Deliberation 2020-051 of May 8, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Thursday May 14, 2020NOR: CNIX2011646Deliberation 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 draft law extending the state of health emergencyThe National Commission for Computing and Liberties,

Seizure by the Minister for Solidarity and Health of a request for an opinion concerning a draft decree relating to the information systems mentioned in article 6 of the bill extending the state of health emergency;

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 public health code;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8;

Considering the decree n° 2019-536 of May 29, 2019 taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to the amended 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 emergency;

Having regard to deliberation no. 2020-044 of April 20, 2020 of the CNIL issuing an opinion on a draft decree 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; Having heard Mrs. Valérie PEUGEOT, commissioner, in her report, and Mrs. Nacima BELKACEM, government commissioner, in her observations, Issues the following opinion: The commission is seized under conditions of extreme urgency of a draft decree setting the terms under which the information systems provided for in article 6 of the bill extending the state of health emergency can be implemented.

.

It emphasizes that this opinion relates to a draft decree issued pursuant to a bill still under discussion in Parliament. The observations it makes are therefore only valid subject to the adoption of the law, and on the condition that it authorizes what appears in the draft decree.

According to the bill, the objective of the information systems envisaged is to allow:

- the identification of infected persons, by the organization of medical biology screening examinations and the collection of their results;

- the identification of people presenting a risk of infection, by collecting information relating to contacts of infected people and, if necessary, by carrying out health surveys, in particular in the presence of grouped cases;

- the orientation of infected people and people likely to be infected, depending on their situation, towards medical prescriptions for prophylactic isolation, as well as medical follow-up and support for these people during and after the end of these measures ;

- epidemiological surveillance at national and local levels, as well as research on the virus and the means of combating its spread. The intervention of the legislator for the implementation of the information systems envisaged is justified by the need to provide a derogation from the provisions relating to medical secrecy guaranteed by the public health code. The bill under discussion provides that this decree shall specify in particular, for each authority or body (…), the services or personnel whose interventions are necessary for the purposes (…) and the categories of data to which they have access, the duration of this access, as well as the organizations they can call on, on their behalf and under their responsibility, to ensure the processing thereof, insofar as the purpose mentioned in 2° of the same II justifies it.

The committee notes that the development of a new derogation from the principle of medical secrecy entails the sharing of very sensitive data likely to concern the entire population, thus characterizing an unprecedented situation.

To meet these purposes, the draft decree creates two personal data processing operations: Contact Covid, implemented by the National Health Insurance Fund (CNAM) and whose main purpose is to allow the conduct of health investigations , and SI-DEP (National Screening Information System), implemented by the Ministry of Health (General Directorate of Health), which will centralize the results of SARS-CoV-2 tests. The commission notes that these information systems, on the one hand, are not subject, under the terms of the decree, to automated linking and, on the other hand, are not directly linked to the draft application of StopCovid contact tracing which should, where applicable, be subject to a specific regulatory framework.

The treatments envisaged are part of the implementation of a global health strategy in the context of the covid-19 epidemic. The purposes pursued, in particular the implementation of a policy of screening and health surveys throughout the territory, appear determined, explained and legitimate, in accordance with Article 5 of Regulation (EU) 2016/679 of 27 April 2016 on the

protection of natural persons with regard to the processing of personal data (hereinafter GDPR).

The commission stresses that the invasion of privacy by this processing is only admissible if this policy constitutes the appropriate response to slow the spread of the epidemic, in particular in the context of the deconfinement of the population scheduled from 11 May 2020. If it notes that this is the case, given the state of the scientific opinions on which the Government relies, it insists, as the Council of State has already done in its opinion on the bill extending the state of health emergency, so that the need for this processing of personal data is periodically reassessed in view of the evolution of the epidemic and scientific knowledge.

The committee recalls that, whatever the emergency context, sufficient guarantees with regard to respect for the fundamental principles of the right to the protection of personal data must be provided.

