted on the necessary insertion of this device in a global health policy.

In this respect, the Commission notes that the Ministry intends to complete, by implementing the treatment, the contact tracing system authorized by the aforementioned decree of 12 May 2020 and thus contribute more effectively to reducing the chains of contamination. The purpose of the processing is thus to allow contact cases to be informed and alerted more quickly as to the risks of exposure to the virus, in particular when it comes to contact cases that the contaminated or exposed persons do not necessarily know, such as for example the people you meet on public transport or in shops. It also makes it possible to alert certain contact cases of people who do not wish to respond to the health investigators.

It also notes that the Ministry has reported on several scientific and epidemiological studies, including foreign ones, demonstrating the interest, for health authorities, of being able to have contact tracing applications, in support of manual monitoring of the spread of chains of transmission, in order to identify the contacts of the detected cases as quickly and widely

as possible. The ministry specified that some of these studies lead to the conclusion that such an application is useful in reducing the chains of contamination, including when it is downloaded only by a limited part of the population. It also refers to the favorable positions of the covid-19 scientific council and the National Academy of Medicine.

It is also necessary to take into account the uncertain nature of the information available to the Ministry in this matter at the start of the deployment of this tool and the difficulty of comparing the planned treatment with those already tested or envisaged in other countries, in particular within the European Union.

Finally, the usefulness of the application comes from the fact that the planned treatment will be articulated with the health care system for people exposed to the virus, once the person alerted via the StopCovid application and who would decide, following and in accordance with this notification, to consult a health professional would then be recorded in the aforementioned Contact Covid or SI-DEP treatments.

With regard to these elements, the usefulness of the application and the necessity of the planned processing to accomplish the mission of public interest thus entrusted to the public authority, within the meaning of the data protection rules, are sufficiently demonstrated upstream of the implementation of the treatment.

Thirdly, with regard to the proportionality of the planned device, numerous safeguards are provided by the Ministry in order to limit the breaches of data protection likely to be caused by such a device.

Several substantial guarantees were provided for from the initial Government project, such as the choice to store in the central server pseudonymous identifiers of people exposed to the disease and not of infected people, the use of Bluetooth proximity communication technology to assess the proximity between two smartphones and not the use of geolocation technology, the choice of a system based on voluntary participation or even the use of pseudonyms minimizing the possibilities of identifying the persons concerned.

In addition, the Commission notes that several of the additional guarantees it requested in its opinion of April 24, 2020 have been integrated into the government's plan. This is the case, in particular, of the precise definition of the purposes of the planned processing, of the fact that the responsibility for the processing is entrusted to the ministry in charge of health policy or even the implementation of certain technical security measures. Similarly, if the alerts generated by the application will be articulated with the rest of the health system, the ministry has confirmed that it does not plan to attach adverse legal consequences to the fact of not having downloaded the application and that no specific rights will be reserved for the persons

who will use it. Finally, the Commission's recommendation to have an explicit and precise legal basis in national law, on which it would be consulted beforehand, to enable its implementation, was followed by the Ministry, as evidenced by its referral to a draft decree in Council of State concerning the processing based on articles 6.1.e and 9.2.i of the GDPR.

The Commission considers that these elements are 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.

Fourthly, it recalls that the principle of proportionality also implies that the rights to privacy and the protection of personal data should only be infringed for the time strictly necessary to achieve the objective pursued.

In this regard, the Commission takes note of the temporary nature of the planned application, the term of which is set at six months from the end of the state of health emergency by the draft decree. This duration corresponds to that provided for Contact Covid and SI-DEP processing, the application only being useful in connection with the more general framework for conducting health surveys.

The Commission considers this to be a maximum duration. It requests that the effective impact of the device on the overall health strategy be, independently of the evaluation report provided for by the decree after the global cessation of StopCovid treatment, studied and documented on a regular basis throughout the period of use of that. this, in order to ensure its usefulness over time.

It is aware that this assessment of the usefulness will be delicate and must be able to take into account, if necessary, possible periods of resurgence of the epidemic. It nevertheless considers this assessment to be essential, since an automated tool for automatic contact tracing, made available by the public authorities and installed on the smartphones of individuals, is not admissible, as it underlined in its opinion of April 24, only if it makes a useful contribution to health policy. The Commission asks that these follow-up reports be sent to it as they are drawn up.

