Deliberation 2021-152 of December 16, 2021 National Commission for Computing and Liberties Nature of the deliberation: Authorization Legal status: In force Date of publication on Légifrance: Saturday February 26, 2022 Deliberation n° 2021-152 of December 16, 2021 authorizing the French Society of Cardiology to implement automated processing of personal data for the purpose of setting up a health data warehouse, called "Cardiohub" (authorization request no. 2222005)The National Commission for Computing and Liberties, Seizure by the French Cardiology Society of a request for authorization concerning the automated processing of personal data for the purpose of setting up a health data warehouse called Cardiohub; Having regard to Regulation (EU) 2016/679 of the Parliament European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and t to the free movement of such data, and repealing directive 95/46/EC (RGPD); Having regard to law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms liberties), in particular its articles 44-3° and 66-III; After having heard the report of Mrs Valérie PEUGEOT, commissioner, and the observations of Mr Benjamin TOUZANNE, commissioner of the Government, Makes the following observations: On the data controller :The French Society of Cardiology (SFC) is a learned society created in 1937 and governed by the law of July 1, 1901. It is mobilized to advance research against cardiovascular diseases.As part of the constitution of the Cardiohub warehouse , the SFC defines the lines of research, selects the projects proposed within it and ensures the financing of the warehouse. On the person in charge of the implementation: The company Clinityx is in particular in charge of the technical implementation of the warehouse and management ion of data after collection; it acts as a subcontractor of the SFC. On the purpose of the processing, its lawfulness and the conditions for processing data concerning health: The SFC wishes to set up a health data warehouse in order to carry out research on pathologies This warehouse will be fed by personal data from: the Mitragister register; the National Health Data System (SNDS) for people included in the Mitragister register. The Commission considers that the purpose of the processing is determined, explicit and legitimate, in accordance with the provisions of Article 5-1-b) of the General Data Protection Regulation (GDPR). The processing implemented by the SFC is necessary for the performance of the public interest mission entrusted to it. This processing is, as such, lawful under Article 6-1-e) of the GDPR and fulfills a condition allowing the processing of data concerning health under Article 9-2-i) of the GDPR. The establishment of this database requires matching between data from the historical SNDS and data from the Mitragister register. This database is similar to a data warehouse, subject to the provisions of articles 44-3° and 66-III of the amended law of 6 January 1978, which provide for authorization for processing involving data relating to health

and justified, as in this case, by the public interest. The data contained in this warehouse cannot, in accordance with the principle of the prohibited purposes of use of the national health data system (SNDS), be used for promotional purposes health products to health professionals or health establishments, or for the purpose of excluding guarantees from insurance contracts and modifying contributions or insurance premiums for an individual or a group of individuals presenting the same risk. Similarly, the Commission recalls the prohibition on compiling and using, for prospecting or commercial promotion purposes, files composed from data resulting directly or indirectly from medical prescriptions, since these files make it possible to identify directly or indirectly the prescriber (article L.4113-7 of the public health code). The Commission recalls that future uses of the data contained in this warehouse will fall within the framework of the provisions of Articles 66 and 72 and following of the Data Protection Act, which require that each research project, study or evaluation be justified by the public interest and will have to be the subject of specific formalities. On the governance of the warehouse: The SFC has set up a governance system for the Cardiohub warehouse consisting of: a registry commission, in charge of: proposal of strategic orientations, determination of the scope of the relevant data, of the Mitragister scientific committee in charge of: the determination of its specific orientations, the development of the electronic form of data to be collected, the reassessment of the relevance of the data collected, the validation of research projects aimed at reusing data based on their originality, their feasibility, their scientific relevance and strategic, the validity of the methodology with regard to the defined objectives, ethics and the character of public interest. The committee verifies the impossibility of targeting patients or prescribers with regard to the statistical analysis plan submitted, advises researchers and project leaders in order to promote collaboration between experts, Mitragister's operational steering committee, in charge of management of data collection from the centers and communication with them. The Commission strongly recommends that these governance committees be made up of members who are qualified in terms of SNDS data processing. On the nature of the data processed: The data from Mitragister are clinical hospitalization data collected for two years from the hospitalization of the person concerned: administrative identification data: surname and first name, telephone number, postal contact details, electronic contact details. health data: inclusion criteria demographic data: date of birth, gender, weight, height, lifestyle data (single, i solé, professional activities), medical history and cardiac risk factors, clinical characteristics of the heart disease studied, reports of cardiac imaging examinations, reports of additional examinations, quality of life data, biological examination data , treatment data, hospital follow-up data, follow-up data (reports of additional examinations), discharge data. Data from the Mitragister register will be matched with data from the SNDS covering the two