Thus, beyond its opinion on this draft decree, the commission will be attentive to the conditions of implementation of this processing, in particular with regard to the planned security measures. As such, it asks to be informed of the conditions of their deployment by the CNAM and the Ministry, in particular within the framework of the realization and the evaluation of the impact analyzes relating to data protection (AIPD) which will have to, for each of the processing operations, be carried out in application of article 35 of the GDPR. The committee asks that these be sent to it in their final version as well as, where applicable, their updates.

This draft decree calls for the following observations from the commission:

As a preliminary point, the committee notes that the Government did not intend to oblige patients to reveal the identity of the persons with whom they were in contact, nor to the persons who would be contacted within the framework of a health investigation to answer to the investigator. On the other hand, the laboratories carrying out the tests will be required to enter the personal data of the people screened in the SI-DEP. In addition, at the time of ruling, the commission observes that doctors are not required to register their patients in the Contact Covid application. In any case, the refusal of doctors, patients or contact persons to participate in health surveys cannot lead to consequences of any order whatsoever (administrative, financial, care, etc.). The committee takes note of this and calls for these elements to be clarified by the time the system comes into force.

In view of the temporary nature of the information systems created by the bill, the committee recommends that they remain independent of other processing so that the end of their implementation is effective within the time limits provided for.

Regarding Contact Covid treatment:

Chapter I of the draft decree organizes the conditions for implementing Contact Covid processing. This processing is implemented by the National Health Insurance Fund, on the basis of the execution of a mission of public interest (article 6-1-e of the GDPR).

On the purposes:

According to the ministry, the purposes of Contact Covid processing, as provided for in article 1 of the draft decree, are to:

- collect the information necessary to determine the people who have been in contact with the people diagnosed as carriers of SARS-CoV-2 or presenting proven symptoms;

- contact these people to ensure their follow-up and allow them to be taken care of;

- carry out health surveys;

- ensure the information of the competent authorities to adapt the measures according to the circumstances of the contaminations (identification of an outbreak/cluster, quarantine, etc.);

- allow the management of medical biology screening examinations for contact cases requiring it;

- allow the dispensing of masks in pharmacies for contact cases requiring it;

- inform the organizations that provide social support for some of the people contacted;

- ensure the management and statistical monitoring of actions;

- allow studies, research and evaluation to be carried out on these actions. state of health emergency under discussion and comply with the provisions of Article 5-1-b of the GDPR.

In view of the extent of the processing and the sensitivity of the data that will be processed there, the commission recalls that these purposes must be understood strictly and that any use of the data that does not fall within them would be penalized.

On the categories of data collected:

Article 2 of the draft decree lists the exhaustive list of categories of personal data that may be collected; these may concern the person tested positive (known as patient 0), each person considered to be a contact at risk and the healthcare professionals or establishments concerned.

The committee notes the very high sensitivity of this data. Some are medical data and others relate to the private lives of individuals (link between patient 0 and contact cases, recent trips made, presence or passage in EPHAD, in a health

establishment or in a penitentiary establishment, profession, etc. .).

The commission recalls that the data must be relevant with regard to the purposes of the processing and recalls the principle of data minimization which must lead to the collection of only the strictly necessary data. The lists of data categories must be exhaustive and cannot exceed those provided for by law when it is enacted.

It considers that the collection of data provided for in the draft decree is relevant subject to the following reservations.

It notes firstly that certain categories of data are the subject of an imprecise description and calls on the Ministry to detail them: birth order data, data relating to the doctor at the origin of the registration in the treatment, data relating to the profession, which include in particular the quality of health professional.

In particular, the committee questions the category of data relating to the link with patient 0 which, so designated, appears particularly broad, intrusive and irrelevant. In the event that the qualification of this link is essential, the commission would like this to be expressed in the form of predefined generic categories, to be chosen from a drop-down menu. The committee invites the ministry to clarify this point.

Secondly, it emphasizes that certain data only appear relevant in the context of specific investigations linked to the follow-up of grouped cases carried out by the ARS.

