DELIBERATION n°2019-124 of 10 OCTOBER 2019National Commission for Computing and LibertiesNature of the deliberation: AuthorizationLegal status: In force Date of publication on Légifrance: Tuesday 05 November 2019Deliberation n° 2019-124 of 10 October 2019 authorizing the Hospital Center Grenoble Alpes University to implement personal data processing for the purpose of a health data warehouse called "CHUGA-EDS" (Request for authorization no. 2210263)The National Commission for Computing and Liberties,Saisie by the Grenoble Alpes University Hospital Center for an authorization request concerning a health data warehouse called "CHUGA-EDS"; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to 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 natural persons at with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); Having regard to the Public Health Code; Having regard to Law no. ° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its articles 44-3° and 66-III; Considering the decree n ° 2019-536 of May 29, 2019 taken for the application of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Considering the file and its supplements, and in particular the impact analysis relating to data protection; On the proposal of Mrs Valérie Peugeot, commissioner, and after having heard the observations of Mrs Nacima BELKACEM, government commissioner, Makes the following observations: On the data controller The Grenoble Alpes University Hospital Center (CHUGA) On the purpose and legal basis of the processing The CHUGA wants to build a data warehouse of called CHUGA-EDS. This warehouse will group the data produced during the care of patients by the CHUGA for the purposes of: research in the field of health carried out by the professionals of the CHUGA and its external partners; improvement of the management of patients in the establishment; the management of the establishment. The file specifies that, like the National Health Data System (SNDS), the data from the CHUGA-EDS will not be used for purposes of promoting health products for 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. The Commission takes note of this. The Commission notes that specific governance is planned for the warehouse. A project steering committee, assisted by a scientific committee and an ethics and professional conduct committee, is in charge of examining requests for access to data from the warehouse. The Commission acknowledges that the ethics and professional conduct committee will notably include at least one outside personality involved in health ethics. The legal basis for the

processing is the exercise of a task in the public interest, within the meaning of Article 6-1-e of the European Data Protection Regulation (hereinafter GDPR). 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 GDPR. It considers that the provisions of Article 44-3 should be applied. ° and 66-III of the amended law of 6 January 1978, which require authorization for processing involving data relating to health and justified, as in this case, by the public interest. The Commission recalls that the processing of data of a personal nature which will be implemented, for the purposes of research in the field of health, from the data contained in the warehouse are separate processing operations which must be the subject of specific formalities under Articles 72 et seq. of the Data Protection Act. On the data processed The warehouse will group the data produced in the context of the care of patients by the CHUGA. These are care data, administrative data and data generated by the operation of the CHUGA. More specifically, with regard to patients, the following data is collected: identification data (surname, first name, address, date and place of birth, internal patient identifier, sex, nationality, contact details [telephone number, email], mutual affiliation and/or private insurance); data relating to the family, professional situation, lifestyle, assessments of the social difficulties of people, sexual life; health data (including biological, physiological and pathological information likely to influence the patient's reaction to his medical care) and genetic data linked to biological samples ; data relating to vital status (date of death, medical cause of death if the person died at the CHUGA); medico-administrative data from the PMSI. of the CHUGA, the following data is collected: identification data: surname, first name, RPPS number, Adeli code, personnel number, sex, year of birth, telephone number, e-mail, job/profession, assignment history services. Finally, there are data from the operation of the CHUGA (such as sterilization or catering data, for example). The Commission considers that the data whose processing is envisaged are 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 recipientsThe members of the The care team, as defined by the provisions of Article L. 1110-12 of the Public Health Code, will have access to all the data contained in the warehouse concerning the patients they care for. The professionals who are members of the Department of Medical Information (DIM) will have access to the data as part of their missions. External partners (such as health establishments, research institutes, universities and industrialists) not belonging to the team care providers will have access to data from the warehouse, within the limits of strictly necessary and relevant data with regard to the objectives of the research project, their functions and the mandate given by the sponsor. The Commission recalls that this access must be carried out with strict respect for the confidentiality of the data.

