CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Deliberation No. 2020-051 of 8 May 2020 delivering an opinion on a draft decree relating to the information systems mentioned in Article 6 of the draft law extending the state of health emergency

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

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

Following a request by the Minister of Solidarity and Health for an opinion on a draft decree concerning 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;

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

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

Having regard to the amended Order of 23 March 2020 prescribing the measures for the organisation and functioning of the health system necessary to deal with the covid-19 epidemic in the context of the state of health emergency ;

Having regard to deliberation n° 2020-044 of 20 April 2020 of the CNIL giving its opinion on a draft decree supplementing the decree of 23 March 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 ;

After hearing Ms. Valérie PEUGEOT, Commissioner, in her report, and Ms. Nacima BELKACEM, Government Commissioner, in her observations,

Adopts the following opinion:

Under conditions of extreme urgency, a draft decree setting out the terms and conditions under which the information systems provided for in Article 6 of the draft law extending the state of health emergency may be implemented has been submitted to the Commission.

It points out that this opinion concerns a draft decree issued pursuant to a bill still under discussion in Parliament. Her comments are therefore only valid subject to the passage of the Act, and on the condition that the Act authorizes what is contained in the draft Order in Council.

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

- the identification of infected persons, by organising medical biology screening tests and collecting their results ;
- the identification of persons at risk of contamination, by collecting information on contacts of infected persons and, where appropriate, by carrying out health investigations, particularly in the case of grouped cases ;
- the referral of infected persons and persons at risk of infection, depending on their situation, to prophylactic isolation medical prescriptions, as well as the medical monitoring and accompaniment of these persons during and after the end of these measures ;
- epidemiological surveillance at national and local levels, as well as research on the virus and ways of combating its spread.

The intervention of the legislator for the implementation of the envisaged information systems is justified by the need to derogate from the provisions on medical secrecy guaranteed by the Public Health Code. The bill currently 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 such access, and the bodies they may call upon, on their behalf and under their responsibility, to ensure the processing thereof, insofar as this is justified by the purpose mentioned in 2° of the same II*".

The Commission notes that the introduction of a new derogation from the principle of medical confidentiality entails the sharing of highly sensitive data which may concern the entire population, thus caracterising a new 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 enable health investigations to be conducted, and "SI-DEP" (national screening information system), implemented by the Ministry of Health (Directorate General of Health), which will centralise 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 "StopCovid" contact monitoring application project, which should, where appropriate, be subject to a specific regulatory framework.

The processing operations 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 health screening and surveys throughout the territory, appear to be determined, explicit and legitimate, in accordance with Article 5 of Regulation (EU) 2016/679 of 27 April 2016 on the protection of individuals with regard to the personal data processing (hereinafter GDPR).

The Commission stresses that the invasion of privacy by these processing operations is only admissible if this policy is the appropriate response to slow the spread of the epidemic, particularly in the context of the population lift of lockdown planned from 11 May 2020. If it notes that this is the case, given the state of the scientific opinions on which the government is relying, it insists, as the Council of State has already done in its opinion on the draft law extending the state of health emergency, that the need for such processing of personal data be periodically reassessed in the light of the evolution of the epidemic and scientific knowledge.

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

Thus, in addition to its opinion on the draft decree, the Commission will pay close attention to the conditions of implementation of this processing, particularly with regard to the security measures provided for. In this regard, it requests to be informed of the conditions of their deployment by the CNAM and the Ministry, particularly in the context of the conduct and evaluation of the impact assessments relating to data protection (AIPD) that must, for each of the processing operations, be carried out pursuant to Article 35 of the GDPR. The Commission requests that these be sent to it in their final version and, where appropriate, their updates.

