Deliberation 2020-087- of September 10, 2021 National Commission for Computing and Liberties Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Thursday December 23, 2021 Deliberation n° 2020-087 of September 10, 2020 issuing a public opinion on the conditions for implementing information systems developed for the purpose of combating the spread of the COVID-19 epidemic (May to August 2020) (request for opinion no. 20014534) The National Commission for Computing and freedoms, 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; Having regard to Law No. 78-17 of January 6, 1978 modified relative data processing, files and freedoms; Having regard to law n° 2020-546 of May 11, 2020 extending the state of health emergency and supplementing its provisions, in particular its article 11; Having regard to law n° 2020-856 of July 9, 2020 organizing the end of the state of health emergency; Considering the decree n ° 2019-536 of May 29, 2019 modified taken for the application of the law n ° 78-17 of January 6, 1978 relating to data processing , files and freedoms; Having regard to Decree No. 2020-551 of May 12, 2020 relating to the information systems mentioned in Article 11 of Law No. 2020-546 of May 11, 2020 extending the state of health emergency and supplementing its provisions; Decree No. 2020-650 of May 29, 2020 relating to the processing of data called STOPCOVID; Considering Decree No. 2020-1018 of August 7, 2020 taken pursuant to Article 3 of Law No. 2020-856 of July 9 2020 organizing the end of the state of health emergency and modifying 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; Having regard to the decree of July 10, 2020 prescribing the general measures necessary to deal with the COVID-19 epidemic in the territories emerging from the state of health emergency and in those where it was extended; On the proposal of Marie-Laure DENIS, President, and after having heard the observations of Mr. Benjam in TOUZANNE, Government Commissioner,Issuing the following opinion:As part of the progressive deconfinement strategy, the law of May 11, 2020 extending the state of health emergency authorized the temporary creation of two national files: SI -DEP and CONTACT COVID. This processing of personal data is governed by a Conseil d'Etat decree of 12 May 2020 which specifies their methods of creation and implementation. These files must make it possible to identify people infected with COVID-19, people they are likely to have contaminated and the chains of contamination. They aim to provide health care and support for people with the virus or likely to be, as well as epidemiological

surveillance. Alongside these files, there is the deployment of the STOPCOVID mobile application. treatment, governed by decree no. 2020-650 of May 29, 2020 and implemented by the Minister responsible for health, aims to inform users that they have been close to people diagnosed positive for COVID-19 who have of the same application. The SI-DEP and CONTACT COVID files containing a large amount of personal data, including health data and which can be consulted by a large number of actors, in particular by health investigators for the benefit of whom the law has expressly authorized the lifting of medical secrecy, the legislator wished to regulate their implementation. It thus, on the one hand, set up a COVID-19 Control and Liaison Committee and, on the other hand, provided that the Government ment sends Parliament a detailed report on the application of these measures every three months from the promulgation of the law of 11 May 2020 and until the disappearance of the information systems. Finally, the legislator wished to supplement these reports with a public opinion from the National Commission for Computing and Liberties, the subject of this deliberation. In an exceptional context of health crisis and emergency, the Commission has intensified the relations that it maintains regular contact with Parliament as part of its mission to support the public authorities (opinions on draft texts; hearings). The Commission has thus responded to the latter's many requests (ANNEX 1), within particularly short deadlines, given the timetable for the adoption of bills. It was thus heard five times in April and May 2020. In addition, five opinions issued by the Commission in this context of health emergency were able to make a useful contribution to parliamentary debates on fundamental issues related to respect for life. privacy and personal data. This opinion of the Commission issued on the basis of article 11 of the law of May 11, 2020 will endeavor, in particular with regard to the recommendations it has issued in its opinions, to recall the framework standard in which these treatments fall, and, to be assessed for the period from May to August 2020: the interest of these treatments with regard to the health situation as described by the Government; the operational conditions for the implementation of these treatments with regard to the findings made within the framework of its supervisory powers.I – REMINDER OF THE NORMATIVE FRAMEWORK AND OF THE COMMISSION'S RECOMMENDATIONSIn accordance with the law, the opinion of the Commission was requested by the Govern ment on all the texts governing the implementation of processing related to the health crisis.o The Commission's opinion on the SI-DEP and CONTACT COVID information systemsIn its first opinion on the draft decree creating the SI-DEP and CONTACT COVID processing dated May 8, 2020, the Commission considered that the device presented was globally compliant with the General Data Protection Regulation (GDPR), a certain number of guarantees being provided (temporary nature of this device , limitation of the health data processed or the voluntary nature of participation