The draft decree therefore calls for the following comments from the Commission.

On the purposes and responsibility for processing

On the purposes of the processing

Article 1 of the draft decree specifies that the purposes of the processing are: - to inform a user of the application that he or she has been close to at least one other user of this same application having was later diagnosed positive for covid-19, so

there is a risk that she was also infected;

- raising awareness of users of the application, identified as a contact at risk of having been contaminated by SARS-CoV-2, on the symptoms of the disease, the barrier gestures and the behavior to adopt to fight against the spread of the virus ;

- referral of high-risk contacts to competent healthcare providers for their care and access to screening tests;

- improvement of the efficiency of the model used by the application for the definition of contact cases thanks to the use of anonymous statistical data at the national level.

Firstly, with regard to the referral of high-risk contacts to the competent health actors, the Commission notes that the draft decree will be amended in order to specify that the establishment of contact between the user and the professional of health will be recommended but will remain at the discretion of the user.

Secondly, the Commission takes note of the clarifications provided by the Ministry according to which the purpose of improving the efficiency of the health model used by the application on the definition of contact cases is aimed at improving the performance of the application and not to the extent of its health utility. The Commission understands that other methods, such as statistics or surveys, will make it possible to meet this last requirement.

Thirdly, the following purposes are expressly excluded from the purposes pursued by the processing: operations to identify infected people, identify the areas in which these people have moved, make contact with the alerted person or monitor compliance with the measures containment or any other health recommendation. The processing must not allow the monitoring of the social interactions of the persons either.

Fourthly, given the sensitive nature of the data collected and the purposes pursued by the processing, the Commission welcomes the fact that, in accordance with what it recommended in its deliberation of 24 April 2020, the Ministry responsible for health be designated as the controller. It considers that such a designation helps to ensure that both the development and deployment and the possible evolutions of the system are defined by or in conjunction with the competent national health authorities.

An application based on the voluntary participation of users

The Government has followed the recommendations of the European Data Protection Board in its opinion No. 04/2020 of April 21, 2020 and of the Commission in its opinion of April 24, 2020 by basing the StopCovid application on a mission of public interest. , integrated into health policy. The Commission recalled that the choice of this legal basis does not exclude the

downloading and use of the application being voluntary.

Article 1 of the draft decree enshrines the principle that the downloading and use of the StopCovid application must be based on a voluntary approach by the user.

The Commission takes note that volunteering materializes in all the components of the system: installation of the application, activation of communication by Bluetooth, contact with a health professional, notification of the positive character of its diagnosis or positive result to a covid-19 screening examination in the application, carrying out the screening following receipt of a notification, uninstalling the application.

On the data collected and processed

Regarding the data collected

As a preliminary point, the Commission notes that the StopCovid application will be based on the ROBERT protocol, specified by INRIA. It notes that this protocol was designed with a logic of data minimization and data protection from the design stage. It also notes that this protocol takes the position of disseminating the identifiers of people exposed to the virus rather than disseminating the identifiers of people actually infected, and that it guarantees that no link will be kept between infected people and the list of people that they could have exhibited. The Commission points out that this choice protects the privacy of the persons concerned.

Article 2 of the draft decree lists the exhaustive list of personal data that may be collected as part of the StopCovid application. As the Commission has already noted in its deliberation of April 24, 2020, if the device is intended to process personal data within the meaning of the GDPR, the application only collects data that is adequate, relevant and limited to what is necessary with regard to the purposes for which they are processed, in compliance with the principle of data minimization set out in Article 5.1.c of the GDPR.

In addition, personal data relating to health will be processed. The processing of this sensitive data is based on article 9.2.i of the GDPR as previously mentioned.

However, certain data mentioned in the AIPD are not mentioned in article 2 of the draft decree. The Commission takes note of the Ministry's commitment to modify the project in order to mention the collection of periods of exposure of users to contaminated persons as well as the country codes. Furthermore, given the particularities of the processing, it recommends that the collection of the dates of the last query of the server should also be mentioned.

Regarding the accuracy of the data

The Commission recalls that ensuring the accuracy and updating of data is a legal obligation under Article 5.1.d of the GDPR.

In this respect, the Commission welcomes the fact that the possibility of intentionally introducing false positives in the notifications sent to individuals in order to limit the risks of re-identification in certain types of attacks is no longer envisaged.