The draft decree gives rise to the following observations by the Commission:

As a preliminary point, the Commission notes that the Government did not intend to oblige patients to reveal the identity of the persons with whom they had been in contact, nor did it intend to oblige persons who would be contacted in the context of a health investigation to respond to the investigator. On the other hand, the laboratories carrying out the tests will be obliged to enter the personal data of the persons screened in the SI-DEP. Furthermore, at the time it is ruling, the Commission notes that doctors are not required to register their patients in the "Contact Covid" application. In any event, the refusal of doctors, patients or "contact" persons to participate in health surveys cannot lead to consequences of any kind (administrative, financial, payment, etc.). The Commission takes note of this and calls for these elements to be clarified by the entry into force of the system.

In view of the temporary nature of the information systems created by the bill, the Commission recommends that they remain independent of other processing operations so that their implementation can be completed within the time limits laid down.

About the "Contact Covid" processing operation

Chapter I of the draft decree organises the conditions of implementation of the "Covid Contact" processing operation. This processing is implemented by the Caisse nationale de l'assurance maladie, on the basis of the execution of a mission of public interest (article 6-1-e of the GDPR).

About the purposes

According to the Ministry, the purposes of the "Contact Covid" processing, as provided for in Article 1 of the draft decree, are:

- Collect information necessary to identify persons who have been in contact with persons diagnosed as carriers of CoV-2-SARS or who have proven symptoms;
- contact these people to ensure their follow-up and allow them to be taken care of;
- conducting health surveys;
- ensure that the competent authorities are informed so that they can adapt measures according to the circumstances of the contamination (identification of an outbreak/cluster, quarantine, etc.) ;
- to allow the management of medical biology screening tests for "contact cases" requiring it;
- allow the dispensing of masks in pharmacies for contact cases requiring it;
- to inform the organisations that provide social support for some of the people contacted;
- ensure the steering and statistical monitoring of the actions;
- allow studies, research and evaluation to be carried out on these actions.

The Commission considers that the purposes and functions provided for in the draft decree are in line with those laid down in Article 6-II of the bill extending the state of health emergency currently under discussion and are in accordance with the provisions of Article 5(1)(b) of the GDPR.

In view of the scale of the processing and the sensitivity of the data to be processed, the Commission would point out that these purposes must be strictly understood and that any use of the data that does not fall within these purposes will be subject to criminal penalties.

Regarding the categories of data collected

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

The Commission notes the very high sensitivity of these data. Some are medical data and others relate to the private life of individuals (link between "patient 0" and contact cases, recent movements made, presence in or passage through EPHAD, a health establishment or a prison, profession, etc.).

The Commission recalls that the data must be relevant to the purposes of the processing operation and recalls the principle of data minimisation, which should lead to the collection of only strictly necessary data. The lists of categories of data must be exhaustive and may not exceed those provided for by the law when it is promulgated.

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

Firstly, it points out that certain categories of data are not described precisely and calls on the Ministry to provide details: "birth rank" data, "data relating to the doctor responsible for registration in the processing operation" and data relating to the profession, which include "in particular" the status of health professional.

In particular, the Commission questions the category of "data relating to the relationship with “patient 0" which, so designated, appears particularly broad, intrusive and irrelevant. Should it be essential to qualify this link, the Commission would like it to be expressed in the form of predefined generic categories, to be chosen from a drop-down menu. The Commission invites the Ministry to clarify this point.

Secondly, it stresses that certain data only seem relevant in the context of specific surveys linked to the follow-up of grouped cases carried out by the LRAs.

Thirdly, the Commission notes that personal health data will be collected (test result and existence of symptoms). The processing of these sensitive data is based on Article 9(2)(g) of the PGRD (grounds of substantial 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 Commission considers that these data, in particular because they will be made accessible to a significant number of persons not part of the health 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 data relating only to the positive nature of the test or, for a hospitalized patient, to the existence of symptoms associated with a CT scan. No other health data may therefore be collected in the context of "Contact Covid", in particular from other databases implemented by the Health Insurance.

Fourthly, the draft decree also provides for the collection of the registration number in the National Identification Register of Natural Persons (NIR). The Commission notes

that this collection is justified on identity-vigilance grounds as well as to allow the organization and financial coverage without prescription of medical biology examinations and the distribution of masks.