years preceding the person concerned and up to ten years after he or she is taken in charge and coming from: the national health insurance inter-scheme information system (SNIIRAM) with regard in particular to consultations with general practitioners, cardiologists and medical treatments; Program for the medicalization of information systems (PMSI) with regard to events, hospitalizations and re-interventions during the follow-up of the Center d'ép idemiology on the medical causes of death (CépiDC) with regard to the vital status of participants. passive monitoring of data subjects. The administrative identification data collected for monitoring and matching purposes are kept in a compartmentalised manner and kept by a separate trusted third party. The Commission considers that the data whose processing is envisaged is adequate, relevant and limited to what is necessary with regard to the purposes of the processing, in accordance with the provisions of Article 5-1-c of the GDPR. On the data circuit collected in Cardiohub: When a person is included in the Mitragister register, a cohort number is generated individually. Investigating doctors (cardiologists) complete a structured electronic form (eCRF) in order to indicate the data relating to the hospitalization of the person concerned. In order to allow the collection of specific data, such as ultrasound images, a follow-up of the persons concerned is carried out by authorized persons within the SFC or by the investigating doctor, subject to professional secrecy and made aware of the confidentiality of data. collected. Authorized persons collect the information transmitted in electronic forms. On the matching of data from Mitragister and the SNDS in the context of Cardiohub: Prior to the request to extract data from the SNDS addressed to the National Health Insurance Fund (CNAM), the SFC randomly generates a specific project identifier (ISP). The matching is indirect: Clinityx produces a matching file containing the variables common to Mitragister and the SNDS as well as the ISP and sends it securely to the CNAM. The Commission takes note of this. On the retention period of the data: The health data of patients from the various sources will be kept in an active database for a period of fifteen years from the inclusion of the person concerned in Mitragister. The data administrative identification will be kept for a period of ten years from the inclusion of the persons concerned in Mitragister. Beyond that, the data will be anonymized or deleted. In this respect, the Commission notes that this operation will be automated. The Commission considers that these data retention periods do not exceed the periods necessary for the purposes for which they are collected and processed, in accordance with the provisions of article 5-1-e) of the GDPR. On the recipients of Cardiohub data: Academic research organizations, health authorities, manufacturers of medical devices, patient associations may, after the agreement of the committees of governance of the Cardiohub warehouse and the completion of the prior formalities provided for by the Data Protection Act, to be recipients of data from the warehouse in order to carry out