in surveys). However, it considered it necessary for the draft decree to be supplemented and called for certain legal, technical and organizational safeguards to be strengthened. according to the categories of users, so that this can only be carried out within the strict limits of their missions; the deletion in the draft text of the collection, without further specification, of information on the links between a patient 0 1 and a contact case. The decree removed this mention and only provides for the collection of precise and circumscribed information on this point (the fact of knowing each other or not, the existence of a cohabitation, the date of the last contact); the implementation of training adapted to the use of these tools for the investigators and the other persons concerned (personnel of the analysis laboratories, doctors and other health professionals, pharmacists, researchers, etc.); the implementation of a consultation traceability system in order to identify abuses and be able to sanction them; the need to carry out a more detailed reflection on the data retention periods. Guarantees were provided on this point in the law of May 11, 2020; the right of opposition, which was excluded in the project, except to allow patient 0 not to have his name revealed to his contact cases and for certain transmissions of their data for research purposes. The Commission has requested that the restriction of the right to object to files be kept to a minimum. In this sense, a right of opposition has been opened by the decree to contact cases for the processing of their data in CONTACT COVID and patient 0 must have given his consent for his identity to be revealed to contact cases. Its second opinion, issued on July 23, 2020, concerned a draft decree extending to six months after the end of the state of health emergency the retention period for pseudonymised data collected in the context of these information systems for the purposes of epidemiological surveillance and research on the COVID-19 virus, as previously authorized by the law of July 9, 2020. Indeed, the law of May 11, 2020 had provided strong guarantees on the retention periods of data in limiting the retention of data in information systems to three months from their collection. The Commission's observations were mostly followed by the Government in Decree No. improving the methods of informing the people concerned; access by the regional health agencies (ARS) to CONTACT COVID data for epidemiological surveillance and research purposes, which was not planned. u by the decree of 12 May; the limitation of the addition of other identification numbers only if the registration number in the identification directory of natural persons (NIR or social security number) cannot be collected. The Commission's proposal to draw up an exhaustive list of data allowing the purpose of epidemiological monitoring and research on the virus was not taken up, however.o The Commission's opinion on the centralization of certain health data in the within the Health Data Hub (PDS or Health Data Hub) and the National Health Insurance Fund (CNAM) As of April, the Government, in the context of the emergency linked to the management of health crisis, wished, by decree, to

organize the grouping of certain personal data, including health data and data from the National Health Data System (SNDS), in order to allow their use in order to monitor and project them evolutions of the epidemic, to prevent, diagnose and treat the pathology as well as possible and to organize the health system to fight the epidemic and mitigate its impacts. To do this, it wanted to modify the traditional information feedback circuits relating in particular to medical activity, and allow the centralization of useful data within the Health Data Platform (PDS), then later by including certain data from the SI-DEP and CONTACT COVID files (decree of 12 May 2020). The Commission, in its urgent opinion issued on 20 April 2020, drew the Government's attention in particular to: the risks linked to the conditions for the early start of the technical solution of the PDS in a context where it had to, in order to guarantee data security, carrying out operations in a few weeks, some of which were structuring, which were planned to take place over several months; the use by the PDS of IT data hosting providers who transfer data outside the European Union European Union and the possible material and legal risks in terms of direct access by the authorities of third countries. Indeed, the contract concluded between the Platform and its host mentions the existence of data transfers outside the European Union as part of the day-to-day operation of the Platform, in particular for maintenance or incident resolution operations. In its judgment of July 16, 2020 in the so-called Schrems II case, the Court of Justice of the European Union (CJEU) held that the law of the United States of America does not ensure an essentially equivalent level of protection. to that guaranteed by EU law. However, the PDS recently sent the Commission an amendment concluded with one of its service providers, through which the latter provides additional guarantees relating to the storage and processing of data. These guarantees will have to be analyzed in detail in order to determine whether they make it possible to conclude that there is no transfer outside the European Union. The Commission will also be attentive to the consequences of the analysis of the legislation of the United States of America, by the Schrems II decision of the CJEU, on the situation of the PDS; the importance of pseudonymisation measures: pseudonymisation is a security measure which makes it possible to limit the risks for the people whose data will be processed.The decree of April 21, 2020 authorizing the centralization of certain health data within the PDS for the management of the health emergency and the improvement of knowledge on COVID-19 was the subject of an urgent appeal to the Council of State. By an order issued on June 19, 2020, the Council of State essentially dismissed the appeal and ordered the PDS to provide the Commission with all the information relating to the pseudonymization methods used. The elements transmitted are currently being examined. This centralization and the possible uses of this data are today governed by article 30 of the decree of July 10, 2020 prescribing the general measures necessary to deal with the epidemic. of