Fifthly, the Commission notes that only the contact details of the persons listed in 'Contact Covid' can be derived from processing operations already carried out by the CNAM under one of its missions, - which excludes the re-use of any other health data.

Sixthly, the Commission recalls that minimising data collection requires, in a logic of "privacy by design", certain functional measures in the parameterisation of the processing operation. In particular, it calls for the exclusion of "comments" or "notepad fields" which may contain irrelevant data. Where a multiple choice is necessary, it must be proposed by means of drop-down menus providing objective information and assessments.

Finally, in more general terms, the Commission stresses that clear and uniform instructions - taking up the instructions of the health authorities - must be given to all those involved as to the definition of a "contact case", which will lead to the processing of personal data relating to it. Regular training and awareness-raising of the personnel who will be called upon to intervene will therefore be essential.

On the persons who may consult, record or be recipients of the data

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

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

The decree lists the persons who can access the information systems. The supervision of access to health data is essential with regard to the requirements set out in Article 9-2-g of the GDPR recalled above.

In this respect, the Commission considers that the statement in Article 3 of the draft decree that persons consult or record data "within *the limits of their need to know*" constitutes an essential guarantee. This guarantee must be reflected in additional details in the decree, in access restrictions set up in the information system and in its rules of use.

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

It notes that the draft decree already distinguishes between persons who, because of their function, are authorised to consult and record all data (doctors, members of health survey teams, ARS agents, etc.) and certain data listed restrictively (medical biology laboratory professionals and pharmacists). These differentiated accesses must result in access limitations.

Secondly, it will be up to the "Contact Covid" data controller to set up these write and read accesses according to the functions of each of the organisations or persons authorised by the decree. This clearance matrix must be a central element of the security of the processing. The data controller must thus define functional profiles strictly limited to the need to know for the exercise of the missions of the authorised personnel. Furthermore, measures must be put in place as soon as possible to ensure that, as far as possible, authorised persons can access the various data relating to the data subjects only when they actually need them, and in particular, for certain authorised persons, only in the presence of the data subjects. These measures may for example consist of the granting of access rights by a hierarchical superior, or the provision of information specific to him/her (confidential code, QR code, etc.) to the data subject, which must be transmitted to the authorised person so that he/she can unlock access to the data.

Thirdly, the Commission notes that the draft decree authorises numerous bodies to consult and/or record data. The Ministry states, in view of 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 needs of each type of user, for example by restricting consultation to a geographical area or to certain contact cases relevant to an investigator's mission.

The Commission therefore draws the attention of the bodies concerned to the need for them to use a set of complementary protective measures.

These measures include informing staff and raising their awareness of the rules governing the use of the information system. Each organisation whose staff (health insurance organisations, ARS, army health service, etc.) or personnel (private medical biology laboratories, pharmacists, persons under the authority of a doctor) will be authorised to consult or record data, must have made them aware of their obligations: protection of personal data, respect for professional secrecy and the risk of criminal penalties in the event of misuse of the purpose of the processing operation.

It would be appropriate for a formal undertaking to comply with 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 processing operation.

It is also necessary to define a very strict authorization policy for their agents so that only those who need to know about it have access to "Contact Covid". The authorisations issued must be limited in time and regularly reviewed, in particular to take into account possible staff departures or changes of assignment.

Finally, the Commission draws the Ministry's attention to the very strong guarantees that should surround the possible delegation of health survey missions to other organisations, in the context of a health emergency, in particular to users outside the sphere of those trained in accessing and processing health data, in view of the risks that such delegation would pose in view of the authentication measures provided for.

With regard to the data recipients

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 prefectures, to organizations "that provide social support" to individuals.

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

The Commission considers that, in view of the sensitivity of the planned transfers of information and the particular health context leading a person to request accompaniment, the list of bodies to which such data could be transmitted must be precisely defined. The Commission takes note of the Ministry's undertaking to specify in the draft decree the categories of recipients who could have access to the data in this context. These bodies will in any event have to present the guarantees required by the GDPR with regard to data processing.