research projects. On the information of persons: The persons concerned will be individually informed of the processing of data concerning them within the framework of the Cardiohub warehouse by post, electronic or telephone means. Persons already included es in Mitragister before the implementation of Cardiohub will be informed of the progress of the treatment by the CFS during their follow-up at six months, one or two years. A transparency portal on which the information note relating to the constitution of the warehouse, as well as the various information notes relating to future research carried out on the warehouse, will be available on the SFC website. The SFC will have to communicate to the establishments including people in Mitragister the information notices so that they make them available on their own website. The Commission notes that the SFC undertakes to publish on its website the type of data available within its repository as well as a summary of the research carried out on this data. For transparency purposes, the summary and results of each research, study or evaluation project carried out on the data in the warehouse will be published on the SFC's transparency portal. Article L. 1461- 3 of the CSP makes access to data from the SNDS and its components subject to the communication to the Health Data Platform (PDS) of several elements by the data controllers, before and after the studies. Research, study or evaluation projects carried out using data from the Cardiohub warehouse must be registered in the public directory of the PDS. The Commission is asking for the warehouse to also be included in the public directory of the Health Data Platform. Finally, the Commission is asking for a report to be sent to it every three years on the operation of the warehouse and on the research carried out from the data it contains. The Commission considers that these methods comply with the principle of transparency and the information requirements provided for in Articles 12 and following of the GDPR. On the rights of the persons concerned: The rights are exercised with the delegate at the data protection of the SFC. In the event of exercise of the right of opposition, the data of the person concerned will no longer be used for research purposes within the framework of Cardiohub. In this case, the SNDS data relating to the person who objected will not be collected. The Commission considers that the procedures for exercising the rights of data subjects do not call for further comment. data and traceability of actions: The technical infrastructure of the person responsible for implementing Cardiohub, used for hosting child systems of the SNDS, has been analyzed by the Commission on various occasions. in support of the authorization request, an impact analysis relating to data protection specific to the creation of the Cardiohub warehouse, as well as a risk analysis on the security of information systems. An approval of the secure bubble was also carried out by the approval authority on April 21, 2021, in accordance with the decree of March 22, 2017 relating to the security reference system applicable to the National Health Data System. This registration

decision is only valid until December 31, 2022, subject to the implementation of the action plan that the registration authority has defined. It must therefore be renewed before the expiry of this period, if the processing is still implemented. within their technical solution. Separate environments based on software containerization solutions are implemented in particular to prevent any data merger. Health data will be encrypted at rest by state-of-the-art algorithms within a certified host for the hosting of health data, located in France, and exclusively subject to the laws and jurisdictions of the European Union. This data will also be encrypted in transit. Backups will be encrypted at rest. Separate project spaces from each other and from the warehouse itself, will be set up through the use of software containerization solutions and encrypted file systems for the data of each study. Unique pseudonymous numbers specific to each project space, based on a cryptographically secure pseudo-random number generator, will also be implemented in order to reduce the risks of re-identification of the persons concerned. At the end of the study, the dedicated project space will be closed and the data will be deleted. Administrative data will be physically partitioned from health data through the use of a separate trusted third-party host, certified for hosting health data, located in France and exclusively subject to the laws and jurisdictions of the European Union. This administrative data will be encrypted at rest and will use similar partitioning mechanisms to those implemented for health data. The administrative identification data will pass through state-of-the-art protocols and algorithms on a dedicated virtual local area network at the main host in order to carry out security checks and the generation of the ISP before being forwarded to the separate host. No administrative identification data will be stored at the main host. The export of data outside Cardiohub will consist exclusively of statistical reports which may contain one or more models that do not allow any re-identification of persons and transmitted exclusively to data controllers. for carrying out further research. To this end, a minimum threshold of eleven individuals will be retained for each aggregation. The Commission nevertheless recalls that the data controller must carry out an analysis to demonstrate that its anonymization processes comply with the three criteria defined by Opinion No. 05/2014 on anonymization techniques adopted by the group in Article 29 (G29) on April 10, 2014. Otherwise, if these three criteria cannot be met, a study of the risks of re-identification must be carried out. Data entry will be carried out using an application located within Cardiohub. Multi-factor authentication including a password in accordance with deliberation no. 2017-012 of January 19, 2017 adopting a recommendation on passwords, or any other subsequent update of this recommendation, is required to access it. . Cardiohub data and administration access for both hosts relies on the use of separate state-of-the-art encrypted virtual private networks as well as similar multi-factor authentication mechanisms. Administration bastions allow connections to be traced. Finally, the

Commission notes that the technical and functional traces will be kept for a period consistent with its recommendations and backed by a proactive mechanism for regular monitoring. The security measures described meet the requirements provided for by Articles 5.1, f) and 32 of the General Data Protection Regulation taking into account the risks identified by the data controller. It will be up to the latter to carry out a regular reassessment of the risks for the persons concerned and an update update, where applicable, of these security measures. Under these conditions, the Commission authorizes the French Society of Cardiology to implement the processing of personal data for the purpose of setting up a health data warehouse called Cardiohub for a period of ten years.The PresidentMarie-Laure DENIS