COVID-19 in territories that have emerged from the state of health emergency and in those where it has been extended, replacing the decree of April 21, 2020 supplementing the decree of March 23, 2020. This decree provides that the data may be processed only for projects pursuing a public interest purpose in connection with the current COVID-19 epidemic and until the entry into force of the SNDS decree and no later than 30 October 2020.The Commission will to decide soon on the draft SNDS decree which will frame the respective roles of data controllers and specify the categories of data collected within it.o The Commission's opinion on the STOPCOVID mobile application Since the start of the epidemic ie of SARS-Cov-2, several States in the world have chosen to use automated "contact tracing" devices whose practical implementation, with variable geometry, proves to be more or less respectful of fundamental rights and freedoms and including respect for the privacy of its users. Very early on, the Commission focused on the development of these tools, which enabled it to exchange very quickly with its European counterparts in order to work on the development of common requirements for this type of device. context, the European Data Protection Board (EDPB) published, on 21 April 2020, guidelines on the use of geolocation data and "contact tracing" tools in the context of the coronavirus pandemic. COVID-19. These guidelines notably clarify the legal framework applicable to "contact tracing" applications and issue recommendations for Member States wishing to use such devices as part of their health strategy. Thus, the guidelines are accompanied by a technical guide aimed at developers of contact tracing applications. Without being exhaustive, the guide draws up a list of concrete technical recommendations aimed at integrating the principle of data protection by design enshrined in the GDPR. The recommendations mainly concern the nature of the data processed, the functionalities as well as the security measures. They are the result of a harmonized European vision of the guarantees that must be implemented in the context of the use of such devices: use based on the voluntary participation of individuals, use of Bluetooth technology, use of pseudonymised personal data (pseudonymous identifiers), publication of the source code of the device, etc. It is on the basis of this European analysis grid that the Commission issued its opinions in the context of referrals from the Government on the STOPCOVID application. The first opinion , adopted on April 24, 2020, dealt with the possible implementation of the STOPCOVID application. At this stage, the deployment of this application and its exact methods of implementation had not yet been decided. In its opinion, the Commission: insisted on the need to demonstrate that the usefulness of the application for the management of the crisis is sufficiently proven and that the appropriate guarantees are provided (use of pseudonymised data, technical security measures, limitation of the device in time, limited retention period of the data, etc.); it has been confirmed that the application would process many personal data (in particular data concerning

health) in a pseudonymised form (therefore well subject to the GDPR) and not anonymized as has sometimes been put forward; welcomed the voluntary nature of the use of such a device and asked that no negative consequences be attached to the choice not to use the application (access to tests and care, access to certain services, etc.); issued a series of recommendations on the additional safety measures to be taken. Following the Commission's recommendation to have an explicit and precise legal basis in national law, on which it would be consulted beforehand, the Ministry in charge of Health referred the matter to the Commission, on May 15, 2020, of a request for an opinion concerning a draft decree relating to the mobile application called STOPCOVID. This new referral enabled the Commission, on the one hand, to note that the main recommendations formulated in its previous opinion had been taken into account and, on the other hand, to make several observations both on the draft decree and on the operational conditions for deploying the application: the Commission considered in a second opinion dated 25 May 2020, that the application could be legally deployed since it appears to be a complementary instrument to the manual contact tracing device and that it allows faster alerts in the event of contact with an infected person, including contact with unknown persons. However, the Commission highlighted the need to dynamically assess the effective impact of the system on the overall health strategy in order to ensure its usefulness over time. The duration of the system's implementation should be conditional on the results of this regular assessment; given the sensitivity of the application, the Commission has made several recommendations, including: improving the information provided to users, in particular with regard to the conditions of use of the application and the procedures for erasing personal data; the need to issue specific information for minors and parents of minors ;consecration, in the forthcoming decree, of a right of opposition and a right to erasure of pseudonymised data recorded both on the user's smartphone and on the central server;the opportunity to develop an alternative technology to that used to verify that the application is indeed used by a natural person. Indeed, the use of a "captcha" system provided by a third party was not only likely to lead to the collection of personal data not provided for in the decree, but also to lead to the transfer of data outside the European Union. European Union as well as read/write operations which would require the user's consent; free access to all the source code of the mobile application and the server. The publication of decree no. 2020-650 of May 29, 2020 enabled the Commission to observe that many observations have been followed by the government: the list of data collected has been completed, the right to object and the right to erasure are no longer set aside by the text, the sub-sections processors have been mentioned as accessors or recipients of the personal data they will need to know, the concept of computer code has been replaced by the concept of