Thirdly, the commission observes that personal data concerning health will be collected (result of the test and existence of symptoms). The processing of this sensitive data is based on Article 9-2-g of the GDPR (ground of important public interest) and, as such, must be proportionate to the objective pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject.

The committee considers that these data, in particular because they will be made accessible to a large number of people who are not part of the care team within the meaning of Article L. 1110-4 of the Public Health Code, must be subject to special protection.

The draft decree thus limits their collection to only data relating to the positive nature of the test or, for a hospitalized patient, to the existence of symptoms associated with a scanner. No other health data can therefore be collected within the framework of Contact Covid, in particular from the other databases implemented by the health insurance.

Fourthly, the draft decree also provides for the collection of the registration number in the national identification directory of natural persons (NIR). The commission notes that this collection is justified by reasons of identity monitoring as well as to allow

the organization and financial support without a prescription for medical biology examinations as well as the distribution of masks.

Fifthly, the commission observes that only the contact details of the people appearing in Contact Covid can come from processing already implemented by the CNAM under one of its missions, - which excludes the reuse of any other health data.

Sixthly, the commission recalls that the minimization of data collection requires, in a logic of data protection by design (privacy by design), certain functional measures in the processing settings. In particular, it calls for the exclusion of comment areas or notepad areas likely to contain irrelevant data. When a multiple choice is necessary, it must be offered by means of drop-down menus offering objective information and assessments.

Finally, in a more general way, the commission underlines that clear and uniform instructions - taking up the instructions of the health authorities - must be given to all those involved in the definition of a contact case, which will lead to the processing of data at personal character concerning him. Regular training and raising awareness of the personnel who will be called upon to intervene will therefore be essential.

On the persons who can consult, save or be recipients of the data:

Article 3 of the draft decree lists the categories of people who can access the information system or be recipients of the data contained in the Contact Covid application. The committee emphasizes that the categories provided for must ultimately correspond to those authorized by law.

With regard to the persons who can consult and save data:

The decree lists the people who can access the information systems. The supervision of access to health data is essential with regard to the requirements provided for by article 9-2-g of the GDPR mentioned above.

In this respect, the commission considers that the statement in article 3 of the draft decree that persons consult or record the data within the limits of their need to know constitutes an essential guarantee. This guarantee must in particular take the form of additional details in the decree, of access limitations configured in the information system and of its rules of use.

Firstly, the commission calls for the decree, as far as possible, to specify the purposes for which each category of user has access to the information system and the corresponding data.

It notes that the draft decree already distinguishes in particular the persons who, by reason of their position, are authorized to consult and record, on the one hand, all the data (doctors, members of the investigation teams health, ARS agents, etc.) and,

on the other hand, certain data listed exhaustively (professionals of medical biology laboratories and pharmacists). These differentiated accesses must result in access limitations.

Secondly, it will be up to the Contact Covid data controller to configure these write and read accesses according to the functions of each of the organizations or persons authorized by the decree. This authorization matrix must be a central element of processing security. The data controller must thus define functional profiles strictly limited to the needs to know for the exercise of the missions of the authorized personnel. In addition, measures must be put in place as soon as possible so that, as far as possible, authorized persons can only access the various data relating to the persons concerned when they actually need it, and in particular, for certain authorized persons, only in the presence of the persons concerned. These measures may, for example, consist of the allocation of access rights by a hierarchical superior, or by the delivery of information specific to him (confidential code, QR code, etc.) to the person concerned who must be transmitted to the authorized person so that he can unlock access to the data.

Thirdly, the committee notes that the draft decree authorizes many organizations to consult and/or record data. The Ministry indicates, with regard to the purposes pursued and the operational constraints encountered, that it does not intend to configure the system in such a way as to further limit access to the sole needs of each type of user, for example by restricting consultation to a geographic scope or certain contact cases relevant to an investigator's mission.

The committee therefore draws the attention of the organizations concerned to the need for them to have recourse to a set of additional protective measures.

