DELIBERATION n°2019-113 of SEPTEMBER 5, 2019National Commission for Computing and LibertiesNature of the deliberation: AuthorizationLegal status: In force Date of publication on Légifrance: Tuesday, November 05, 2019Deliberation n° 2019-113 of September 5, 2019 authorizing Assistance public — Hôpitaux de Paris to implement automated processing of personal data for the purpose of setting up and implementing a data warehouse, called the "National Rare Diseases Data Bank" (BNDMR)(Request for authorization n° 2211418) The National Commission for Computing and Liberties, Seizure by the Public Assistance - Hôpitaux de Paris of a request for authorization concerning the automated processing of personal data for the purpose of setting up a warehouse database called “National Rare Diseases Data Bank” (BNDMR); 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 individuals with regard to the processing of personal data and on free movement of this data, and repealing Directive 95/46/EC; Having regard to the Public Health Code; Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms, in particular its articles 44-3° and 66-III; Considering decree n° 2019-536 of May 29, 2019 taken for the application of law n° 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; Having heard Mrs Valérie PEUGEOT, commissioner, in her report, and Mrs Nacima BELKACEM, government commissioner, in her observations; Formulates the following observations: On the data controller: Public Assistance – Hôpitaux de Paris (hereinafter the “AP-HP”) On the legal basis and the purpose of the processing epidemiological and medico-economic studies. More specifically, the purposes pursued by the processing are as follows: management of public policies, creation and publication of indicators and establishment of an annual report on rare diseases; carrying out feasibility studies; carrying out research in the field of health (non-interventional research involving the human person or research not involving the human person). The Commission notes that specific governance is planned for the BNDMR, through two committees: the steering committee (COPIL BNDMR) and the scientific committee (COSCI BNDMR). The Commission also notes that the conditions of participation and access to the BNDMR will be governed by a charter. The legal basis for processing is the exercise of a mission in the public interest, within the meaning of Article 6-1 -e of the General 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 et seq. 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 personal health data which will be implemented subsequently, for the purposes of research, study and evaluation in the field of health are separate processing operations which must be subject to specific formalities under Articles 72 et seq. of the law “IT and freedoms”. On the data processed: The BNDMR brings together the administrative and medical data produced by the BaMaRa databases, from the rare disease reference centers and rare disease competence centers. The categories of personal data processed concerning patients are as follows :identifying information: date of birth (day, month and year of birth), place of birth and residence (INSEE code), gender; rare disease identifier number (IDMR) (non-reversible identifier made up of surname, first name, date of birth, gender); health data: diagnosis(es) of interest, medical and paramedical observations, drug treatments, neonatal data; care pathway data: care number generated by the system, date of care , structure responsible for treatment, context of treatment; participation in research or studies, willingness to participate in studies, existence of biological samples gic; notification of individual information. The Commission also notes that the birth name, birth name, date of birth, sex, place of birth, place of residence and national health identifier (INS) will be processed within the framework of identity-vigilance and reconciliation of identities. This data will be kept on a temporary server for the time necessary for identity-vigilance operations. The surname, first name and INS will not be kept in the BNDMR once these operations have been carried out. The data processed concerning the professionals taking care of the patients are as follows: registration number in the shared directory of health professionals (RPPS); place of practice (FINESS number). The categories of personal data processed concerning AP-HP agents who use the BNDMR are as follows: surname, first name; e-mail address; APH code; connection data. 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 General Data Protection Regulation. The Commission is informed that the data collected is likely to completed as part of the implementation of the National Rare Diseases Plan (PMNR)3 (2018-2022), which entrusts new missions to the BNDMR. The data controller indicates, however, that it will always be data relating to health collected as part of the treatment, with a level of sensitivity comparable to the data described in the initial request. It will be up to the data controller to determine whether the changes require submitting a request for modification of this authorization to the Commission. national health data system (SNDS). Such a modification will have to be the subject of specific formalities with the Commission. On the recipients: For the constitution and management of the data warehouse: the

BNDMR is accessible to the members of the operational cell BNDMR, within the premises of the 'AP-HP.For the dissemination of indicators: the Ministry of Health, the ARS, as well as the partner rare disease centers and manufacturers are recipients of the exact results representing the actual numbers of the indicators.For the performance of studies of feasibility and carrying out of research in the field of health (non-interventional research involving the human person or research not involving the human person), may be recipients of the data: health professionals from rare disease reference centers (CRMR) and rare disease competence centers (CPMR), belonging to the care team and relating to data from the patients they take care of directly; health professionals from CRMRs and CPMRs (possibly associated with external partners) concerning the data of patients treated in several departments or establishments, or even patients from all CRMRs and CPMRs; external organizations from the public sector or private, provided that the processing requested is in the public interest. the form of an overall number of patients concerned. The results of the correspondence tests are communicated to the recipients by the operational unit of the BNDMR in the form of a percentage of patients concerned. When the research is carried out under the responsibility of the AP-HP, the data remains in the warehouse and is processed exclusively by members of the BNDMR operational unit, after going lidation by the COSCI BNDMR. When the research is carried out under the responsibility of an entity other than AP-HP, indirectly identifying data strictly necessary for the purpose of the processing may be extracted from the warehouse and transmitted to the third-party investigator, under conditions guaranteeing their security and confidentiality and after validation by the COSCI BNDMR. particular nature and high risks of re-identification.The Commission considers that the categories of recipients do not call for observation.On information and procedures for exercising rights:Patients included in the CEMARA research project (request no. 1187326 ): In 2007, the Commission authorized data processing for the purpose of carrying out a research project entitled CEMARA. The purpose of this project was to assess and develop health strategies aimed at improving the care of patients with rare diseases. The data collected as part of the study was integrated into the BaMaRa application. Pursuant to