source code. II - ON THE MAINTENANCE OF THE SYSTEMS WITH REGARD TO THE PRINCIPLES OF NECESSITY AND PROPROTIONALITY As underlined by the Commission in its various opinions, the derogatory nature of the various processing operations implemented can only be justified if their usefulness is sufficiently proven with regard to the health developments in the country. The seriousness of the crisis linked to the health situation created by the COVID-19 epidemic, of exceptional magnitude, has led the Government to leave aside no tool to fight against the epidemic. This fight, which falls under the constitutional objective of protecting health, constitutes a major imperative likely to justify, under certain conditions, infringements of the right to protection of privacy and personal data. 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 Human Rights human 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 such systems which allow in particular nt the processing and sharing of health data, which can be consulted by a large number of actors and require additional protection. The principle of proportionality also implies not infringing the rights to privacy and data protection to personal nature only for the time strictly necessary to achieve the objective pursued. In this regard, the Commission took note of the temporary nature of these measures, the term of implementation of which is set by the decrees governing their creation, at six months from the end of the state of health emergency, i.e. as of January 11, 2021.While the assessment of the need to maintain these systems does not belong to the Commission as part of its missions, it is aware that the assessment of their usefulness is delicate and that it must be able to take into account, where applicable, possible periods of resurgence of the epidemic. However, it considers this assessment to be essential since these devices are only admissible if they make a useful contribution to health policy and asks the Government to ensure this. liaison COVID-19 in its report appended to the Government report addressed to Parliament, to have performance indicators for the information systems deployed, in order to be able to measure their effectiveness with regard to the objectives pursued. It considers that an analysis grid should be established with regard to health efficiency indicators. In addition, the Commission had requested, in its opinion of 25 May 2020 relating to the STOPCOVID mobile application, that the of the system on the overall health strategy is studied and documented by the Government on a regular basis throughout its period of use. It was however noted, on the day of the

checks, that the formal evaluation of the effectiveness of the application n had not yet started and that the timetable for the evaluation work had not yet been drawn up by the Ministry. In this respect, and without calling into question the usefulness of these mechanisms at this stage, the Commission regrets that the report of the Government sent to Parliament on September 9, 2020 does not mention more specific elements justifying the need to maintain these treatments in view of the current health context. The Commission is aware that the deployment of these systems is recent and that the Government has little perspective on their operation. She is also aware that these measures were implemented when the epidemic was decreasing and that a revival is currently underway. However, it considers that this assessment is essential and urgent, in particular with regard to the risks inherent in this processing for the rights and freedoms of individuals. For example, if the report mentions the number of downloads of the STOPCOVID mobile application, it does not make it possible to sufficiently assess the effective impact of this system in the fight against the epidemic (lack of analysis relating to usage statistics, the results of any surveys carried out among users, professionals or the general public, at the number of cases identified through the application). The Commission points out that these files are used for the purpose of combating the spread of the COVID-19 epidemic for the duration strictly necessary for this purpose or, at most, for a period of six months from the end of the state of health emergency declared by article 4 of law n° 2020-290 of March 23, 2020. Any extension of these information systems beyond January 11, 2021 can therefore only be authorized by law In addition, the Commission recalls that it must be informed of any modification made to the decree relating to the SI-DEP and CONTACT COVID information systems. Similarly, the personal data collected by these information systems cannot be kept after a period of three months after their collection, with the exception of data collected for the purposes of epidemiological surveillance at national and local, for research on the virus and the means of combating its spread, for which a maximum storage period of six months from the end of the state of health emergency has been set by Decree No. 2020- 1018 of August 7, 2020. III- COMMISSION'S ASSESSMENT OF THE OPERATIONAL CONDITIONS FOR IMPLEMENTING PROCESSING In parallel with its mission of advising and supporting compliance, the Commission may inspect organizations in order to verify the concrete conditions of implementation of any processing of personal data. These checks can be carried out online, by hearing, on documents or on site. Thus, in accordance with what she announced during her public hearing before the National Assembly on May 5, 2020, the President of the Commission decided to carry out a series of checks on the SI-DEP and CONTACT COVID devices and the STOPCOVID2 application. of the three aforementioned devices. This opinion includes summary elements resulting from the findings made by the