Furthermore, the Commission requests that the role of the prefectures should consist 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 persons who have expressly requested it may be transmitted.

In any event, it is the responsibility of the National Health Insurance Fund, in its capacity as data controller, to transmit data only to bodies capable of ensuring the security of the data transmitted.

On the other hand, the draft decree provides that competent public health bodies (National Public Health Agency, Ministry of Health (DREES), Health Data Hub (HDH), etc.) may be recipients of certain data in "pseudonymised" form. The Commission draws the Government's attention to the fact that such transmission will have to comply with the law as it will be promulgated. It also notes that the precise list of data transmitted to each body is not detailed in the draft decree and therefore requests that it be completed.

With regard to the transmission of information to the CNAM and the HDH, the Commission notes that it will act in strict compliance with the provisions of the Order of 23 March 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. Consequently, it will be necessary to ensure that the purposes of the processing operations that would be implemented in this context will be in line with the purposes set out in the draft decree as well as those set out in the order. The Commission would also point out that the only data that may be transmitted in this context are those listed in the Order.

Retention period

The draft decree stipulates that the data shall be kept in the "Contact Covid" processing operations 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 value, particularly in the light of health policy and the changing state of knowledge about the epidemic, of keeping the data collected in this way for a period of one year, it considers that this imperative alone should not guide the determination of the period for which data should be kept. It would like the relevance of this period to be evaluated after three months of use of the "Covid Contact" system.

The Commission also notes the Ministry's commitment to put in place a mechanism that will switch to intermediate archiving within three months of the closure of a survey, as the data are no longer useful for a health survey. These data will no longer be accessible in the active database of the "Contact Covid" tool.

With regard to the data that may be transmitted to the CNAM and the HDH, the Commission considers, particularly in view of the purposes and retention periods provided for in the draft decree and the Order of 23 March 2020, that the "Contact Covid" data will only be used to integrate the National Health Data System (SNDS) or a permanent warehouse within the HDH if this is authorized by ordinary law. In the absence of modification of the legal framework applicable to the rp and the SNDS at the end of the retention period provided for in the draft decree, all data collected during this period must be destroyed.

The Commission further specifies that the processing implemented on the basis of the data transmitted to the CNAM and the HDH may not, apart from carrying out new formalities, be implemented beyond the state of health emergency declared in Article 4 of the Act of 23 March 2020, as provided for in the Order of 23 March 2020.

On the rights of individuals

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

The Commission notes that, in addition to the voluntary nature of participation in investigations, the draft decree excludes the right of opposition, which must be analysed as the possibility, provided for in Article 23 of the GDPR, of limiting the rights of persons for, inter alia, important public health objectives. Only a right of opposition of individuals regarding the transmission of their data to the HDH is provided for.

In the light of the explanations it has been given, in particular on the risk of weakening the identification of contact cases and chains of contamination, the Commission does not call this choice into question overall. However, it invites the government to minimise the cases of exclusion from the right of opposition. Moreover, it emphasises that

this reinforces the need to implement a mechanism for intermediate archiving of data so that, in particular, "contact cases" that would like to no longer have their data made accessible to investigators can be rapidly removed from the active database.

The Commission notes that a right of objection is also provided for "patient 0" for the disclosure of their identity to the contact persons. The Ministry specified that this provision, which is contrary to the principle of consent to the disclosure of identity provided for in Article 2 I 1° l), 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 controller's attention to the fact that data subjects must be fully informed about the processing of their personal data, both in the case of direct collection ("patient 0") and in the case of indirect collection ("contact cases"). In this respect, precise and appropriate information must be provided to data subjects in a specific health context.

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

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

On security measures

To begin with, in view of the nature and volume of the data processed and the risks to 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 to guarantee a level of security at the state of the art in the health sector. In this connection, the Commission would point out that compliance with the security obligation laid down in Articles 5(1)(f) and 32 of the PGRD constitutes a condition for the lawfulness of the processing and stresses the importance of technical and organisational measures to ensure, in particular, the confidentiality of data, the traceability of actions and their accountability. The Commission therefore considers that the implementation of the "Contact Covid" processing operation must in particular guarantee control of the authentication of persons and the traceability of users' actions.