These measures include informing and raising staff awareness of the rules for using the information system. Each organization whose agents (health insurance organizations, ARS, army health service, etc.) or personnel (private medical biology laboratories, pharmacists, persons placed under the authority of a doctor) will be authorized to consult or register data, must have made them aware of their obligations: protection of personal data, respect for professional secrecy and risks of criminal penalties incurred in the event of misuse of the purpose of the processing.

It would be relevant for a formal commitment to respect these principles to be obtained prior to authorisation, which should include clear and complete information on the access tracking systems put in place, allowing regular monitoring of the use of the data contained in the treatment.

It is also necessary to define a very strict authorization policy for their agents so that only those who need to know have access

to Contact Covid. The authorizations issued must be limited in time and regularly reviewed, in particular to integrate any departures of agents or changes of assignment.

Finally, the commission draws the Ministry's attention to the very strong guarantees that must surround the possible delegation of health investigation missions to other organizations, in the context of the health emergency, in particular to users outside the sphere actors trained in the access and processing of health data in view of the risks that such delegation would pose given the authentication measures provided for.

With regard to the recipients of the data:

The draft decree also lists the persons who may be recipients of certain data.

On the one hand, the draft decree authorizes the transmission of certain data, via the prefectures, to organizations that provide social support for people.

The committee notes the lack of visibility on this aspect of public action and the lack of precision of this term, which is likely to cover many bodies.

The committee considers that given the sensitivity of the information transfers envisaged and the particular health context leading a person to seek support, the list of organizations to which such data could be transmitted must be precisely defined.

The commission takes note of the ministry's commitment to specify in the draft decree the categories of recipients who could have access to the data in this context. These organizations must in any case present the guarantees required by the GDPR in terms of data processing.

Furthermore, the commission asks that the role of the prefectures consists solely of transmission to the ad hoc bodies, without creating or keeping an additional file.

Above all, the commission understands that only the data of people who have expressly requested it can be transmitted.

In any case, it is up to the National Health Insurance Fund, in its capacity as data controller, to transmit data only to organizations able to ensure the security of the data which would be transmitted.

On the other hand, the draft decree provides that competent bodies in matters of public health (National Public Health Agency, Ministry of Health [DREES], Health Data Platform [PDS], etc.) may be recipients of certain data in pseudonymised form. The committee draws the Government's attention to the fact that this transmission must comply with the law as it will be promulgated. It also notes that the precise list of data transmitted to each organization is not detailed in the draft decree and

therefore requests that it be supplemented.

With regard to the transmission of information to the CNAM and the PDS, the commission notes that it will intervene in strict compliance with the provisions of the decree of March 23, 2020 prescribing the measures for the organization and operation of the system. necessary to deal with the covid-19 epidemic in the context of the state of health emergency. Therefore, it will be necessary to ensure that the purposes of the processing that would be implemented in this context will fall within both the purposes provided for by the draft decree and those provided for by the decree. The commission also recalls that the only data that may be transmitted in this context are those listed in the decree.

On the shelf life:

The draft decree provides that the data is kept in the Contact Covid processing for a maximum period of one year from the date of publication of the law extending the state of health emergency.

While the commission does not underestimate the interest, particularly in the logic of health policy and in an evolving context of knowledge about the epidemic, of keeping the data thus collected for a period of one year, it considers that this only imperative should not guide the determination of the data retention period. It wishes that after three months of use of the Contact Covid device, the relevance of this duration will be the subject of an evaluation.

The commission also takes note of the ministry's commitment to set up a mechanism which will switch to intermediate archiving within three months after the closure of an investigation, the data no longer being useful in the context of a health survey. This data will no longer be accessible in the active database of the Contact Covid tool.

With regard to the data that would be likely to be transmitted to the CNAM and the PDS, the commission considers, in view in particular of the purposes and retention periods provided for both in the draft decree and in the decree of March 23, 2020 , that the data of Contact Covid will only be intended to integrate the national health data system (SNDS) or a permanent warehouse within the PDS, in the event that common law authorizes it. If there is no change in the legal framework applicable to the PDS and the SNDS at the end of the retention period provided for by the draft decree, all the data collected during this period must be destroyed.