Commission during the first phase of checks as well as regular exchanges which take place with the Ministry of Solidarity and Health and the other actors involved, in particular the CNAM and the agencies. (ARS).o Control of SI-DEP and CONTACT COVID files: Investigations have been carried out simultaneously on SI□DEP and CONTACT COVID treatments since June 2020 and give rise to meetings, hearings and on-site and document checks with the various players. HP), which manages the operational implementation of the SI-DEP treatment and private laboratories in order to carry out checks relating to the reception of patients. For the CONTACT COVID treatment, cont roles on documents, on hearing and on site took place with a health establishment, a primary health insurance fund (CPAM), an ARS, the National Council of the Order of Physicians (CNOM) and the National Council of the Order of Pharmacists (CNOP). The verification points mainly concerned: the procedures for obtaining consent and information from individuals; the security of information systems; data flows and recipients; compliance with the rights of access or opposition of persons.The SI-DEP file At this stage of the verifications carried out by the Commission, and subject to the finalization of the examination of the procedure, the control missions carried out with the AP-HP and medical biology laboratories have revealed a satisfactory overall level of compliance. The departments noted the care taken to comply with data protection regulations despite the context of the health crisis, which strongly mobilized hospital resources, as well as a schedule for implementing very short given the scale of the project (more than 4,500 laboratories connected, 4.2 million tests recorded at the end of July). The control teams noted the implementation of the following best practices: the categories of data collected are limited to what is provided for in the decree establishing the processing. The AP-HP has defined the fields that must be filled in in order to ensure the uniformity of patient files and the processing of reliable data despite the multiplicity of parties involved in the treatment; a very significant effort has been made to raise awareness all actors in the processing chain to data protection issues concerning processing (dissemination of guides adapted to the various management software interconnected with SI-DEP used by laboratories, close collaboration with software publishers with a view to their development) ;the recipients of the data correspond to those provided for by the texts. Each organization accessing the file has designated a local administrator, in charge of issuing authorizations to users of the solution within his organization. This principle of delegation of authorizations granted to the users of the tool makes it possible to ensure partitioning and granularity of access to personal data guaranteeing their confidentiality; the implementation of significant means to ensure the information of persons concerned with the processing of their data and this for the various possible points of contact with patients; finally, the processing documentation required under the provisions of the GDPR

(register of processing activities, data protection impact analysis, register data breaches, etc.) is updated as soon as necessary. With regard to data security, the level achieved within the framework of the SI-DEP system is generally satisfactory, in particular due to the use of software solutions already tested and mastered by the AP-HP. In particular, the procedure allowing patients to access their test result is based on strong authentication, avoiding the disclosure of their health data through insecure channels. In addition, a watch is carried out on security incidents that could lead to a breach of personal data, and the anomalies detected are carefully traced. However, some improvements still need to be made concerning the management of administration accounts and the traceability of access. In the current state of the checks, the Commission will approach the Ministry of Solidarity and Health in the very next few days in order to draw its attention to the practices to be improved and the measures to be taken as a result. The COVID Contact File During inspections, the Commission's teams found that the CONTACT COVID teleservice, expressly designed and developed by the CNAM to follow up on contact cases , benefits from regular changes to meet the requests for improvement from the various users (ARS, health professionals working in private practice, health establishments, etc.). The CONTACT COVID treatment allows city doctors/health establishments/health centers (level 1), authorized health insurance personnel (level 2) and ARS (level 3) to collect information on contact cases and chains of contamination. The inspection teams observed different levels of maturity in terms of the protection of personal data depending on the organisations. data protection. Most of them were well aware that this system involved the collection of health data, which is sensitive data by nature and which therefore requires additional protection. In this respect, certain good practices, implemented in a constrained deadline and exceptional health conditions, must be underlined: the development by the CNAM of methodological guides intended for the actors intervening at each level of the system (doctors for level 1, authorized health insurance personnel for level 2 , ARS for level 3 as well as laboratories and pharmacists). These guides allow the actors involved in the teleservice to understand the context of implementation of the processing and the functionalities of the service; the carrying out, by certain controlled bodies, of impact analyzes relating to data protection and the updating as a result of the register of processing activities relating to CONTACT COVID; secure access to the teleservice by the actors involved in the contact tracing system by means of an identification and strong authentication mechanism is satisfactory (e.g. access by health insurance agents using a smart card). Bad practices have also been noted: in the context of checks carried out at a health establishment, it appeared that the information given to patients 0 and contact cases on processing (purpose, data retention period, recipients of the information, etc.) are sometimes

