Deliberation 2020-044 of April 20, 2020 National Commission for Computing and Liberties Nature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday February 08, 2022Deliberation n° 2020-044 of April 20, 2020 providing an opinion on a draft order supplementing the order 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 (request for opinion n° 20006669)The National Commission for Computing and Liberties,Seizure by the Minister for Solidarity and Health of a request for an opinion concerning a draft decree supplementing the decree of March 23, 2020 prescribing the measures organization and operation of the health system necessary to deal with the covid-19 epidemic in the context of the state of health emergency; Having regard to Convention No. 108 of the Council of Europe for the protection of people with respect to the t automated processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on free movement of these data, and repealing Directive 95/46/EC; Having regard to the Public Health Code, in particular its articles L. 1461-1, L. 1462-1, L. 3131-16 and L. 6113-8; Having regard Law No. 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms, in particular Article 8-I-2-e; Having regard to Law No. 2020-290 of March 23, 2020 of emergency to deal with the covid-19 epidemic, in particular its article 4; Having regard to decree n ° 2019-536 of May 29, 2019 taken for the application of law n ° 78-17 of January 6, 1978 relating to the information technology, files and freedoms; Having regard to decree no. 2020-293 of 23 March 2020 as amended prescribing the general measures necessary to deal with the covid-19 epidemic within the framework of the state of emergency nce; Having regard to the decree of December 23, 2016 as amended relating to the collection and processing of medical activity data and the corresponding billing data, produced by public or private health establishments having an activity in medicine, surgery, obstetrics and odontology, and the transmission of information resulting from this treatment under the conditions defined in Article L. 6113-8 of the Public Health Code; Having regard to the amended decree of March 23, 2020 prescribing the organizational and functioning of the health system necessary to deal with the covid-19 epidemic in the context of the state of health emergency; After having heard Mrs Valérie PEUGEOT, Commissioner, in her report, and Mrs Nacima BELKACEM, Government Commissioner , in its observations,Issues the following opinion:The Commission was seized on April 15, 2020 for an opinion, on the basis of Article 8. I.2°-e) of Law No. 1978 amended (hereinafter the Data Protection Act and Liber té), 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 within the framework of the state health emergency, taken pursuant to the provisions of Article L. 3131-16 of the Public Health Code (hereinafter the draft). Pursuant to these provisions introduced by emergency law n° 2020-290 of March 23, 2020 to deal with the covid-19 epidemic, the Minister of Health may prescribe, by reasoned decree, any regulatory measure relating to the organization and operation of the health system aimed at putting an end to the health disaster, with the exception of the measures provided for in article L. 3131-15 of the public health code, covered by a decree. The purpose of the decree is, in the context of the emergency linked to the management of the current health crisis, to organize the grouping of certain personal data, including health data, in order to allow their use with a view to monitoring and to project the evolutions of the epidemic, to prevent, diagnose and treat the pathology as well as possible and to organize the health system to fight the epidemic and mitigate its impacts. To do this, it provides for the addition in the decree of March 23, 2020 of a chapter relating to measures concerning the processing of personal data of the health system.Thus, the draft provides, on a temporary basis and within the specific framework the management of the health emergency: on the one hand, to add a weekly report to the circuit for reporting medical activity information and the corresponding billing data, produced by public or private health establishments having an activity in medicine, surgery, obstetrics and odontology, provided for in article L. 6113-8 of the public health code and by the decree of December 23, 2016 as amended (program for the medicalization of information systems or PMSI); other part, the centralization within the public interest group called Health Data Platform, provided for by Article L. 1462-1 of the Public Health Code (also called Health Data Hub) of data from different sources with a view toe making them available in order to facilitate the use of health data for the purposes of managing the health emergency and improving knowledge of COVID-19. While acknowledging the legitimacy of the objectives pursued by the project, the Commission would like to point out, in view of the urgency, that whatever the context, sufficient guarantees with regard to respect for the fundamental principles of the right to the protection of personal data personal character must be implemented. Thus, it considers that suitable legal and technical measures must be provided for in order to ensure a high level of data protection. does not in any way prejudge the analysis that it will produce in substance, both on the legal and technical levels, with regard to the long-term implementation of the Health Data Platform, in particular for the purpose of making available to data from the National Health Data System (SNDS), as well as on the implementing decree provided for in Article L. 1461-7 of the Public Health Code, which will be amended following the adoption of the law of 24 July 2019. On the creation of a data warehouse within the health data platformThe Commission notes that the centralization of data within the Health Data