The commission also specifies that the processing implemented from the data transmitted to the CNAM and the PDS cannot, apart from the completion of new formalities, be implemented beyond the state of health emergency. declared in article 4 of the law of March 23, 2020, as provided for in the decree of March 23, 2020.

On human rights:

The legal basis of the public interest on which the processing is based makes applicable all the rights provided for by the GDPR for the benefit of individuals, excluding the right to portability.

The committee notes that, beyond the voluntary nature of participation in surveys, the draft decree excludes the right of opposition, which must be analyzed as the option, provided for in Article 23 of the GDPR, to limit the rights people for, in particular, important public health objectives. Only a right of opposition for individuals regarding the transmission of their data to the PDS is provided for.

In view of the explanations provided to it, in particular on the risk of weakening the identification of contact cases and chains of contamination, the commission does not globally question this choice. However, it invites the Government to minimize the cases of exclusion from the right of opposition. In addition, it emphasizes that this reinforces the need to implement an intermediate data archiving mechanism so that, in particular, contact cases who would no longer like to see their data made accessible to investigators are quickly removed from the active database.

The committee notes that a right of opposition is also provided for the benefit of patients 0 for the disclosure of their identity to contact persons. The Ministry specified that this provision, contrary to the principle of consent to the disclosure of identity provided for in Article 2 (I-1°-I), would be deleted. The commission takes note of this and thus invites the ministry to mention the right to withdraw consent.

The commission draws the data controller's attention to the perfect information that must be given to the persons concerned with regard to the processing of their personal data, both in the case of direct collection (patient 0) and in the case of indirect collection (case contact ). As such, precise and appropriate information must be provided to the persons concerned, in a particular health context.

With regard to the right of access for individuals, the committee recalls that this must also cover traceability data in order to provide the individuals concerned with a very high level of transparency. Thus, individuals should be able to access the details of the operations carried out on their data, excluding data which could allow the identification of the authorized persons who carried out the said operations.

Finally, the committee notes that the draft decree does not provide for the implementation of automated decision-making processes (use of algorithmic processing such as those known as artificial intelligence) or profiling.

On security measures:

As a preliminary point, given the nature and volume of the data processed as well as the risks for individuals in the event of a breach of data security, the commission considers it essential that a minimum set of security measures be put in place. in order to guarantee a level of security at the state of the art in the health sector. In this respect, the committee recalls that compliance with the security obligation provided for in Article 5-1-f and Article 32 of the GDPR constitutes a condition for the lawfulness of processing and underlines the importance of technical and organizational to ensure, in particular, the confidentiality of data, the traceability of actions and their accountability. The commission therefore considers that the implementation of Contact Covid processing must in particular guarantee control of the authentication of people and the traceability of user actions.

In this respect, the committee notes that a DPIA is being carried out by the health insurance. It considers that all of the major residual risks identified to date must be dealt with before implementing the application.

Concerning the procedures for authenticating people, the commission notes that the system provided for by the draft decree authorizes authentication by identifier and password alone, which does not comply with the recommendations of the PGSSI-S and the recommendations of the commission concerning access to health data. The commission considers it preferable that all persons authorized to access the processed data use a strong authentication mechanism comprising several authentication factors.

If the implementation of such a measure were to be postponed given the implementation deadlines, the commission invites the ministry to ensure at least that the planned password policy will comply with its deliberation No. 2017- 012 of January 19, 2017 adopting a recommendation relating to passwords, as well as to carry out enhanced monitoring of processing in order to detect any abnormal use as soon as the service is opened.

Furthermore, if processing is opened up to people from other entities, the committee notes that the risks of circumvention of authentication measures would be amplified and that such an opening could only be done under authentication conditions. perfectly state of the art.

Concerning the traceability of actions, the committee notes that the decree provides for the implementation of traceability measures in order to allow any operation carried out by the authorized persons to be attributed reliably, including the operations of searching for patients or contact cases. . These traceability measures are applicable to the persons listed in

article 3 of the draft decree. Given the limitations in terms of access and authorization management, the commission considers that the traceability measures constitute one of the cornerstones of the security of the processing operations authorized by the draft decree.