In this respect, the Commission notes that a SIPD is being carried out by the Sickness Insurance. It considers that all the major residual risks identified to date will have to be dealt with before the application is implemented.

With regard to the modalities for authenticating individuals, the Commission notes that the system provided for in the draft decree authorizes authentication by user ID and password alone, which is not in line with the recommendations of the PGSSI-S and

the Commission's recommendations concerning access to health data. The Commission considers it preferable that all persons authorized to access processed data should use a strong authentication mechanism with several authentication factors.

Should the implementation of such a measure be delayed due to delays in implementation, the Commission invites the Ministry to ensure at the very *least* that the planned password policy will be in line with its deliberation No. 2017-012 of 19 January 2017 adopting a recommendation on passwords, and to carry out enhanced monitoring of processing in order to detect any abnormal use as soon as the service opens.

Moreover, if the processing were to be opened up to persons from other entities, the Commission notes that the risks of circumventing authentication measures would be amplified and that such an opening could only take place under conditions of authentication that are perfectly in line with the state of the art.

With regard to the traceability of actions, the Commission notes that the Decree provides for the introduction of traceability measures in order to make it possible to reliably attribute any operation carried out by authorised persons, including operations to search for patients or contact cases. These traceability measures are applicable to the persons listed in Article 3 of the draft decree. In view of the limitations in terms of access and clearance management, the Commission considers that traceability measures are one of the cornerstones of the security of the processing operations authorised by the draft decree.

Accordingly, it should provide for the establishment of a mechanism for monitoring and sealing traces, for example by means of systems for the automatic detection of abnormal connections and the mobilisation of operational teams dedicated to the analysis of these connection traces, in order to ensure that possible illegitimate operations are not only traced but actually detected. In this respect, the Commission notes that centralised supervision by an operational security centre with management of security alerts is planned and considers that this supervision system should include alerts concerning the traceability of access.

Concerning the national screening information system "SI-DEP" (SI-DEP)

About the purposes

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

- to centralise the results of SARS-CoV-2 screening tests in order to make them available to the organisations responsible for identifying persons who have been in contact with infected persons ;

- to carry out health surveys in the presence of grouped cases in order to break the chains of contamination;

- to guide, follow and accompany the persons concerned;

- to facilitate national and local epidemiological monitoring and research on the virus, as well as on ways of combating its spread.

The Commission considers that the purposes of the draft decree are in line with those laid down in Article 6(II) of the draft law 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 scale of the processing and the sensitivity of the data to be processed, the Commission would point out that these purposes must be strictly understood and that any use of the data that does not fall within these purposes is subject to criminal penalties.

On processing responsibility and subcontracting

The CNIL notes that the controller of the SI-DEP is the Ministry, with the AP-HP being designated as the processor.

The Commission recalls that an agreement will have to be concluded prior to any implementation of the processing operation in accordance with Article 28 of the DMPR.

On data categories

Article 8 of the draft decree provides for the collection of health data and data relating to the identification (including NIR), contact details and situation of the person tested, identification and contact details of doctors, technical characteristics of the sample and results of biological analyses, including a QR-code. Data shall also be collected on the trusted person designated by the person being screened.

The Commission notes that the data collected on the situation of the data subjects include information on persons residing in "collective accommodation". It invites the Ministry to clarify this concept, particularly if it were to include, for example, places of deprivation of liberty, or hostels or reception centres.

She also wondered what was meant by the term "other technical information" relating to the characteristics of the sample and recommended that this information be clarified or deleted. In this regard, she noted the Ministry's commitment not to provide for the collection of information in free text boxes.

As regards information on the results of biological analyses, the Commission notes that the transmission of the analysis report is foreseen. Insofar as its content is not specified in the draft decree, it draws the Ministry's attention to the fact that the transmission of this document must not have the consequence of revealing information which would not be necessary in view of the purposes of the processing operation.

