Deliberation N° 2020-056 from 25 May 2020 delivering an opinion on a draft decree relating to the mobile application known as "StopCovid"

(request for opinion N° 20008032)

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 "Commission"),

Entered by the Minister of Solidarity and Health a request for an opinion on a draft decree relating to the mobile application known as "StopCovid";

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 6-III;

Having regard to the emergency law n° 2020-290 of 23 March 2020 to deal with the COVID epidemic - 19, in particular its article 4;

Having regard to law n° 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions;

Considering the decree n° 2019-536 of 29 May 2019 modified taken for the application of the law n° 7817 of 6 January 1978 relating to data processing, files and freedoms;

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

Having regard to the CNIL's deliberation n°. 2020-046 from 24 April 2020 delivering an opinion on a proposed mobile application called "StopCovid";

Considering deliberation n° 2020-051 of 8 May 2020 giving its opinion on a draft decree relating to the information systems mentioned in Article 6 of the law extending the state of health emergency;

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

Delivers the following opinion:

1. On 15 May 2020, the Commission was urgently requested by the Minister of Solidarity and Health (hereinafter "the Ministry") to deliver its opinion on a draft decree relating to the mobile application known as "StopCovid", pursuant to the

provisions of Article 6.III of the aforementioned Act N° 78-17 of January 6, 1978 (hereinafter the "French data protection act").

2. In accordance with these provisions, this opinion shall be published with the corresponding decree.

This submission comes in the context of the COVID-19 epidemic, and more specifically the so-called "progressive lockdown exit" strategy. In this context, the Government is considering implementing an application, called "StopCovid", available on smartphones and, maybe in the future, on other mobile devices. It is intended to inform users that they have been in close proximity to persons diagnosed as COVID-19-positive and having the same application, as this proximity entails a risk of transmission of the SARS-CoV-2 virus.

3. In its opinion of 24 April 2020, the Commission ruled on the general conformity with the rules on the protection of personal data of a "contact tracing" system as envisaged by the Government at the time. The present submission on a draft decree relating to the so-called "StopCovid" application, along with a privacy impact assessment (hereinafter "PIA") relating to the envisaged system, specifies the proposed conditions of implementation of the contact tracing application. This processing of personal data, which must comply with the applicable provisions of Regulation (EU) 2016/679 of 15 April 2016 referred to above (hereinafter "the GDPR") and the French data protection act, calls for the following comments from the Commission.

Regarding the necessity and proportionality of the system

3. The Commission stresses, firstly, that it is fully aware of the seriousness of the crisis linked to the health situation created by the COVID-19 epidemic, which is on an exceptional scale. The implementation of the "StopCovid" application is part of the Government's strategy to deal with the epidemic and reflects the desire not to overlook any solutions in the fight against the epidemic, and in particular to better manage the period of deconfinement.

4. The fight against this epidemic, which comes under the constitutionally valid objective of health protection, is a major imperative which may justify, under certain conditions, temporary infringements of the right to protection of privacy and personal data. It has thus justified the authorisation, by the above-mentioned Act of 11 May 2020, of measures based on the processing of personal data, which are particularly sensitive and on a national scale. The "Contact Covid" and "SI-DEP" information systems, 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, were authorised in this respect by the aforementioned decree of 12 May 2020, adopted after the Commission's opinion dated May 8, 2020.

5. The Commission would nevertheless point out that the constitutional and conventional protection 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 on Human Rights, require that infringements of these rights by public authorities must not only be justified on grounds of general interest, as is the case here, but must also be necessary and proportionate to the achievement of that objective.

6. In addition, it recalls the sensitive nature of the implementation of a device, made available by the public authorities, for automatically tracking the contacts of users of a mobile application. While the Commission acknowledges that the planned application respects the concept of data protection by design and by default, such a collection, which is intended to apply to the largest possible part of the population, must, in any event, be considered with caution. It refers on this point to its opinion of 24 April 2020.

7. Secondly, with regard to the usefulness of the "StopCovid" application, the Commission pointed out, in its opinion of 24 April 2020, that the planned system would be admissible only if the government had sufficient information to establish its usefulness for the management of the COVID-19 crisis, particularly when the lockdown is lifted. In particular, it had insisted on the need to integrate this system into a global health policy.

8. In this respect, the Commission notes that the Ministry intends, by implementing the application, to supplement the contact tracing system authorised by the abovementioned Decree of 12 May 2020 and thus contribute more effectively to reducing chains of contamination. The purpose of the processing is thus to allow faster information and alert of contact cases regarding the risks of exposure to the virus, particularly in the case of contact cases that the contaminated or exposed persons do not necessarily know about, such as people encountered in public transport or in shopping facilities. It can also alert certain contact cases of users who may not wish to respond to health interviewers.