Consequently, this should provide for the establishment of a mechanism for monitoring and sealing traces, for example via systems for automatically detecting abnormal connections as well as by mobilizing operational teams dedicated to the analysis of these connection traces, in order to guarantee that any illegitimate operations are not only traced but actually detected. In this regard, the commission notes that centralized supervision by an operational security center with management of security alerts is planned and considers that this supervision system should include alerts concerning the traceability of access.

Concerning the SI-DEP national screening information system:

On the purposes:

Article 7 of the draft decree specifies that the purposes of the SI-DEP information system are:

- to centralize the results of screening examinations for SARS-CoV-2 in order to make them available to the organizations responsible for determining the people who have been in contact with infected people;
- to carry out health surveys in the presence of grouped cases to break the chains of contamination;
- to guide, monitor and support the persons concerned;
- to facilitate epidemiological monitoring at national and local levels and research on the virus, as well as the means of combating its spread. article 6 (II) of the bill extending the state of health emergency and that they are determined, explicit and legitimate, in accordance with article 5-1-b of the GDPR.

In view of the extent of the processing and the sensitivity of the data that will be processed there, the commission recalls that these purposes must be understood strictly and that any use of the data that does not fall within them is penalized.

On the responsibility for processing and subcontracting:

The CNIL acknowledges that the data controller of the SI-DEP is the ministry, the AP-HP being designated as the subcontractor.

The commission recalls that an agreement must be concluded before any implementation of the processing in accordance with article 28 of the GDPR.

On data categories:

Article 8 of the draft decree provides for the collection of data concerning health and data relating to identification (in particular the NIR), the contact details and the situation of the person tested, the identification and contact details of doctors , the technical characteristics of the sample and the results of the biological analyses, including a QR-code. Data is also collected on the person of trust who will have been designated by the person undergoing a screening examination.

Among the data collected concerning the situation of the persons concerned, the commission notes information relating to persons residing in collective accommodation. It invites the Ministry to clarify this notion, in particular whether it should include, for example, places of deprivation of liberty, or even homes or reception centres.

It also questions what is covered by the terms other technical information relating to the characteristics of the sample and recommends that this information be clarified or deleted. In this sense, it takes note of the ministry's commitment not to provide for the collection of information in free text areas.

Concerning the information relating to the results of the biological analyses, the committee notes that the transmission of the analysis report is planned. Insofar as its content is not specified in the draft decree, it draws the attention of the Ministry to the fact that the transmission of this document must not have the consequence of revealing information which would not be necessary with regard to for the purposes of the processing.

With regard to the QR-code, the commission notes that if it does not contain identifying data as such, the purpose of the processing envisaged is to assign a QR-code in a unitary manner to people tested as positive. Consequently, once this allocation has been made, the QR-code cannot be considered anonymous. The commission therefore asks the ministry to remove the term anonymous from the draft decree on this point.

Finally, with regard to the data of the person of trust, the committee asks that the draft decree specify the procedures for collecting this data, by specifying the cases in which their collection would be necessary.

On the processing of the NIR, the commission notes that the draft decree provides for the possibility of this, with regard to persons and purposes not provided for by the provisions of the Public Health Code or the provisions of Decree No. 2019- 341 of April 19, 2019 relating to the implementation of processing involving the use of the registration number in the national identification directory of natural persons or requiring consultation of this directory. The commission notes that this collection is justified by reasons of identity monitoring.

Subject to these reservations, the commission considers that these categories of data are adequate, relevant and limited to

what is necessary with regard to the purposes for which they are processed, in accordance with the provisions of Article 5-1-c of the GDPR.

On the recipients of the data:

Article 9 of the draft decree provides for the persons who may access or be recipients of the data contained in the SI-DEP application.

The committee notes that the draft decree authorizes many organizations to be recipients of the data, pseudonymized or not, contained in SI-DEP, for certain specific uses.