The Commission notes that the algorithm used to determine the distance between users of the application is still under development at this stage and may undergo future changes. In this respect, the exchange of messages via Bluetooth technology will also be used to estimate the distance between two mobile devices according to the strength of the signal received, while the timestamping of these messages will make it possible to estimate the duration of the interaction. It is necessary to take into account many parameters in order to be able to correctly estimate distances using this technology. To this end, calibration tests currently in progress aim to propose an appropriate statistical model. The Commission thus notes that the determination of a risky interaction will be carried out in a probabilistic manner, which is in line with the general logic of the application to warn users of a risk of contamination, and that in no case will the receipt of an alert from the application will only mean that the user has actually been infected.

The Commission notes that a mobile contact tracing application does not take into account the context in which people were at the time an exposure to an infected person was recorded. For example, a health professional or a receptionist will be particularly likely to be notified by the application as being at risk of having been contaminated by SARS-CoV-2 even though they were protected (wearing a mask, dividing wall, etc.) at the time the contact was recorded. Thus, the absence of consideration by the application of the context of the contacts is likely to lead to the generation of numerous false positives. Consequently, the Commission is wondering about the advisability of eventually providing in the application the possibility for the user to define periods of time during which contacts should not be considered as potentially at risk.

In any event, in order to take account of these particular cases, the Commission recommends that the information delivered to users can include recommendations as to the use of the application in specific contexts. The presence of an easily accessible temporary deactivation button on the application's main screen could reduce the number of false alerts corresponding to times when the user is not really exposed.

The Commission notes that the transfer of the history of the pseudonymous identifiers of the contact cases of an infected person, from a mobile application to the central server, requires the use of a single-use code given by a health professional

following a positive clinical diagnosis or a positive screening test for covid-19. Consequently, a user will not be able to falsify the application's central server database by declaring themselves positive without having been screened. Furthermore, the Commission notes that verification of the single-use code will be limited to its validity, and will not involve verification of the identity of the person to whom it was issued. The Commission also notes that this transmission will take place without the contact history transmitted to the server being able to be linked to the infected person.

On the recipients and accessors of the data

Article 3 of the draft decree specifies that the users of the application who will be notified as being at risk of having contracted covid-19 are recipients of the information that they have found themselves near another user. diagnosed or tested positive for the virus.

Furthermore, the Commission notes that the DPIA sent lists several organizations acting as processors on behalf of the controller.

Firstly, the Commission recommends that the draft decree be supplemented in order to mention that subcontractors will be accessing or receiving the personal data that they will need to know.

Secondly, the DPIA specifies that the subcontracting relations between the controller and its subcontractors, in particular as host, are concluded or are provided for in the form of an agreement, during the different phases of the project. application, namely the development, production and operation phases. The Commission recalls that such an agreement must specify the obligations of each party, in compliance with the provisions of Article 28 of the GDPR, in particular with regard to the exercise of the rights of data subjects and security measures.

The Commission notes that the cloud computing service provider hosting the application infrastructure, acting as a subcontractor, has data centers located in France. The subcontracting contract linking it to the data controller must in particular specify the geographical areas from which the administrators access the infrastructure.

Finally, it notes that Article 1 of the draft decree qualifies INRIA as a subcontractor and specifies that the implementation of the processing by INRIA, on behalf of the Ministry, is done under the conditions provided for in Article 28 of the GDPR. It wonders about such a qualification with regard to the definition of the subcontractor given by article 4.8 of the GDPR.

On data transfers outside the European Union

The draft decree as well as the AIPD mention that personal data are not transferred outside the European Union. The

Commission therefore takes note that the processing will take place exclusively on the territory of the Union.

On retention periods

The Commission notes that Article 4 of the draft decree provides for the retention of the keys and identifiers associated with the applications for the duration of the operation of the StopCovid application and at the latest six months from the end of the state of health emergency, and conservation of local history of people diagnosed or tested positive for fifteen days from their issue.

In accordance with the principle of retention limitation (Article 5.1.e of the GDPR), the data retention period must be limited to what is strictly necessary with regard to the purposes described above. Consequently, the temporary identifiers exchanged between the applications as well as the associated timestamps cannot be kept for a period longer than that during which this data is actually useful to determine whether contact may have caused contamination. Thus, this period was estimated at fifteen days, in accordance with the recommendation of Public Health France and the ministry.