admitted prior to the constitution of the warehouse: The Commission notes that given the number of people concerned (1,500,000), the age of part of the data (the CHUGA indicates in its file that it has 1% of email addresses and 39% of valid mobile phone numbers) and the financial cost that information by post would represent, the CHUGA considers that individually informing all the persons concerned would require a disproportionate effort. Pursuant to Article 14-5-b of the GDPR and the first paragraph of Article 69 of the Data Protection Act, the obligation to provide individual information to the data subject may be subject to exceptions in the event that the provision of such information proves impossible, would require disproportionate efforts or would seriously compromise the achievement of the objectives of the processing. In such cases, in accordance with the GDPR, the controller takes appropriate measures to protect the rights and freedoms, as well as the legitimate interests of the data subject, including by making the information publicly available. In the present case, the Commission notes that an exception will be made to the principle of individual information for persons with regard to patients whose data has been collected prior to this authorization and that appropriate measures will be implemented for patients for which the CHUGA does not have reliable contact details, in particular by means of the distribution on its website and in the waiting rooms of the establishment of collective information relating to the warehouse. This collective information will also be relayed via social networks, regional media and press releases and during public events taking place at the CHUGA. As regards patients admitted after the establishment of the warehouse: The Commission notes that they will be informed individually as follows depending on the patient's treatment method: by handing over the circulation sheet distributed to all patients who come for consultation at the reception terminals; by handing over the welcome booklet and the discharge situation bulletin to all hospitalized patients; by the dissemination of information on the online platform for dialogue between the patient and the establishment "MyCHUGA". The CHUGA also provides for collective information via dissemination on its website, the posting of information notices in the establishment's waiting rooms and the use of information campaigns (on social networks, regional media, press release and at public events within the CHUGA). With regard to CHUGA staff: The staff will be informed individually via the establishment's intranet and a newsletter accompanying the delivery of the payslip. The rights of the persons concerned are exercised with the data protection officer. The Commission requests that the information media be supplemented in order to contain all of the information provided for in Articles 13 and 14 of the GDPR. Subject to these observations being taken into account, the Commission considers that these methods of information and exercise of rights are satisfactory with regard to the provisions of the GDPR and the law "Informatique et Libertés". On security measures The

Commission takes note of the completion by the CHUGA of a data protection impact study which made it possible to build and demonstrate the implementation of the principles of protection of privacy in the constitution of the warehouse. The constitution of the warehouse is carried out by the deposit then the organization and the cleaning of the data related to the care of the patients of the CHUGA (data resulting from actions of care, administrative data and data generated by the operation of CHUGA). In the warehouse database, the directly identifying data (surname, first name, address, date of birth of the patient) are partitioned and can only be handled routinely by the personnel responsible for importing the data and administering the warehouse. The other health data will be pseudonymised using an identifier generated by a secret key hashing procedure. As regards access to the warehouse for research projects, the Commission notes that these are issued by a Participant orientation of warehouse governance. Following the submission of an application and its validation, the administrators of the warehouse prepare the data which will be made available to the applicants. The Commission notes that it will be necessary to ensure that each set of data thus created has a duration of use defined in advance and strictly limited to the needs of the project concerned. The Commission notes that the methods of access by users to the data prepared by the administrators will be defined later. In this regard, it recalls the need to implement effective security conditions, of a high level and such as to guarantee the confidentiality of data for the provision of files. These conditions must be based on means making it possible to ensure the authentication of recipients, confidentiality and integrity of transmissions as well as management of authorizations allowing recipients to be granted the right to access only the data they need. The Commission notes that different authorization profiles are provided to allow preparation and extraction of data from the warehouse, in order to manage access to data as needed, with the combination of four independent rights: access to de-identified structured data; access to the textual search tool; direct access to unstructured data; access to directly identifying structured data. Access rights to the warehouse are open erts to persons mandated by a research project, for a limited time and according to the data strictly necessary with regard to the protocol and the principle of data minimization. Access permissions are removed for any user who is no longer authorized and closed automatically at the end of the authorization period. In addition, the Orientation Committee carries out periodic checks on all authorisations. The Commission observes that a strong authentication policy is implemented, based on an individual identifier and a password in accordance with Commission deliberation no. 2017-012 of 19 January 2017, as well as on the use of a healthcare professional card (CPS). The Commission notes that depending on the availability requests that will be made, the data may be subject to different types of pre-processing. In accordance with the protocol for each research