Platform implies the creation of a health data warehouse with a view to of their availability to other data controllers. The processing operations related to this project are subject to Regulation (EU) No. 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the GDPR) and the relevant provisions of the Data Protection Act. The Commission takes note of the choice of the Ministry to create this treatment by means of an order issued in the context of the state of health emergency. It recalls, however, that the constitution of this database, which is part of a particular context of emergency and management of an ongoing health crisis, can only be framed by this decree for the period of state of health emergency. declared in article 4 of the law of March 23, 2020. Beyond that, this processing would no longer have a legal basis. It recalls that essential elements concerning the operation of the platform outside the context of the state of emergency health will be specified in the Conseil d'Etat decree provided for in Article L. 1461-7 of the Public Health Code and that the centralization of data within the Platform's catalog, which constitutes a data warehouse, will be subject to with prior authorization from the Commission, in application of the provisions of articles 44-3° and 66 of the Data Protection Act. On the responsibility for processing The Commission notes that the Health Data Platform and the National Health Insurance Fund (CNAM) will be jointly responsible for the processing operations described in the draft. As such, the draft mentions that the Health Data Platform is responsible for storing and making data available and that it is authorized to cross-reference data. The draft also mentions that the CNAM is responsible for pseudonymisation operations in the context of data matching and can process the registration number in the national identification register of natural persons for this purpose. The Commission notes, however, that the draft provides that the data can be processed in the technical solution of the Health Data Platform, as well as in that of the CNAM. As a result, the CNAM could also be required to store and make available data in the context of the processing envisaged. In this respect, the Commission takes note of the ministry's commitment to specify in the draft that the CNAM is: also authorized to receive the data listed,responsible for storing and making the data available,authorized to cross-reference the data,and to implement processing in response to its missions under 3° of article 65 of the IT law and freedoms. The Ministry has also undertaken to ensure that an agreement defining in a transparent manner the respective obligations of the Health Data Platform and the CNAM will be concluded, in accordance with the provisions of Article 26 of the General Data Protection Regulation. data. This agreement will specify in particular the procedures for transferring data between the Health Data Platform and the CNAM. The Commission takes note of this. On the implementation of further processing The draft provides that only the following parties may process the data thus collected by the Health Data Platform: authorized processing

managers under the conditions provided for in Articles 66 and 76 of the Data Protection Act, the State implementing the processing operations mentioned in 6° of Article 65 or the organizations and services responsible for a public service mission mentioned in Article 67. In this respect, the Commission was informed that the Ministry was planning to issue the order provided for in Article 67, in order to determine the lists of organizations and services responsible for a public service mission in connection with the health alert. It therefore recalls that 'apart from the organizations and services appearing on this list, as well as the State, for the processing provided for in Article 65-6° of the Data Protection Act, the processing implemented from data co Held in this warehouse must be the subject of a request for authorization from it, which can only intervene, with regard to research, studies and evaluations in the field of health, after the opinion of the competent committee. The compliance of this processing with the MR-004 reference methodology is in fact excluded, insofar as the persons concerned will not be informed individually either of the constitution of this warehouse, or of the subsequent processing implemented from the data that it contains. On the purposes pursued by the processing and subsequent processing The purpose of setting up the data warehouse is to allow it to be made available for carrying out subsequent processing. The Commission notes in this regard that the draft mentions that the data contained in this warehouse may only be processed for projects pursuing a purpose of public interest in connection with the current COVID-19 epidemic. The Commission takes note of this that this purpose, which is very general, will be interpreted with regard to the purposes for setting up the warehouse indicated in Article 1 and the recitals of the project, which specify in particular that the ability to mobilize health data is an essential axis of the fight against the covid-19 epidemic and that it is necessary to continue and anticipate the evolutions of the epidemic, prevent, diagnose and treat the pathology as well as possible and adapt the organization of our health system to fight the epidemic and mitigate its impacts. It also notes that the draft decree does not, except by mentioning its legal basis, refer either to the urgency attached to the production of the results of the analyzes carried out in the context of this processing, or to the duration of their implementation. As this is a temporary solution deployed specifically to deal with the -COVID19 epidemic in the context of the state of health emergency, the Commission takes note of the ministry's commitment to specify in the decree that the processing implemented from the data of the warehouse is not intended to be part of the duration and cannot, apart from the completion of new formalities, be implemented beyond the state health emergency declared in article 4 of the law of March 23, 2020. On the data whose processing is envisagedThe draft lists the categories of data likely to be transmitted to the Health Data Platform with a view to their made available. The Commission notes, beyond the very generic nature of the categories