fragmented, in the absence of delivery of an information medium issued by the CNAM. However, incomplete information does not allow patients 0 and contact cases to fully understand the processing that is carried out on their data and the rights they hold in this regard (right of access or opposition where applicable) . As of June 25, 2020, however, it was noted that 42% of patients 0 who declared contact cases exercised their right to oppose the communication of their identity to at least one contact and that 21% of them refused dissemination to all of their contacts; in an ARS, the Commission's control teams found that no procedure for exercising computer rights and freedoms for patients 0 and contact cases had been formalized ; it was found that CPAMs sent health data by email to an ARS without using secure messaging; it was found in a hospital that, on instructions from the CNAM, it was the occasional sending of health data recorded in files separate from the main information system, which leads to the scattering of files and does not allow satisfactory management of the retention period of the data. Initial exchanges have taken place between the CNAM and the Commission on the various practices noted during this first phase of control. The Commission is aware of the difficulty, at this stage, for the data controller to ensure the correct application of the personal data protection rules by all the bodies called upon to participate in the processing in a very large number of places. . It also points out that the checks were carried out at the very beginning of the implementation of the processing operations which are still in the process of being developed. It was decided to send a request for compliance as soon as possible to each organization involved (CNAM, ARS, Ministry of Health) in the coming days. Failing to comply with the requirements of the GDPR, it will be up to the President of the Commission to determine whether the adoption of a corrective measure is necessary.o Control of the STOPCOVID application: On June 2, 2020, the STOPCOVID application was deployed by the Ministry of Solidarity and Health in application stores accessible to the general public. Checks on this application were then carried out with the Ministry of Solidarity and Health, responsible for this processing, but also with other organizations involved in its implementation, including in particular the National Institute for Research in Digital Sciences and Technologies (INRIA), which designed the protocol on which the application is based and which acts as an assistant to mastering the work. The verification points focused in particular on: the procedures for obtaining consent and information from individuals; the security of information systems; data flows and the destinations areas; respect for the rights of access or opposition of persons and organizations involved in the implementation of processing. The checks carried out have shown that the operation of the STOPCOVID mobile application essentially complies with the applicable provisions. relating to the protection of personal data and that most of the recommendations formulated by the Commission in its opinions of April 24 and May 25, 2020 have been

taken into account by the Ministry of Solidarity and Health. During the checks, certain shortcomings to the provisions of the GDPR and the Data Protection Act were noted in the first version of the application called v1.0. Concomitantly with the Commission's control, the ministry quickly deployed a second version of the application called v1.1 in order to make changes to the way data is processed. In view of the shortcomings noted, the Ministry of Solidarity and Health has been suspended. dies on July 15, 2020, within one month, to: stop transmitting the data of all the people with whom the user has been in contact with the central server, for example by forcing the update of the application STOPCOVID to the new version v1.1 by blocking the application in its version v1.0; complete the information provided to users of the STOPCOVID application, by providing users with complete information on the recipients or categories of recipients of personal data from the application; ensure that the subcontracting contracts concluded in the context of the operation of the STOPCOVID application contain the information provided for in Article 28 of the GDPR; complete the AIPD issued of the STOPCOVID application in accordance with article 35 of the GDPR:by mentioning the collection of the IP address of the mobile equipment of the user of the application within the framework of the security measures of the system based on the DDOS solution of the company ORANGE; by mentioning the collection of information present on the the user's mobile equipment as part of GOOGLE's reCaptcha technology deployed as part of version v1.0 of the application, in the event that this data is still collected; ensure, where applicable, to inform and obtain the consent of the persons concerned to the actions of reading and writing information present on the electronic communication terminals by the company GOOGLE within the framework of the reCaptcha technology (version v1.0 of the application), in accordance with the provisions of Article 82 of the Data Protection Act. This injunction targets the case of users who have downloaded version v1.0 of the application and have not yet activated it for the first time. Given the number of people concerned (approximately two million three hundred thousand downloads as of this opinion) and the sensitive nature of the personal data used in the STOPCOVID application, which relates to the state of health of some of the users, the Commission has decided to make this formal notice public. By letter dated August 14, 2020 , the Ministry of Solidarity and Health sent the Commission some responses and documents relating to the measures taken to comply with the formal notice adopted by the President of the Commission. Actions taken by the ministry included technically forcing users to use a new version of the app (v1.1) where contact history pre-filtering is done at the phone level. . With this version, it is now impossible for the user's entire contact history to be transmitted to the central server, without pre-filtering at the telephone level. Similarly, the ministry no longer uses the reCaptcha system offered by Google. There are therefore no longer any read and write