The Commission notes that the user of the application may at any time request the deletion of his data from his smartphone and from the central database of the server by means of a functionality made available to him in the application, before uninstalling . Indeed, if the user can uninstall the application at any time, this will lead to the deletion of his data from his smartphone, but will have no effect on the data stored at the server level. The Commission considers that if it appears technically impossible to delete the data on the server after the application has been deleted by the user, the data relating to the applications should be deleted after a period of inactivity, to ensure that in such a case, data that has become useless is not kept. Furthermore, users of the application should be advised to delete their data from the central server prior to any uninstallation of the application.

On information and people's rights

On the information of people

With regard to compliance with the transparency obligations (Articles 5.1.a and 12 to 14 of the GDPR), Article 5 of the draft decree specifies, on the one hand, that the persons concerned are informed of the main characteristics of the processing and their rights at the time of installation of the StopCovid application and, on the other hand, that information notices are also made available to the public through the website https://www.stopcovid.gouv .Fr .

In addition, the AIPD specifies that infographics will complete the information by making it possible to popularize the underlying

technological concepts.

Firstly, the Commission draws the Ministry's attention to the fact that all the information must be made available to the user within the application itself. However, such an obligation does not preclude the possibility of adopting a multi-level approach whereby the data controller chooses to include the main characteristics of the processing initially. In any case, information that complies with the provisions of the GDPR must be easily accessible both when installing the application and throughout its use.

Secondly, the Commission insists on the need to provide information that can be understood by as many people as possible, insofar as a large part of the population is likely to be affected by the system. Information should also be made available in ways that enable people with disabilities to learn about it.

Particular attention should also be paid to minors, even though the information provided will be identical for all users of the application. Minors equipped with smartphones by their parents are indeed likely to download the application, under common law conditions. For them, even more than for other users, special attention must be paid to the information provided, so that the application is used wisely and that the alert message likely to be sent to them is adapted and well interpreter. The Commission therefore asks that the information provided to users include specific developments both for the minors themselves and for their parents.

In view of these elements, the examples of information provided in the DPIA will have to be the subject of additional work in order to comply with the provisions of Articles 12 to 14 of the GDPR.

On the rights of access, rectification, the right to portability and the right to limit processing

The Commission notes that Article 5 of the draft decree is intended to exclude the rights of access, rectification and the right to limit processing on the basis of Articles 11 and 23.i of the GDPR.

With regard to the right to rectification and the right to restriction of processing, the Commission considers that with regard to the characteristics of the processing, the latter are not intended to apply. The same applies to the right to portability, given that the processing is not based on Article 6.1.a nor on Article 6.1.b of the GDPR.

The right of access could theoretically concern the consultation by a user of the keys and pseudonymous identifiers associated with the application that he uses. Considering the fact that the consultation of these data presents in principle, taking into account in particular their pseudonymous nature, only a very weak utility for the person concerned and that their free

consultation by any person who can appropriate the smartphone on which the application is installed would be likely to weaken the security of the device, the Commission considers that it follows from provisions 11, 15(4) and 23 of the GDPR that the ministry can dismiss the application of the right of access. The application is indeed designed with a public health objective and pseudonymization is an important element to preserve the privacy of the people who will use this device.

On the right to erasure and the right to object

The Commission notes that the Ministry considers that the right to erasure and the right to object are not applicable in the context of the implementation of the system.

On the one hand, the Ministry considers that the provisions of Article 17.3.b and c of the GDPR exclude the application of the right to erasure and it intends, on the other hand, to derogate from the right of opposition on the basis of Article 23 of the GDPR.

The Commission considers that, in the case of processing based on the voluntary participation of data subjects, the right to erasure and the right to object should be fully applicable. Furthermore, it notes that in practice the DPIA does provide for the possibility for the user to exercise these rights effectively.

First, the user can request the erasure of this data directly via the application both with regard to the data stored on the terminal and those available on the central server.

Secondly, the right to object is materialized by the possibility for the user to stop using the application at any time by unsubscribing from the server or uninstalling it from the terminal. The AIPD specifies, in this regard, that unsubscribing must lead to the erasure of data both locally and on the central server and that uninstallation will lead to the erasure of data locally; the data potentially present on the central server can then no longer be linked to a user.

The Commission takes note of the ministry's commitment to modify the draft decree on these points.

