DELIBERATION n°2019-110 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° 2019-110 of September 05, 2019 authorizing the Hospital Center University of Limoges to implement a general register of cancers in the Limousin region (Request for authorization n° 999305)The National Commission for Computing and Liberties,Seizure by the University Hospital Center of Limoges of a request for authorization concerning a general register of cancers in the Limousin region; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of 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 this 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 6 January 1978 as amended relating to data processing , to files and to 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 the law n ° 78-17 of January 6, 1978 relating to information technology, files and freedoms; Having regard to 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 controller The Limoges University Hospital Center (Limoges University Hospital) On the legal basis and purpose of the processing The Limoges University Hospital implements a general register of cancers in the region Limousin. This register allows an exhaustive collection of ca s of cancers in people residing in Haute-Vienne. The data thus grouped are used for epidemiological surveillance purposes and will ultimately be used for health research purposes. The legal basis for the processing is the exercise of a mission 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. considers that it is necessary to apply the provisions of articles 44-3° 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, for the purposes of research in the field of health, from the data contained the warehouse are separate treatments that i must be subject to specific formalities under articles 72 and following of the Data Protection Act.On the data processedThe register groups together administrative

and medical data produced by different sources of information, such as the departments of medical information from public and private establishments, health insurance funds, pathological anatomy laboratories in particular. The categories of personal data processed concerning patients are as follows: patient identification data: names, first name, date of birth and place of birth, gender, address at the time of diagnosis; patient health data related to the tumor pathology: history, history of the disease, diagnosis of the tumor and its specific characteristics (date of diagnosis, location, morphology, grade of differentiation, tumor behavior and extension), the results of complementary examinations ires allowing to identify the basis of the diagnosis, the seat of the tumor and its morphology (samples of biological fluids or organs, imaging examinations); the vital status and the date of death. The surnames and first names of the attending physicians data are also collected where applicable. 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 recipients The Commission notes that only the registry staff has access to personal data. Any transmission outside the register takes place in anonymised form. Anonymous data are sent to the national database of cancer registries for regional and national estimates. They can also be made available to research teams that are partners of the registry. On information and the rights of individuals Patients are informed of the processing of their data within the registry and of their rights by the delivery of a notice information by their treating doctor or the doctor taking charge of them within the health establishment. Information is also provided by the Health Insurance Fund in the notification letter of 100% coverage for a long-term condition. The rights of the persons concerned are exercised with the doctor responsible for the register. The Commission requests that the information media be completed in order to contain all the information provided for in Articles 13 and 14 of the GDPR. Subject to the modification of the information documents, the Commission considers that these methods of information and exercise of rights are satisfactory. On security measures The regulatory team stre is made up of five people (a doctor, a data manager and three research associates). The database is only visible and accessible to this team. No subcontractor has access to the data or the registry database. The Commission recommends that an overall review of authorizations be carried out regularly, during staff movements and at least once a year. The members of this team have signed a data confidentiality clause. Access to workstations requires a identifier and a password or a card specific to each member of staff to open their session. Access to the register data then requires two levels of authentication: a first authentication to access the digital environment of the CHU , then a second authentication to access the database of the register. With regard to the complexity of passwords, the

Commission recalls that the policy put in place must comply with deliberation no. 2017-012 of 19 January 2017 adopting a recommendation relating to passwords. The Commission recalls that communications to the servers and applications hosting the register must be encrypted and use prototypes state-of-the-art cryptographic schools and algorithms, in their latest versions. The Commission also recommends encryption of the registry database. Electronic files transmitted from the various data sources or sent to recipients are encrypted with state-of-the-art software and algorithms. Logging of connections, access to data and user actions is implemented. The Commission recalls that maintenance interventions must be subject to traceability measures. Physical access to the server hosting the register is restricted by means of locked doors controlled by a means of personal authentication. Regular backups are made. They are encrypted and stored in a place that guarantees their security and availability. The Commission recalls that these must be tested regularly in order to verify their integrity. Access to aggregated statistics from the program for the medicalization of information systems (PMSI) has been set up in order to verify the completeness of the data in the register. . The Commission recalls that only data resulting from anonymization processes, such that the direct or indirect identification of individuals is impossible, can be extracted. To claim the anonymity of a data set, the controller must carry out an analysis to demonstrate that its anonymization processes meet the three criteria defined by Opinion No. 05/2014 on data processing techniques. anonymisation adopted by the Article 29 group (G29) on April 10, 2014. Failing this, if these three criteria cannot be met, a study of the risks of re-identification must be carried out. Subject to the above observations, the measures described by the data controller comply with the security requirement provided for in Articles 5.1.f and 32 of the GDPR. risks. In this respect, it recalls that specific attention should be paid to the reassessment of security measures as part of the update of the impact analysis. On the data retention period The CHU wishes to keep the registry data 20 years from the last notification received. He argues the need for the registry to keep the patient's medical history and history in terms of cancer in order to distinguish recurrences from new cases. 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. Authorizes the University Hospital Center of Limoges, in accordance with this deliberation, to implement the processing mentioned. For the President The Deputy Vice-President Sophie LAMBREMON