described, that there is no mention of the historical depth of the data, nor of their exact nature, in particular with regard to the interest that may present their analysis in the context of the COVI epidemic D-19. By way of example, the project mentions, without further detail, the possible reporting of data from the SNDS or pharmacy data. It recalls that in application of the principle of data minimization provided for in Article 5-1-c of the GDPR, the data must be adequate, relevant and limited to what is necessary in view of the purpose pursued, both in terms of data contained in the warehouse within the Health Data Platform, and data made available for subsequent processing. In this respect, the Commission takes note of the Ministry's commitment to complete the project so that it clearly specifies that the Health Data Platform and the CNAM can only, within the framework of the decree examined, collect the data necessary for the performance of the processing operations implemented within the framework of the projects pursuing a purpose of interest public in connection with the current COVID-19 outbreak. It recalls that the decree must not allow systematic and exhaustive feedback of all the data listed in the draft, independently of the needs of these projects. warehouse thus constituted, that it must first have been created and implemented in accordance with the provisions of the GDPR and the Data Protection Act, in particular with regard to the formalities provided for by the latter where applicable. Finally, it notes that the draft provides that the technical solutions for making data available may not contain either the surnames and first names of persons, nor their registration number in the identification directory of natural persons (NIR), nor their address. On the retention period of data The draft does not mention a precise retention period for the data contained in the warehouse. However, since the project falls within the framework of the state of health emergency declared in Article 4 of the law of March 23, 2020, the Commission deduces from this that the data should only be kept in it for the duration of the state of health emergency. With regard to these data, the ministry specified that those whose conservation will be provided for by the decree mentioned in article L. 1461-7 of the public health code, as well as by the decree which will specify the databases appearing in the catalog of the Data Platform, will be kept in application of the rules of common law, while the other categories of data will be destroyed. The Commission takes note of this. However, it considers that in the event that the adoption of the common law legal framework applicable to the health data platform could not have been finalized at the end of the state of health emergency, all of the data collected during this period must be destroyed. On the procedures for informing individuals and exercising their rights The Commission notes that apart from the constitution, within the Health Data Platform, of a public directory listing the list and characteristics of all the projects relating to data from the warehouse, the project does not provide for any particular method of information or exercise of rights with regard to the constitution of the

warehouse or the processing carried out subsequently. However, the Commission points out that the persons concerned must be informed, with regard to the processing of data aimed at setting up the repository, then of each research project carried out using the data it contains, of under the conditions provided for in Article 14 of the GDPR. In this respect, pursuant to the provisions of Article 14-5-b) of the GDPR, the obligation to provide individual information to the data subject may be subject to exceptions in the event that the provision of a such information would prove impossible, would require disproportionate efforts or would seriously compromise the achievement of the objectives of the processing. In such cases, it is up to the data controller to take appropriate measures to protect the rights and freedoms, as well as the legitimate interests of the data subjects, including by making the information publicly available. It therefore requests, taking into account the context current health crisis does not allow individual information to be given to all the persons concerned, that appropriate measures are taken and that information relating to the processing of data aimed at setting up the warehouse and each project of research carried out from the data it contains is made public, in particular by including in the public directory mentioned in the project, all the information provided for in Article 14 of the GDPR. It recalls in particular that this information must detail the procedures for exercising the rights of data subjects and that data controllers must provide for the measures necessary to comply with these requests.On transfers of data to third countries and disclosures not authorized by EU lawThe Commission notes that the contracts provided to it do not themselves provide for the location of the data or all the guarantees relating to the methods of access to the data by the administrators of the host. However, the contract allows the Platform, through the Online Services Conditions, to choose the place where the data is hosted. In addition, the information provided by the Health Data Platform explicitly mentions the use of a certified health data host. In this regard, the Commission takes note of the Ministry's commitment that the Health Data Platform will require its host to host data at rest within the European Union. However, the Commission stresses that this location only applies to data at rest, even though the contract mentions the existence of data transfers outside the European Union as part of the day-to-day operation of the platform, in particular for maintenance or incident resolution. In this respect, the contractual outsourcing provisions concluded between the Health Data Platform and the service provider responsible for hosting the data, stipulate that the data processed may be transferred to the United States for be stored and processed there, as well as in any other country in which the processor or its subsequent processors are located. These transfers are subject to a framework in accordance with Chapter V of the GDPR, being governed in this case by standard contractual clauses, in accordance with Article 46-2-c of this regulation. The Commission recalls, in this context ,