9. The Commission further notes that the Ministry has reported several scientific and epidemiological studies, including foreign studies, demonstrating the value to health authorities of having "contact tracing" applications available to support manual tracing of the spread of chains of transmission, in order to identify contacts of detected cases as quickly and widely as possible. The Ministry stated that some of these studies lead to the view that such an application is useful for reducing chains of contamination, even when it is downloaded only by a limited part of the population. It also referred to the favourable positions of the COVID-19 scientific council and the National Academy of Medicine.

10. Account should also be taken of the uncertain nature of the information available to the Ministry in this area at the beginning of the deployment of this tool and the difficulty of comparing the planned processing with those already experienced or envisaged in other countries, particularly within the European union.

11. Finally, the usefulness of the application lies in the fact that the planned processing will be linked to the health care system for people exposed to the virus, since the person alerted *via* the "StopCovid" application and who decides, following and in accordance with this notification, to consult a health professional, will then be recorded in the above-mentioned "Covid Contact" or "SI-DEP" information systems.

12. In the light of these elements, the usefulness of the application and the necessity of the planned processing to accomplish the public interest task entrusted to the public authority, within the meaning of the data protection rules, shall be sufficiently demonstrated prior to the implementation of the processing.

13. Thirdly, with regard to the proportionality of the proposed system, the Ministry provides numerous guarantees to limit the data protection infringements that may be caused by such a system.

14. Several substantial safeguards were included in the Government's initial plan, such as the choice to store pseudonymous identifiers of persons exposed to the disease and not of infected persons on the central server, 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 voluntary application and the use of pseudonyms that minimise the possibility of identifying the persons concerned.

15. In addition, the Commission notes that several of the additional guarantees it requested in its opinion of 24 April 2020 have been included in the Government's draft. This applies, in particular, to the precise definition of the purposes of the planned processing, the fact that the data controllership is entrusted to the ministry responsible for health policy and the implementation of certain technical security measures. Similarly, while the alerts generated by the application will be linked to the rest of the health system, the Ministry has confirmed that it does not intend to attach any adverse legal consequences to the fact that the application has not been downloaded and that no specific rights will be reserved for those who use the application. 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 the Council of State of a draft decree on processing based on Articles 6.1(e) and 9.2(i) of the GDPR.

16. The Commission considers that these elements are such as to reduce the risks posed by data processing to the fundamental rights and freedoms of data subjects and make the harm proportionate to the estimated usefulness of the system.

17. Fourthly, the Commission points out that the principle of proportionality also implies that the rights to privacy and the protection of personal data should be affected only for the time strictly necessary to achieve the objective pursued.

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

19. The Commission considers this to be a maximum duration. It requests that the actual impact of the system on the overall health strategy be, independently of the evaluation report provided for in the decree following the overall cessation of the “StopCovid” processing, studied and documented on a regular basis throughout the period of its use, in order to ensure its usefulness over time.

20. It is aware that this assessment will be delicate and must be able to take into account, where appropriate, possible periods of renewed outbreaks of the epidemic. However, it considers that this assessment is essential, since an automated contact tracing tool, made available by the public authorities and installed on the smartphones of individuals, is only admissible, as it stressed in its opinion of 24 April 2020 if it makes a useful contribution to health policy. The Commission requests that these monitoring reports be communicated to it as they are drawn up.

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

Regarding the purposes and responsibility for processing

Concerning the purposes of the processing

22. Article 1 of the draft decree specifies that the purpose of the processing is :

- to inform a user that he/she were in close proximity to at least one other user of the same application who subsequently tested positive for COVID-19, so that there is a risk that they may have been contaminated in turn ;
- to educate users of the application, identified as contacts at risk of becoming infected with SARS-CoV-2, on the symptoms of the disease, protective measures and how to control the spread of the virus;
- referral of at-risk contacts to the competent health actors for their care and access to screening tests;
- to improve the efficiency of the model used by the application for the definition of contact cases through the use of anonymous statistical data at the national level.

23. Firstly, with regard to the referral of contacts at risk to the competent health actors, the Commission notes that the draft decree will be amended to specify that contact between the user and the health professional will be recommended on the notification but will remain at the user's discretion.

24. Secondly, the Commission takes note of the Ministry's clarification that the aim of improving the effectiveness of the health model used by the application on the definition of contact cases is to improve the performance of the application and not to measure its health utility. The Commission understands that other methods, such as statistics or surveys, will make it possible to meet the latter objective.