operations on the terminal in connection with this technology, even for users of the first version of the application (v1.0). associated supporting documents (screenshots, source code of the different versions of the application, updated contracts, etc.), it appears that all of the requests expressed by the President of the Commission in the formal notice to the July 15, 2020 have been satisfied. As the processing operations implemented now comply with the requirements of the GDPR, the President of the Commission declared the closure of this formal notice on September 3, 2020. In the event of changes to the application, the Commission will always be able, if necessary, to carry out new verifications.o A continuous control procedure: The Commission stresses that the controls will continue throughout the period of use of the files, until the end of their implementation. work and sup pressure of the data they contain. It also recalls that the checks carried out give rise to numerous exchanges with the Ministry of Solidarity and Health but also with other organizations (CNAM, ARS, laboratories, CNOM, etc.). This opinion is therefore only a summary of these exchanges and the findings made during the first phase of inspections. In this respect, the second phase of inspections is already planned and will begin before the end of September. 2020. It will mainly concern the following points: Concerning SI-DEP processing: the interconnection of the Health Data Platform with the SI-DEP file, not operational on the date of the first checks; the transfer of data to organizations third parties (data feedback for epidemiological monitoring (pseudonymized data) from the DREES or Public Health France; Concerning CONTACT COVID processing: the procedures for implementing the CONTACT COVID processing access portal for partners who do not have no ameli pro account; the information provided to patients by doctors and pharmacists on the CONTACT COVID treatment. For these two treatments, the investigations will also cover on the effectiveness of the measures provided for the exercise of the rights of data subjects. The next public notice from the Commission will report on the results of these checks. Finally, a third wave of checks will be carried out once the processing has been implemented. On-site checks will thus be carried out with the organizations concerned, in order to verify in particular the effective deletion of the data. The checks should relate to the retention periods of the data, their deletion and/or their possible anonymization. This last point also concerns the STOPCOVID application. The verifications carried out by the Commission on this occasion may also relate to aspects referred to in the formal notice of July 15, 2020. The President Marie-Laure DENISANNEX 1: List of parliamentary hearings and opinions issued by the CommissionList of Commission hearings: April 8, 2020: hearings before the National Assembly's law commission and before the two rapporteurs of the National Assembly's economic affairs commission; April 15, 2020: hearing before the Senate's law commission; May 1, 2020: hearing before the rapporteur of the Senate Social Affairs

Committee on the bill extending the state of emergency; May 5, 2020: hearing before the National Assembly's law committee on the bill extending the state of emergency emergency; List of opinions given on the three treatments SIDEP, CONTACT COVID and STOPCOVID: CNIL deliberation no. 2020-044 of April 20, 2020 providing an opinion on a draft co supplementing the decree of March 23, 2020 prescribing the organizational and operational measures of the health system necessary to deal with the COVID-19 epidemic in the context of the state of health emergency; Deliberation No. 2020- 046 of April 24, 2020 of the CNIL issuing an opinion on a draft mobile application called StopCovid;Deliberation n° 2020-051 of May 8, 2020 issuing an opinion on a draft decree relating to the information systems mentioned in article 6 of the bill extending the state of health emergency; Deliberation n° 2020-056 of May 25, 2020 issuing an opinion on a draft decree relating to the mobile application called StopCovid; Deliberation n° 2020-083 of July 23, 2020 issuing an opinion on a draft decree taken pursuant to Article 3 of Law No. 2020-856 of July 9, 2020 organizing the end of the state of health emergency relating to the retention period of pseudonymised data collected for the purposes of epidemiological surveillance and research on vi rus de la COVID-19ANNEX 2: Description of SI-DEP, CONTACT COVID and STOPCOVID treatmentsSI-DEP treatment is a national information system implemented by the Ministry of Health which allows the centralization of test results at SARS CoV-2 carried out by public or private laboratories. These results are transmitted to SI-DEP either automatically (4500 laboratories connected) or manually. This centralization then allows data to be transmitted to various recipients, in particular: to the regional health agencies (ARS) and to the Primary Health Insurance Fund (CPAM), with a view to carrying out investigations relating to contact cases, within the framework from the CONTACT COVID teleservice.to the Department of Research, Studies, Evaluation and Statistics (DREES) and to Public Health France in a pseudonymised form, for the purposes of epidemiological surveillance and the dissemination of statistical information.to the Health Data Platform (PDS) and the National Health Insurance Fund (CNAM) for the sole purpose of facilitating the use of health data for the purposes of managing the health emergency and improving knowledge on the virus. The CONTACT COVID treatment implemented by the National Health Insurance Fund (CNAM) collects information on contact cases and chains of contamination and aims to detect the contact cases at three different levels. It allows: community doctors/health establishments/health centers to initiate a follow-up sheet for patient 0 and their contact cases (level 1); authorized insurance personnel disease (or to persons to whom this mission is delegated by the texts) (level 2):