the concerns repeatedly raised by the European Data Protection Board (EDPB) regarding access by United States authorities to data transferred to the United States, more specifically the collection and access to personal data national security purposes pursuant to Section 702 of the US FISA Act and Executive Order 12333. These issues are currently before the Court of Justice of the European Union in a request for preliminary ruling from the High Court of Ireland concerning the validity of Decision 2010/87/EU, by which the European Commission established standard contractual clauses for certain categories of transfers. A judgment of the Court in this case (C□311/18) is expected in the coming months. transfers and disclosures not authorized by Union law. Any request for access from a court or administrative authority of a third country, addressed to the processor, outside an applicable international agreement or, according to the interpretation of the EDPS, the application of a derogation relating to the vital interest of the data subject, could therefore not be considered lawful. to the subcontractor in France, unless prohibited by law, which can only be based on Union or national law. In view of this context and the sensitivity of the data whose processing is envisaged, for which higher protection must be ensured, as well as possible material and legal risks in terms of direct access by the authorities of third countries, the Commission calls for particular vigilance to be given, in the implementation implementation of the decree, the conditions of storage and the procedures for accessing the data, and recommends that the Health Data Platform provide hosting and processing of the data on the territory of the European Union. In the longer term, it takes note of the fact that it has been told that the warehouse to be set up within the Health Data Platform is not linked to the services of a single provider and would like, given the sensitivity of the data in question, that its hosting and the services related to its management may be reserved for entities coming exclusively under the jurisdictions of the European Union. effective implementation of the technical solution for the storage and provision of data from the Health Data Platform, as well as the constitution of its data catalog, were initially to take place only after the entry into force of a framework precise legal framework accompanied by the implementation of an action plan as a whole. Indeed, the Commission notes that the technical solution was the subject of an overall analysis of the risks and impacts on privacy, followed by approval on 16 December 2019 according to the SNDS security reference system, with a plan action plan for the implementation of security measures spread over a period of several months. It also notes that the approval of project spaces by project processing managers could be subject to a derogatory procedure in the context of the health crisis. The Commission therefore wonders about the conditions for the early start of the technical solution in a context where the Health Data Platform had to carry out operations in a few weeks, some of which were structuring, to guarantee the security of the data processed were planned for s spread over

several months. The Commission therefore stresses that the Health Data Platform will have to ensure that this early implementation does not create any additional risk for the persons concerned. Furthermore, the Commission recalls the importance of the establishment of centralized governance of the IT security of the technical solution, which must be ensured with a sufficient level of independence vis-à-vis the management of the Health Data Platform. It notes that this requirement does not currently seem to be met, while the context of the urgent implementation of the technical solution makes this requirement all the more relevant. Although the current situation is only transitory, the Commission calls on the Health Data Platform to put in place as soon as possible a dedicated and independent governance responsible for security. The Commission also notes that the Health Data Platform carried out an impact analysis relating to data protection devoted to the technical solution in its version dedicated to projects related to COVID-19, as well as an updated analysis of compliance with the SNDS security reference system. It notes that this analysis makes it possible to correctly understand all the measures put in place by the Health Data Platform in its approach to compliance with the principles of the protection of personal data, and underlines that this analysis was carried out in accordance with the principles of the GDPR. Concerning the transmission of data from data producers to the Platform, the Commission notes that the procedure which will be applied has been the subject of discussions with the National Information Systems Security Agency. The data will be encrypted with encryption keys renewed with each exchange and transmitted through a secure channel set up on the initiative of the project operators, ensuring in particular the authentication of the source and the recipient and the encryption of the flow. Given the diversity of possible sources, case-by-case discussions on transfer modalities are also envisaged. The Commission recalls that while the operational transfer methods can indeed be adapted to specific cases, this should in no way weaken the level of data security. In this respect, a data transfer agreement must be signed between the Platform health data and each data provider in order to regulate the transmission of information, specifying in particular the frequency of updates and the security conditions of the transfer. The Commission notes that the Health Data Platform will only receive data previously pseudonymized by the data producers, according to the terms also specified in the data transfer agreement. Following discussions with the Ministry, the Commission was told that in the particular case of a deterministic matching by of the NIR of the persons concerned, via the CNAM circuit, a pseudonym obtained from an irreversible cryptographic function ble applied to the NIR is also provided to the Health Data Platform. However, the Commission notes that these pseudonymization methods do not seem to be detailed in the impact assessment relating to data protection and that the consequences in terms of the risk of re-identification for