Firstly, without calling into question the legitimacy of this access, it draws the attention of the organizations concerned to the need for them to define a very strict authorization policy for their agents so that only those who need it can access SI -DEP. The clearances issued must be regularly reviewed, in particular to incorporate any departures or changes in assignment of agents. It will be up to the Ministry of Health or, under its instructions, to its subcontractor, to configure these write and read accesses according to the functions of each of the organizations or persons authorized by the decree. This empowerment matrix must be a central element of the DPIA.

Secondly, more specifically, the commission notes in particular that it is planned that the investigators will have access to all the data mentioned in article 8 of the draft decree.

However, it considers that access by all of these persons to all of the data, for some of which a derogation from medical secrecy had to be provided by the legislator, does not appear necessary.

In this sense, by way of example, the sample number and the analysis report do not seem necessary to carry out investigations on people who have been in contact with people who tested positive for SARS-CoV-2.

It therefore draws the Ministry's attention to the need to justify, for each category of data whose processing is envisaged, the need to know of each category of recipients.

The committee considers that if it is impossible to define limited access conditions, in particular for imperative operational needs, extremely protective measures must be put in place.

Each organization whose agents (health insurance organizations, ARS, army health service, etc.) or personnel (private medical biology laboratories, pharmacists, persons placed under the authority of a doctor) will be authorized to consult or register data, must have made them aware of their obligations: protection of personal data, respect for professional secrecy,

risks of criminal penalties incurred in the event of misappropriation of processing. It would be relevant for a formal commitment to respect these principles to be obtained prior to authorisation. As such, clear and complete information must be provided to them on the access tracking systems put in place, allowing regular monitoring of the use of the data contained in the processing.

Thirdly, with regard to access to data by authorized personnel of the National Public Health Agency (ANSP), the committee notes that it is intended for two distinct purposes, requiring the transmission of data from one different granularity. Thus ANSP personnel would access, subject to authorization:

- to all the data listed in article 8 of the draft decree necessary to carry out investigations on people who have been in contact with people who tested positive for SARS-CoV-2, to monitor and support the people and carrying out health surveys, possibly including personal data;

- within the framework of its epidemiological surveillance missions, to pseudonymised data. The commission draws the attention of the ministry to the need to distinguish the authorizations.

Fourthly, the draft decree provides that competent public health bodies (National Public Health Agency, Ministry of Health [DREES], PDS, etc.) may be recipients of certain data in pseudonymised form. The committee draws the Government's attention to the fact that this transmission must comply with the law as it will be promulgated.

It also notes that the precise list of data transmitted is not detailed in the draft decree, and therefore requests that it be supplemented in order to mention the precise list of data likely to be transmitted to each organization in this context.

With regard to the transmission of information to the CNAM and the PDS, the commission notes that it will intervene in strict compliance with the provisions of the decree of March 23, 2020 prescribing the measures for the organization and operation of the system. necessary to deal with the covid-19 epidemic in the context of the state of health emergency. Therefore, it will be necessary to ensure that the purposes of the processing that would be implemented in this context will fall within both the purposes provided for by the draft decree and those provided for by the decree. The commission also recalls that the only data that may be transmitted in this context are those listed in the decree.

On information and the rights of data subjects:

The commission draws the ministry's attention to the need to provide for methods allowing the dissemination to all those concerned of clear, transparent and educational information.

In this sense, it invites the ministry to plan:

- the provision of analysis laboratories and doctors of an information document, containing all the information provided for in Article 13 of the General Data Protection Regulation, which could be given to people who do not do not have Internet access or who would like to have such a document;

- on all information media, the mention of a postal address, in addition to an e-mail address, in order to allow the persons concerned to request information on the processing and to exercise their rights by this means as well .The commission notes that the draft decree excludes the right of opposition, which must be analyzed as the implementation of the option, provided for in article 23 of the GDPR, to limit in particular the rights of persons for, in particular, important public health goals. Only a right of opposition is provided for individuals with regard to the transmission of their data to the CNAM and the PDS for processing that would be implemented for research purposes.