With regard to the QR-code, the Commission notes that although the QR-code does not contain identifying data as such, the purpose of the planned processing operation is indeed to assign a QR-code to each person tested as positive. Consequently, once this

allocation has been made, the QR-code cannot be considered anonymous. The Commission therefore asks the Ministry to delete the word "anonymous" from the draft decree on this point.

Lastly, with regard to the data of the trusted person, the Commission requests that the draft decree should specify the procedures for the collection of such data, specifying the cases in which their collection would be necessary.

With regard to the processing of NIR, the Commission notes that the draft decree provides for the possibility of processing NIRs for persons and purposes not covered by the provisions of the Public Health Code or the provisions of Decree No 2019-341 of 19 April 2019 on the implementation of processing operations involving the use of the registration number in the national identification register of natural persons or requiring consultation of that register. The Commission notes that this collection is justified on the grounds of identity surveillance.

Subject to these reservations, the Commission considers that these categories of data are adequate, relevant and limited to what is necessary for the purposes for which they are processed, in accordance with the provisions of Article 5(1)(c) of the GDMP.

About the data recipients

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

The Commission notes that the draft decree authorises many bodies to be recipients of the data, whether pseudonymised or not, contained in SI-DEP, for certain specific uses.

First of all, without questioning the legitimacy of such access, it draws the attention of the organizations concerned to the need for them to define a very strict empowerment policy for their agents so that only those who need it have access to SI-DEP. The authorizations issued must be regularly reviewed, in particular to take into account possible departures or changes in the assignment of agents. It will be up to the Ministry of Health or, under its instructions, its subcontractor, to set up 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 the AIPD.

Secondly, more specifically, the Commission notes 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 these persons to all the data, some of which have had to be exempted from medical secrecy by the legislature, does not appear necessary.

In this sense, as an example, the sample number and the analysis report do not seem necessary for the investigation of persons who have been in contact with persons who have tested positive for SARS-CoV-2.

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

The Commission considers that where it is not possible to define limited access conditions, in particular for imperative operational needs, highly protective measures must be put in place.

Each organisation whose staff (health insurance organisations, ARS, army health service, etc.) or personnel (private medical biology laboratories, pharmacists, persons under the authority of a doctor) will be authorised to consult or record data, must have made them aware of their obligations: protection of personal data, respect for professional secrecy, risk of criminal sanctions in the event of misuse of processing operations. It would be appropriate for a formal commitment to respect these principles to be obtained prior to authorisation. In this respect, clear and complete information should be provided on the access tracking systems in place, enabling regular monitoring of the use of the data contained in the processing operation.

Thirdly, as regards access to data by authorised staff of the National Public Health Agency (ANSP), the Commission notes that it is intended for two distinct purposes, requiring the transmission of data of different granularity. ANSP staff would thus have access, subject to authorisation:

- 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 have tested positive for SARS-CoV-2, to monitor and accompany people and to carry out health surveys, possibly including nominative data;

- as part of its epidemiological surveillance missions, to pseudonymised data.

The Commission draws the Ministry's attention to the need to distinguish between clearances.

Fourthly, the draft decree provides that competent public health bodies (National Public Health Agency, Ministry of Health (DREES), HDH, etc.) may be recipients of certain data in "pseudonymised" form. The Commission draws the Government's attention to the fact that such transmission will have to 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 body in this context.

With regard to the transmission of information to the CNAM and the HDH, the Commission notes that it will act in strict compliance with the provisions of the Order of 23 March 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. Consequently, it will be necessary to ensure that the purposes of the processing operations that would be implemented in this context will be in line with the purposes set out in the draft decree as well as those set out in the order. The Commission would also point out that the only data that may be transmitted in this context are those listed in the Order.

On information and the rights of data subjects

The Commission draws the Ministry's attention to the need to provide for arrangements enabling clear, transparent and educational information to be disseminated to all those concerned.