Article 14-5-b of the GDPR, the obligation to provide individual information to the person concerned 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 have been collected within the framework of the CEMARA research project and that appropriate measures will be implemented. , in particular by posting on the website dedicated to the BNDMR and by displaying information relating to the processing whose implementation is envisaged. Patients included in the BaMaRa application before the creation of the BNDMRA from the he year 2017, the year of deployment of the BaMara application, patients were individually informed by the delivery of an information note: of the processing of data concerning them, within the framework of care; of the reuse of this data for research projects, within the framework of the future BNDMR; procedures for exercising their rights. The information note refers the patient to the page dedicated to transparency on the BNDMR website, on which the details of all treatments implemented will be kept up to date. The healthcare professional taking charge of the patient is required to trace in the BaMaRa application, by means of a checkbox, the delivery of the information and the patient's non-objection to the use of the data concerning him in the framework of the BNDMR. The right of opposition will be exercised, at any time, either directly with the clinician, or with the BNDMR operational unit by electronic message (at the address indicated on the information form); in the latter case, the box provided for exercising the right of opposition will be checked a posteriori and the data already transmitted will be deleted. Patients treated after this authorizationPeople treated after the authorization will be informed of the creation of the BNDMR as well as the treatments implemented from the BNDMR by means of an information notice provided individually by the healthcare professional caring for them. This professional will be required to trace in the BaMaRa application, by means of a checkbox, the delivery of information and the patient's non-objection to the use of data concerning him for research purposes. individual information refers to a transparency portal made available to the public on the website dedicated to the BNDMR. Each of the processing operations (steering indicators, feasibility studies, correspondence tests, research involving or not involving the human person, etc.), implemented using data from the BNDMR, will be documented there. exercised with the AP-HP, more specifically with the data protection officer, via a dedicated form on the BNDMR website, or by sending an email to a specific address mentioned in the information notice .The Commission requests that the information media be supplemented in order to contain all the information provided for in Articles 13 and 14 of the GDPR. Subject to this reservation, the Commission considers that these methods of information and exercise of rights are satisfactory. On security measures: Firstly, the Commission takes note of the performance by AP-HP of an impact analysis on data protection which has made it possible to build and demonstrate the implementation of the principles of data protection in the constitution of the health data warehouse. The Commission notes that the AP-HP is an approved host of health data. 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, during disposal, the stored equipment is cleaned of any personal data. Used or broken down storage media are subject to a destruction or erasure procedure. The Commission notes that encryption of the data stored within the BNDMR has been put in place. The Commission considers that the nature of the data requires that it be subject to encryption measures in accordance with appendix B1 of the general security reference system, both in terms of databases and backups. The Commission notes that the data stored within the various BaMaRa databases are subject to pseudonymization. Once pseudonymized, this data will be transmitted by secure flow to the BNDMR storage area. additional information, such additional information to be kept separately and subject to adequate technical and organizational measures. surname, first name, date of birth and sex. In this respect, the Commission recommends the use of a hashing algorithm with a secret key. to manage data access as needed. Access to warehouse data is carried out within the AP-HP internal network itself, in particular to allow the preparation of aggregated data. Aggregated data is then available on the AP-HP web portal for a time window of up to one week. Access to the portal is secured through encrypted communication channels and provides source authentication and of the recipient. Regarding the use of the HTTPS 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. With regard to access to pseudonymised data accessible via the APHP intranet, the Commission recommends the implementation of a strong authentication policy. It also recalls that access to health data by health professionals must be in accordance with the interoperability and security standards pursuant to Article L 1110-4-1 of the CSP. The Commission also notes that access to the aggregated data available via the AP-HP portal is based on an individual identifier and a password. In this regard, it recalls that a satisfactory password policy must comply with its deliberation no. 2017-012 of January 19, 2017 adopting a recommendation relating to passwords. In particular, it recommends that access keys be transmitted via a channel separate from email. A logging of operations for consulting, creating and modifying BNDMR data is in place. The logs are analyzed monthly. The Commission also recommends carrying out automatic monitoring of traces, in order to detect abnormal behavior and generate alerts if necessary. The Commission also recommends that measures be implemented to ensure the integrity of the logs and that the administrator who is able to consult the logs of the accesses does not access the health data. The Commission notes that management measures security

incidents and data breaches are put in place. It recalls the need to set up a procedure for managing incidents and data breaches that is documented, regularly updated, and tested through regular tests. The security measures described by the data controller comply with the security requirement provided for by 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 periods: Data relating to patients The data necessary for identity-vigilance operations (birth name, first name of birth, date of birth, sex, place of birth, place of residence and INS) are kept on a temporary server for the duration of the said operations (duration less than one day). They are then deleted. Other data is kept for 20 years. At the end of this period, the data will be deleted. The data relating to requests for the exercise of rights (identity of the applicant, type of supporting document, date of response, copy of the response) will be kept for five years. Supporting documents are kept for one year. Data relating to professionals caring for patients: Data is kept for 20 years. At the end of this period, the data will be deleted. Data relating to AP-HP agents who use the BNDMR: The connection logs are kept for five years. The information associated with the accounts is kept for one year after the departure of the agent. The Commission considers that these data retention periods do not exceed those necessary for the purposes for which the data are collected and processed, in accordance with the provisions of the Article 5-1-e of the GDPR. Under these conditions, the Commission authorizes Assistance Publique – Hôpitaux de Paris to implement automated processing of personal data for the purpose of setting up and implementing a warehouse database, entitled “National Rare Diseases Database”. The President Marie-Laure DENIS