It invites to inform very clearly the persons concerned. It also invites the Ministry to provide for procedures allowing each person concerned to exercise their right to oppose the transmission of information to the CNAM and the health PDS as soon as the file concerning them is created in the IS. -DEP, for example by the addition of a checkbox by the personnel of the analysis laboratory.

On the shelf life:

The draft decree provides that the data is kept in the SI-DEP processing for a maximum period of one year from the date of publication of the law extending the state of health emergency.

While the commission does not underestimate the interest, particularly in the logic of health policy and in an evolving context of knowledge about the epidemic, of keeping the data thus collected for a period of one year, it notes that this period is fixed in a general manner, without distinction of the categories of data processed, the persons they concern or the purposes for which they are processed. It would like, after three months of use of the system, for the relevance of this undifferentiated duration to be assessed and for the possibility of deleting certain categories of data to be studied.

With regard to the data that would be likely to be transmitted to the CNAM and the PDS, the commission considers, in view in particular of the purposes and retention periods provided for both in the draft decree and in the decree of March 23, 2020 , that SI-DEP data will only be used to integrate the national health data system (SNDS) or a permanent warehouse within the PDS, in the event that common law authorizes it. In the absence of any modification to the legal framework applicable to the PDS

and the SNDS at the end of the retention period provided for by the draft decree, all the data collected during this period must be destroyed. The commission also specifies that the processing implemented from the data transmitted to the CNAM and the PDS cannot, apart from the completion of new formalities, be implemented beyond the state of health emergency. declared in article 4 of the law of March 23, 2020, as provided for in the decree of March 23, 2020.

On security measures:

As a preliminary point, the commission considers that given the nature and volume of the data processed and the risks for individuals in the event of a breach of data security, it seems essential that a minimum base of security measures be put in place to guarantee a state-of-the-art level of security applicable to health data. In this respect, the committee recalls that compliance with the security obligation provided for in Article 5-1-f and Article 32 of the GDPR constitutes a condition for the lawfulness of processing and underlines the importance of technical and organizational measures to ensure, in particular, the confidentiality of data, the traceability of actions and their accountability. The commission therefore considers that the implementation of SI-DEP processing should in particular guarantee control of the exchange and hosting of data, authentication of individuals and traceability of user actions.

The committee notes that a DPIA is being prepared by the ministry.

Regarding the exchange and hosting of data, the commission notes that the data transmitted by medical biology laboratories, data concentrators and external organizations will be subject to state-of-the-art encryption measures. 'art, and that the databases as well as the backups of the processing will be encrypted. It recalls that state-of-the-art cryptographic algorithms must be used and recommends that the implementation of this security measure be one of the priorities of the ministry.

Regarding the methods of authentication of users authorized to access processing, the committee takes note of the use of strong authentication using a password and a single-use code for access by certain categories of authorized persons, which it considers desirable for all persons authorized to access the data. It also notes that the patients tested can be notified of the result of their analysis by SI-DEP. It notes that the Ministry undertakes that the procedures for authenticating patients prior to access to their results will be brought into line with deliberation no. 2017-012 of 19 January 2017 adopting a recommendation relating to passwords.

Concerning the traceability of actions, the committee notes that the decree provides for the implementation of traceability measures in order to allow any operation carried out by authorized persons to be attributed reliably, including patient search

operations. These traceability measures are applicable both to the doctors or professionals mentioned in articles 8 and 9 of the draft decree and to the technical administrators. Given the absence of a mechanism for limiting the scope of access, the commission considers that the traceability measures constitute one of the cornerstones of the security of the processing authorized by the draft decree. Consequently, the latter should provide for the establishment of a trace monitoring mechanism, for example via automatic detection systems for abnormal connections and operational teams dedicated to the analysis of these connection traces, in order to guarantee that possible illegitimate transactions are not only traced, but actually detected. In this respect, the commission notes that global supervision with management of security alerts is planned, and considers that this supervision system should include alerts concerning the traceability of access.

The president,

M. L. Denis