On security measures

As a preliminary point, the Commission notes that the system envisaged has been the subject of additional measures on a certain number of points which it had noted in its deliberation of April 24, 2020.

Firstly, concerning the security of the server responsible for centralizing the identifiers of people exposed to the virus, the Commission's opinion drew attention to the need to implement organizational and technical security measures to provide the the highest possible guarantees against any misuse of purpose, due to the centralized nature of the protocol implemented

within the StopCovid application. In this regard, the Commission notes that the Ministry will use security modules to protect the encryption keys allowing access to the identifiers of the persons concerned.

It also notes that the data controller provides for the establishment of a committee bringing together several entities to which fragments of the encryption keys would be entrusted, in order to guarantee the impossibility for a single actor to misuse the use of the data. . It considers that such a measure is likely to limit the risks of misappropriation of the central database, and it calls on the ministry to include in this committee organizations of different natures and presenting a high level of independence, and notes that the participation of several scientific research organizations would be likely to further increase the level of guarantee provided by the system. However, it calls on the Ministry to specifically assess the level of guarantee offered by such a measure in the DPIA, and to put in place additional guarantees if necessary.

Secondly, on the use of cryptographic mechanisms, the Commission recalls having ruled in its opinion on the need to use state-of-the-art cryptographic algorithms that comply with the general security reference system published by the National Information Systems Security Agency (ANSSI). It notes in this regard that the protocol has evolved, the 3DES encryption algorithm having been replaced by SKINNY-CIPHER64/192, as recommended by ANSSI.

Thirdly, concerning the publication of the source code, the draft decree mentions that certain elements of the computer code of the application or of the central server will not be made public, as this would endanger the integrity and security of the application. Even if the configuration of the software used and the details of the security measures are not intended to be made public, it is important that the entire source code be made public. The Commission welcomes the ministry's commitment to make the entire source code public and suggests that the decree be amended accordingly.

Furthermore, the Commission notes that the use of the certificate pinning mechanism on mobile applications constitutes good practice, allowing applications to securely authenticate the server with which they are communicating and thereby guarantee the strict confidentiality of the data exchanged with the server.

The Commission notes that only individually authorized persons will be able to access the data recorded on the central server. It recalls that the procedures for authenticating these people must comply with deliberation no. 2017-012 of January 19, 2017 adopting a recommendation relating to passwords, and that given the nature of the processing, it recommends that strong authentication mechanisms are put in place.

The Commission notes that the provider of the infrastructure hosting the StopCovid platform, acting as a subcontractor, is

qualified SecNumCloud by ANSSI, that it is certified as a health data host (HDS) and that it implements ISO/IEC 27001 certified data centers.

In addition, the Commission notes that, in accordance with the general security reference system, a security certification of StopCovid is planned, prior to the production of the application. It also notes that ANSSI is involved in the implementation of the application, and that a certain number of recommendations have been issued by the latter for the data controller.

In addition, the Commission welcomes the fact that security audits are scheduled by ANSSI throughout the development of the application. The Commission also notes that audits will be carried out by third parties.

The Commission notes that the Ministry plans to use a captcha when initializing the application, in order to verify that it is indeed being used by a natural person. It notes that the captcha envisaged is based, initially, on the use of a service provided by a third party. The Commission notes that the use of this service is likely to lead to the collection of personal data not provided for in the decree, data transfers outside the European Union, as well as read/write operations which would require the consent of the 'user. The Commission also notes that the end user should be informed of these processing operations in accordance with the GDPR and that the relationship with this third party should be governed by an outsourcing contract. Consequently, it calls on the ministry to be vigilant and would like further developments of the application to quickly allow the use of an alternative technology.

Lastly, the Commission notes that certain transactions are subject to logging measures. With regard to data relating to technical errors, the Commission recommends that only the minimum amount of data strictly necessary for verifying the correct operation of the system be logged, and in particular that these logs be free of identifiers or cryptographic keys relating to users. Concerning the logging of the actions carried out by the administrators, the Commission recommends that it be kept for a period of six months under conditions guaranteeing its integrity, and that automatic analysis mechanisms be put in place in order to detect any abnormal operation.

The Commission notes that changes to the application and the contact tracing protocol, in particular to allow interoperability at European Union level, are likely to be developed in the medium term. It also takes note of the Ministry's intention to contact it again, including on an optional basis, for any modification that may be made to the processing.

The president,

M. L. Denis