project, they may thus be aggregated, pseudonymised or anonymised. In this respect, the Commission notes that an export committee, made up of a doctor and two engineers, assisted by two operational link with the projects concerned, will be responsible for checking beforehand the data intended to be exported, by checking in particular, in accordance with the state of the art in the matter: the minimum number of patients acceptable in a data set; allocation of a different patient identifier for each export (except in the particular case of cohort monitoring, where a correspondence table will be kept to ensure chaining between exports); maintenance of secrecy concerning the internal pseudonym at CHUGA- EDS and its generation key, which will never be exported or exposed; the use of appropriate and state-of-the-art tools for the pseudonymization of unstructured data. The export committee will also ensure ent, through scientific monitoring and exchanges with other EDS, the development of export rules and good practices, as well as the qualification and implementation of specific tools that will be made available by the EDS. subjects, the Commission recalls that: in the case of anonymisation: it will be necessary to demonstrate the compliance of the solution and the anonymisation techniques implemented with the three criteria defined by G29 opinion No. 05/2014, and forward it to the Commission; Failing that, if these three criteria cannot be met, a study of the risks of re-identification will have to be carried out. This study consists of demonstrating that the risks, linked to the publication of the dataset, have no impact on the privacy and freedoms of the persons concerned; in the case of pseudonymization: the data manipulated must no longer be attributed to a specific person without having recourse to additional information, this additional information having to be kept separately and subject to adequate technical and organizational measures. In particular, the Commission recalls the need to exclude any identifying data such as first name, surname, maiden name, postal address, e-mail address, telephone number, date of birth/death, place of birth/death, visit number , technical identifier, etc.; in the case of the pseudonymization of unstructured documents (such as medical reports for example): such an operation must be carried out with vigilance, in particular if it implements automated tools and for which errors are likely to occur. The actions of users accessing the warehouse are subject to traceability measures. In particular, the connections to the warehouse are traced (identifiers, date and time) and the requests and operations carried out. Traces are checked at the end of each authorization period linked to a research project. The Commission also recommends setting up an automatic trace control, in order to detect abnormal behavior and raise alerts if necessary. The Commission observes that the warehouse is accessible only on the CHUGA internal network from an interface provided for this purpose. Access is secured using the HTTPS protocol. This uses encrypted communication channels and ensures the authentication of the source and the recipient. Regarding the use of this

protocol, the Commission recommends using the most up-to-date version of TLS possible. In addition, measures are planned to ensure the compartmentalization of processing. The network is subject to filtering measures aimed at restricting the transmission and reception of network flows to identified and authorized machines. The Commission notes that software updates are installed on a regular basis. Specific measures are planned to guarantee the availability of data and services. An anti-malware policy is defined and anti-virus software is installed and regularly updated on all hardware involved in processing. Finally, an IT environment maintenance policy is defined, ensuring that appropriate data security measures are implemented. Maintenance interventions are thus subject to traceability. A backup policy is implemented. Backups are tested regularly to verify their integrity. The transfer of backups is secure. They are stored in a place that guarantees their security and availability. In addition, when scrapped, the stored equipment is cleaned of any personal data. Used or broken down storage media are subject to a destruction or erasure procedure. Access to the premises housing the equipment taking part in the processing is restricted by means of locked doors controlled by a means of personal authentication. . Detection and protection measures against the risk of fire, water damage and loss of power supply are proposed. The security measures described by the data controller comply with the security requirements provided for in articles 5-1-f and 32 of the GDPR. The Commission recalls, however, that this obligation requires the updating of security measures with regard to the regular reassessment of the risks. On the retention period of the data The data is kept in the warehouse for twenty years and then deleted. The Commission considers that this data retention period does not exceed the period necessary for the purposes for which they are collected and processed, in accordance with the provisions of Article 5-1-e of the GDPR. Grenoble Alpes University Hospital Center, in accordance with this deliberation, to implement the treatment mentioned. For the President The Deputy Vice-President Sophie LAMBREMON