individuals do not seem clearly established at this stage. . It also notes that the draft decree does not provide for the transmission of the NIR to the Health Data Platform. Given the context of the referral and the information transmitted, the Commission is unable to fully understand the consequences of using such a pseudonym and cannot comment on this point. After receipt of the data, the pseudonyms used for the transmission will be replaced by random pseudonyms in the operator space of the technical solution. The Commission notes that a correspondence table between the initial pseudonyms and those generated by the Platform will be kept. The Commission notes that this correspondence table will be kept in an isolated sub-part of the operator space, that it will be encrypted with a dedicated key and whose use will require the joint action of two employees of the Data Platform healthcare with distinct roles. In order to further improve the level of security and insofar as access to these keys does not seem necessary in the context of the day-to-day operation of the projects, the Commission recommends that these keys be stored in a separate database managed by the health data itself or by another subcontractor. When the data is made available within the project spaces, new pseudonyms will be generated, thus ensuring the use of different identifiers within each project for the same individual. However, the Commission is wondering about the practical pseudonymisation methods implemented by the Health Data Platform for this provision, in particular in the event of data updates within these project spaces. It therefore draws the Ministry's attention to the need to provide data pseudonymization methods specifying, where applicable, the choice of the irreversible cryptographic operation used as well as the procedure for managing the associated secrets or even the reinforced security applied in consequence to the correspondence table. The Commission takes note that all data exchanges taking place during the use of the project spaces of the technical solution will be carried out via encrypted communication channels and ensuring the authentication of the source and recipient. The Commission also notes that the stored data will be encrypted with state-of-the-art algorithms from keys generated by Platform managers on an encryption box controlled by the Data Platform health. The Commission notes, however, that in order to benefit from all the capabilities of the host's technical solution, these passwords should be entrusted to him. They will be kept by the host in an encrypted box, which has the effect of technically allowing the latter to access the data. The Commission notes that technical measures have been put in place to control the access of administrators subcontractors in charge of the technical solution. A functionality of prior authorization of administrator access is activated according to the impact analysis relating to data protection carried out. However, the Commission notes that this functionality does not seem to be mentioned in the contracts provided. In addition, the Commission questions the effectiveness of this measure, which does not seem to cover

all possible accesses. The Commission notes that the draft provides that data can only be processed in the technical solutions of the Data Platform of health and the CNAM, and cannot be extracted from them. The automatic export functionalities will not be usable by entities accessing data in project spaces. However, the Commission questions the effectiveness of the blocking of any possibility of export. The documents in the file indicate that the procedures for systematic audits of exports by data operators are maintained, as well as the obligation for users to undertake not to export personal data and to put in place traceability mechanisms for export operations. Consequently, the Commission calls on the Ministry to explicitly indicate that all data export functionalities will be completely deactivated and inaccessible to users, either by indicating that the personal data hosted on the platform cannot be exported , that only data that has undergone an anonymization procedure in the rules of the art can be exported and that these exports will be previously and systematically audited in order to ensure the anonymous nature of the exported data. The Commission recalls that only anonymous data can be exported outside an approved environment in accordance with the decree of 22 March 2017 relating to the security reference system applicable to the SNDS. The Ministry has undertaken to ensure that the Data Platform de santé has at its disposal a register including in particular all the projects implemented and detailing all the accesses open for and by the project processing managers. The Commission takes note of it. the responsibility of the technical director. On the weekly PMSIL data feedback circuit, article 1-II of the project provides that, without prejudice to the circuit provided for by the decree of December 23, 2016 as amended, the health establishments mentioned in article 1 of the same decree transmit, according to on a weekly basis, the anonymous files mentioned in I of article 5 of the same order directly to the Technical Agency for Information on Hospitalization (ATIH). This data will then be transmitted without delay to the CNAM in order to feed the SNDS. The Commission notes, however, that the draft does not specify, unlike the referral letter accompanying it, that this feedback of information vocation, in the context of the strong mobilization of the establishments, to have them carry out exhaustive reports of activity on a weekly basis but to open a weekly report allowing priority integration of activity linked to the epidemic. It therefore requests that this detail be added to the draft. The Commission nevertheless takes note of the ministry's commitment to mention in the draft that the data reported in this context cannot be used for the purposes for which they are usually collected, detailed in Article L. 6113-8 of the Public Health Code, except with regard to health surveillance and vigilance. considered as anonymous within the meaning of the GDPR, as clarified by the opinion of the G29 n° 05/2014 of April 10, 2014 relating to the techniques of anonymization. It takes note of the commitment of the ministry to modify the project on this point , so that reference is no longer made to anonymous

data. Any processing of this data must therefore take place in compliance with the provisions of the GDPR and the Data Protection Act, with regard to data containing personal cter.The other provisions of the draft do not call for any comments from the Commission.The PresidentMarie-Laure DENIS