In this sense, it calls on the Ministry to provide for :

- the provision to 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 persons who do not have access to the Internet or who wish to have such a document ;

- on all information media, the indication of a postal address, in addition to an e-mail address, in order to enable data subjects to request information on the processing and to exercise their rights in this way as well.

The Commission notes that the draft decree excludes the right of opposition, which must be analysed as the implementation of the power, provided for in Article 23 of the GDPR, to limit in particular the rights of individuals for, inter alia, important public health objectives. Only the right of individuals to object to the transmission of their data to the CNAM and the HDH for processing carried out for research purposes is provided for.

It calls for this to be made very clear to those concerned. It also invites the Ministry to establish procedures enabling each person concerned to exercise his or her right to oppose the transmission of information to the CNAM and the HDH as soon as the file concerning him or her is created in the SI-DEP, for example by adding a box to be checked by the staff of the analysis laboratory.

Retention periods

The draft decree stipulates that the data are kept in 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 value, particularly in the light of health policy and in a context of changing knowledge about the epidemic, of keeping the data collected in this way for a period of one year, it notes that this period is fixed in a general way, without distinction as to the categories of data processed, the persons concerned or the purposes for which they are processed. It would like, after three months of use of the system, the relevance of this undifferentiated duration to be evaluated and the possibility of deleting certain categories of data to be studied.

With regard to the data that may be transmitted to the CNAM and the HDH, the Commission considers, in view of the purposes and storage periods provided for in the draft decree and the Order of 23 March 2020, that the SI-DEP data will only be used to integrate the National Health Data System (SNDS) or a permanent repository within the HDH if this is authorized by ordinary law. In the absence of modification of the legal framework applicable to the rp and the SNDS at the end of the retention period provided for in the draft decree, all data collected during this period will have to be destroyed. The Commission further specifies that the processing implemented on the basis of the data transmitted to the CNAM and the HDH may not, apart from the completion of new formalities, be implemented beyond the state of health emergency declared in Article 4 of the Act of 23 March 2020, as provided for in the Order of 23 March 2020.

On security measures

First of all, the Commission considers that, in view of the nature and volume of the data processed and the risks to individuals in the event of a breach of data security, it is essential that a minimum set of security measures be put in place to guarantee a state-of-the-art level of security for health data. In this connection, the Commission would point out that compliance with the security obligation laid down in Articles 5(1)(f) and 32 of the PGRD constitutes a condition for the lawfulness of processing and stresses the importance of technical and organisational 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 must in particular guarantee control of the exchange and hosting of data, the authentication of persons and the traceability of users' actions.

The Commission notes that a MIDA is being carried out by the Ministry.

With regard to the exchange and hosting of data, the Commission notes that the data transmitted by medical biology laboratories, data concentrators and external bodies will be subject to state-of-the-art encryption measures and that the databases and backups of the processing will be encrypted. She noted that state of the art cryptographic algorithms must be used and recommended that the implementation of this security measure be a departmental priority.

With regard to the modalities of authentication of users authorised to access the processing operations, the Commission takes note of the use of strong authentication using a password and a single-use code for the access of certain categories of authorised persons, which it considers desirable for all persons authorised 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 to ensure that the procedures for authenticating patients prior to access to their results are brought into line with Deliberation No. 2017-012 of 19 January 2017 adopting a recommendation on passwords.

With regard to the traceability of actions, the Commission notes that the decree provides for the introduction of traceability measures in order to make it possible to reliably attribute any operation carried out by authorised persons, including operations to

search for patients. 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. In view of the absence of a mechanism to limit the perimeter of access, the Commission considers that the traceability measures are one of the cornerstones of the security of the processing operations authorised by the draft decree. Accordingly, the draft decree should provide for the establishment of a mechanism for monitoring traces, for example *via* automatic systems for detecting abnormal connections and operational teams dedicated to analysing these connection traces, in order to ensure that any illegitimate operations are not only traced but actually detected.

In this respect, the Commission notes that overall supervision with the management of safety alerts is provided for, and considers that this supervision system should include alerts concerning the traceability of accesses.

The Chairwoman

Marie-Laure DENIS