to complete and refine, if necessary, the Patient 0 sheet and the list of his contact cases; to call the contact cases to

communicate to them the instructions for quarantine, tests and other actions to be taken; to the Regional Health Agencies (ARS) to ensure (level 3): their follow-up missions of contact cases; the management of situations requiring specific care. These include, for example, chains of transmission in a school environment, in a health establishment or in a youth center. , made available by the Government as part of its overall strategy of progressive deconfinement. It alerts users of a risk of contamination when they have been near another user who has been diagnosed or tested positive for COVID-19. While in use, the smartphone stores a list of temporary nicknames of devices it has encountered for 14 days (this is called proximity history). When a user is diagnosed or tests positive for COVID- 19, he can choose to declare himself in the application and, thus, send his contacts' data (pseudonymous business cards) to a central server. The transmission of this data to the server will only be possible with a single-use code given by a health professional following a positive clinical diagnosis or a QR Code given to the person at the end of his test. The server then processes each of the contacts listed in the proximity history and calculates the virus contamination risk score for each. A user's application will periodically query this server to see if one of the identifiers attached to it has been reported by a person diagnosed or screened for COVID-19 and if the associated risk score reaches a certain threshold. Once notified that they are a contact, and therefore at risk, the person is notably invited to consult a doctor.ANNEX 3: List of texts and their main contributions to the protection of personal dataLaw n° 2020-546 of 11 May 2020 extending the state of health emergency and supplementing its provisions: authorizes, for the sole purpose of combating the COVID-19 epidemic, the processing and sharing of personal health data within the framework of information systems created by decree in Council of State; 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: creation of SI-DEP and CONTACT COVID processing; Decree No. 2020-650 of May 29, 2020 relating to the processing of data called STOPCOVID: establishes the STOPCOVID application; Law No. 2020-856 of July 9, 2020 organizing exit from the state of health emergency: at authorizes the extension of the retention period of pseudonymised data collected within the framework of the SI-DEP and CONTACT COVID information systems for the purposes of epidemiological surveillance and research on the COVID-19 virus; Decree No. 2020-1018 of August 7, 2020 taken pursuant to Article 3 of Law No. 2020-856 of July 9, 2020 organizing the end of the state of health emergency and amending Decree No. 2020-551 of May 12, 2020 relating to information systems mentioned in Article 11 of Law No. 2020-546 of May 11, 2020 extending the state of health emergency and supplementing its provisions: extended to six months after the end of the state of health emergency the retention period of

pseudonymised data collected within the framework of these information systems for the purposes of epidemiological surveillance and research on the COVID-19 virus Order of July 10, 2020 prescribing the general measures necessary to deal with the epidemic of COVID-19 in the ter territories that have emerged from the state of health emergency and in those where it has been extended: regulates the centralization of data from the SI-DEP and CONTACT COVID files within the Health Data Platform and the CNAM and their use (replaces and repeals the decree of April 21, 2020 supplementing the decree of March 23, 2020 prescribing the organizational and operational measures of the health system necessary to deal with the COVID-19 epidemic within the framework of the state of health. health emergency).APPENDIX 4: List of organizations controlled within the framework of these systemsSI-DEP treatment:The Ministry of Solidarity and Health;Assistance Publique des Hôpitaux de Paris (AP-HP);Private biology laboratories medical;COVID CONTACT treatment:A health establishment receiving patients for consultation;A Primary Health Insurance Fund (CPAM);A regional health agency (ARS);The National Council of the Order of Physicians (CNOM);The National Council of the Order of Pharma aciens (CNOP). STOPCOVID treatment: The Ministry of Solidarity and Health; The National Institute for Research in Digital Sciences and Technologies (INRIA); Other organizations.

(1) Refers to a person tested as positive or confirmed positive by the healthcare establishment which made the diagnosis, also called the index case.(2) A description of these three devices is given in appendix 2 of this opinion.