25. Thirdly, the following are expressly excluded from the purposes pursued by the processing: identification of infected persons, identification of areas in which these persons have moved, making contact with the person alerted or monitoring compliance with containment measures or any other health recommendations. Processing should also not be used to monitor the social interactions of persons.

26. Fourthly, in view of the sensitive nature of the data collected and the purposes of the processing, the Commission welcomes the fact that, in accordance with its recommendation in its deliberation of 24 April 2020, the Ministry of Health is designated as the controller. It considers that such a designation makes it possible to help ensure that both the development and deployment and possible developments of the system are defined by or in conjunction with the competent national health authorities.

A system based on volunteering

27. The government has followed the recommendations of the European data protection board in its opinion N° 04/2020 of 21 April 2020 and of the Commission in its opinion of 24 April 2020 by basing the "StopCovid" application on a mission of public interest, integrated into the global health policy. The Commission had recalled

that the choice of this legal basis does not exclude the fact that the downloading and use of the application is voluntary.

28. 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.

29. The Commission takes note that volunteering materialises in all components of the system: installation of the application, activation of *Bluetooth* communication, contacting a health professional, notification of a positive diagnosis or a positive result of a COVID-19 test in the application, testing following receipt of a notification, de-installation of the application.

Regarding the data collected and processed

Concerning the data collected

30. Firstly, 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 data minimisation and data protection by design in mind right. It also notes that this protocol takes the decision to transmit the identifiers of persons exposed to the virus rather than sending the identifiers of persons actually infected, and that it guarantees that no link will be kept between infected persons and the list of persons they may have exposed to the virus. The Commission notes that this choice protects the privacy of the persons concerned.

31. Article 2 of the draft decree lists the restrictive list of personal data that may be collected in the context of the "StopCovid" application.

32. As the Commission has already noted in its deliberation of 24 April 2020, while the system is intended to process personal data within the meaning of the GDPR, the application only collects adequate and relevant data limited to what is necessary for the purposes for which they are processed, in compliance with the data minimisation principle laid down in Article 5(1)(c) of the GDPR.

33. In addition, personal data concerning health will be processed. The processing of these sensitive data is based on Article 9(2)(i) of the GDPR as mentioned above.

34. However, certain data referred to in the PIA are not mentioned in Article 2 of the draft decree. The Commission takes note of the Ministry's commitment to amend the draft in order to mention the collection of the periods of exposure of users to contaminated persons as well as the country codes. Furthermore, in view of the specificities of the processing, it recommends that the collection of dates of last server query should also be mentioned.

Concerning the accuracy of the data

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

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

37. The Commission notes that the algorithm for determining the distance between users of the application is still under development at this stage and may be subject to future developments. 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 time stamping of these messages will make it possible to estimate the duration of the interaction. Many parameters need to be taken into account in order to be able to correctly estimate distances *via* this technology. To this end, calibration tests are currently being carried out in order to propose a suitable statistical model. The Commission thus notes that the determination of a risky interaction will be carried out on a probabilistic basis, which is in line with the general logic of the application to warn users of a risk of contamination, and that under no circumstances will the receipt of an alert from the application mean that the user has actually been contaminated.

38. The Commission notes that a mobile contact tracing application does not take into account the context in which persons were at the time an exposure to an infected person was recorded. For example, a health professional or a reception agent will be particularly likely to be notified by the application as being at risk of having been contaminated with SARS-CoV-2 even though they were protected (wearing a mask, dividing wall, etc.) at the time the contact was recorded. Thus, failure to take into account the context of the contact by the application is likely to result in the generation of numerous false positives.

39. Consequently, the Commission wonders whether the application should eventually provide for the possibility for the user to define time periods during which contacts should not be considered potentially at risk.

40. In any event, in order to take account of these particular cases, the Commission recommends that the information provided to users should include recommendations on the use of the application in specific contexts. The presence of an easily accessible temporary deactivation button on the main screen of the application could reduce the number of false alarms corresponding to moments when the user is not really at risk.

41. The Commission notes that the transfer of the history of 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 COVID-19 test. Therefore, a user will not be able to falsify the central server database of the application by declaring himself/herself positive without having been diagnosed or tested positive. Furthermore, the Commission notes that the 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.

Regarding the recipients and persons who have access to the data

42. Article 3 of the draft decree specifies that 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 been in proximity of another user which has been diagnosed or tested positive for the virus.

43. Furthermore, the Commission notes that the forwarded PIA lists several actors acting as processors on behalf of the controller.

44. Firstly, the Commission recommends that the draft decree be completed to mention that subcontractors will only be accessing or receiving personal data they need to know with regard to their missions.

45. Secondly, the PIA specifies that the processing relations between the controller and its processors, in particular in their capacity as host, are concluded or provided for in the form of an agreement, during the various phases of the application project, namely the development, production and operating 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 as regards the exercise of the rights of data subjects and security measures.

46. 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 between it and the data controller must, in particular, specify the geographical areas from which the administrators access the infrastructure.

47. Lastly, it notes that Article 1 of the draft decree qualifies INRIA as a subcontractor and states that the processing by INRIA, on behalf of the Ministry, is carried out under the conditions laid down in Article 28 of the GDPR. The Commission wonders about such a qualification in the light of the definition of a subcontractor given in Article 4.8 of the GDPR.

Regarding data transfers outside the European union

48. Both the draft decree and the PIA mention that personal data are not transferred outside the European union. The Commission therefore notes that the processing will take place exclusively on the territory of the European union.

Regarding the storage limitation

49. The Commission notes that Article 4 of the draft decree provides for the keys and identifiers associated with the applications to be kept for the duration of operation of the "StopCovid" application and for no more than six months from the end of the state of health emergency. The local histories of persons diagnosed or tested positive are to be kept for fifteen days from their emission.

50. In accordance with the principle of storage limitation (Article 5(1)(e) of the GDPR), the period of storage of data must be limited to what is strictly necessary for the purposes previously described. Therefore, temporary identifiers exchanged between applications as well as the associated timestamps may not be kept for a longer period of time than the period during which these data are actually useful to determine whether a contact may have led to a risk of contamination. Thus, this period has been estimated at 15 days, in accordance with the recommendation of the French Public Health Agency and the Ministry.

51. The Commission takes note that the user of the application may, at any time, request the deletion of his data from his smartphone and the central server database by means of a feature made available to him in the application, prior to uninstallation. Indeed, if the user can uninstall the application at any time, this will result in 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 to be technically impossible to delete the data on the server after the user has deleted the application,

the data should be deleted after a period of inactivity, to ensure that in such a case data that is no longer needed is not retained. In addition, users should be advised to delete their data from the central server before uninstalling the application.

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

On transparency requirements

52. With regard to compliance with 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 data subjects are informed of the main characteristics of the processing and their rights when the "StopCovid" application is installed and, on the other hand, that information notices are also made available to the public *via* the "https://www.stopcovid.gouv.fr" website.

53. In addition, the PIA states that infographics will complement the information by making the underlying technological concepts more accessible.

54. 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. Such an obligation does not, however, preclude the possibility of adopting a layered approach whereby the controller chooses to include the main features of the processing operation in a first layer. In any case, information in conformity with the provisions of the GDPR must be easily accessible both when the application is installed and throughout its use.

55. Secondly, the Commission insists on the need to provide information that can be understood by as many people as possible, since a large part of the population is likely to be affected by the measures. The information should also be made available in such a way as to enable people with disabilities to become acquainted with it.

56. Special attention should also be paid to minors, even though the information provided will be the same for all users of the application. Minors equipped with smartphones by their parents are indeed likely to download the application, under conditions of common law. For them, even more than for other users, particular attention must be paid to the information provided, so that the application is used properly and the alert message that may be addressed to them is adapted and properly interpreted. The Commission therefore calls for specific developments to be included in the information provided to users, both for the minors themselves and for their parents.

57. In the light of these elements, the examples of information notices provided in the PIA will require further work in order to comply with the provisions of Articles 12 to 14 of the GDPR.

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

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

59. As regards the right to rectification and the right to limit processing, the Commission considers that, in view of the characteristics of the processing, these are

not intended to apply. The same applies to the right of portability, since the processing is not based on Article 6(1)(a) or (b) of the GDPR.

60. The right of access could theoretically concern the consultation by a user of the keys and pseudonymous identifiers associated with his/her own application. Given the fact that consultation of these data is of very little use to the data subject, particularly in view of their pseudonymous nature, and that free consultation of these data by any person who could take possession of the smartphone on which the application is installed would be likely to undermine the security of the system, the Commission considers that it follows from provisions 11, 15(4) and 23 of the GDPR that the Ministry may waive the right of access. This is because the application is designed for public health purposes and pseudonymization is an important element in protecting the privacy of the individuals who will use the system.

On the right of erasure and the right of opposition

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

62. 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 of erasure and, on the other hand, it intends to waive the right of objection on the basis of section 23 of the GDPR.

63. The Commission considers that since the processing is voluntary, the right to erasure and the right to object should be fully applicable. Furthermore, the Commission notes that, in practice, the PIA does provide for the possibility for the user to exercise these rights effectively.

64. Firstly, the user can request the deletion of these data directly *via* the application, both as regards to the data stored on the terminal and the data available on the central server.

65. Secondly, the right to object is materialised 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 equipment. The PIA specifies, in this respect, that the unsubscription must lead to the deletion of data both locally and on the central server and that the uninstallation will lead to the deletion of data locally; the data potentially present on the central server can then no longer be linked to a user.

66. The Commission takes note of the Ministry's commitment to amend the draft decree on these points.

Regarding security measures

67. As a preliminary remark, the Commission notes that the envisaged system has been the subject of additional measures on a number of points raised by the Commission in its deliberation of 24 April 2020.

68. Firstly, as regards to the security of the server responsible for centralising the identifiers of users exposed to the virus, the Commission's opinion drew attention to the need to implement organisational and technical security measures to provide the highest possible guarantees against any misuse of data, given the centralised nature of the protocol implemented within the "StopCovid" application. As such, the

Commission notes that the Ministry will resort to security modules to protect the encryption keys allowing access to data subjects' identifiers.

69. The Commission also notes that the controller plans to set up a committee bringing together several entities to which fragments of the encryption keys would be entrusted, in order to ensure that no single actor can misuse the data. The Commission considers that such a measure is likely to limit the risks of corruption of the central database, and calls on the Ministry to include in this committee organisations of different types and with a high level of independence, and notes that the participation of scientific research institutions would further increase the level of guarantee provided by the system. However, the Commission calls on the Ministry to specifically assess the level of guarantee offered by such a measure in the PIA, and to put in place additional guarantees if necessary.

70. Secondly, regarding the use of cryptographic mechanisms, the Commission recalls that in its opinion it expressed its views on the need to resort to state-of-the-art cryptographic algorithms that comply with the General Security Reference Framework published by the National Cybersecurity Agency of France (ANSSI). The Commission notes in this respect that the protocol has evolved, with the 3DES encryption algorithm replaced by SKINNY-CIPHER64/192, as recommended by the ANSSI.

71. Thirdly, regarding the publication of the source code, the draft decree mentions that some elements of the "computer code" of the application or of the central server will not be made public, as this would compromise 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.

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

73. The Commission notes that only individually authorised persons will be able to access the data stored on the central server. The Commission recalls that the authentication procedures for these persons must comply with Decision No. 2017-012 of 19 January 2017 adopting a recommendation on passwords, and that, given the nature of the processing, the Commission recommends that strong authentication mechanisms be put in place.

74. The Commission notes that the infrastructure provider hosting the StopCovid platform, acting as a data processor, is qualified as SecNumCloud by ANSSI, is certified as a Health Data Host (HDS) and implements ISO/IEC 27001 certified data centers.

75. In addition, the Commission notes that, in accordance with the General Security Baseline, StopCovid will be subject to security certification before the application is put into production. It also notes that ANSSI is involved in the implementation of the application and that a number of recommendations have been issued by ANSSI to the controller.

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

77. The Commission notes that the Ministry plans to use a CAPTCHA when initializing the application, in order to verify that it is being used by a natural person. The Commission notes that the planned CAPTCHA is based, as a first step, on the use of a service provided by a third party. The Commission notes that the use of this service is likely to involve the collection of personal data not provided for in the Decree, data transfers outside the European Union, and read/write operations that would require the user's consent. 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 a subcontracting agreement. Consequently, the Commission calls on the Ministry to be vigilant and would like to see further developments of the application to allow the use of alternative technology in the near future.

78. Finally, the Commission notes some operations are planned to be subject to logging measures. Regarding data relating to technical errors, the Commission recommends that only the minimum amount of data strictly necessary for checking the proper functioning of the system should be logged, and in particular that these logs should be free of user identifiers or cryptographic keys. With regard to the logging of actions carried out by administrators, the Commission recommends that it should be kept for a period of six months under conditions that guarantee its integrity, and that automatic analysis mechanisms should be put in place to detect any abnormal operation.

79. The Commission notes that evolutions in the application and the contact tracing protocol, in particular in order to enable EU-wide interoperability, are likely to be developed in the medium term. The Commission also takes note of the Ministry's intention to request the Commission’s opinion, including on an optional basis, on any changes to the processing operation.

The Chairwoman

Marie-Laure DENIS