Deliberation 2023-040 of April 20, 2023 National Commission for Computing and Liberties Nature of the deliberation: Other authorization Legal status: In force Date of publication on Légifrance: Friday May 05, 2023 Deliberation n° 2023-040 of April 20, 2023 authorizing the National Institute of cancer to modify a processing of personal data for the purpose of a health data warehouse aimed at studying the trajectories of people with cancer, entitled: "Oncology data platform" (Application for authorization no. ° 2228513) The National Commission for Computing and Liberties, Seizure by the National Cancer Institute of a request for modification of the authorization relating to the automated processing of personal data for the purpose of setting up a health data warehouse aimed at studying the trajectories of people with cancer; 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 treatment personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR); Having regard to Law No. 78-17 of January 6, 1978 as amended relating to information technology, files and freedoms, in particular articles 44-3° and 66-III; Having regard to deliberation no. 2019-082 of June 20, 2019 authorizing the National Cancer Institute (INCa) to implement a treatment automated processing of personal data for the purpose of setting up a health data warehouse aimed at studying the trajectories of people with cancer, entitled: "Oncology data platform"; Having regard to deliberation no. 2021-118 of October 7, 2021 adopting a reference system relating to the processing of personal data implemented for the purpose of creating data warehouses in the field of health; Considering the file and its supplements; On the proposal of Mrs. Valérie PEUGEOT, commissioner, and after having heard the observations of Mr. Benjamin TOUZANNE, government commissioner. Makes the following observations: Responsible for processing The National Cancer Institute (INCa). Modifications to data processingThe modifications relate to:the purposes of the processing;the categories of persons concerned by the processing;the existing databases gathered within the PDC (data source);the categories of data processed;the categories of recipients ;the procedures for informing people;the security measures.Points of non-compliance with the reference system concernedThe Commission notes that the application file mentions that the planned processing complies with the provisions of the "data warehouse in the field health", with the exception of: certain purposes pursued; the sources of the data collected; the categories of data concerned; the retention periods; the procedures for informing individuals; the rights of individuals; security measures. Apart from these exceptions, the processing must comply with the framework provided by the "data warehouse in the field of health" reference system. On the purpose and legal basis of the processing The changes envisaged are intended to extend the purposes pursued by the Cancerology Platform (PDC). In addition to the

purposes mentioned in deliberation no. 2019-082, the processing will enable INCa to: define and monitor the ten-year strategy for the fight against cancer; produce public statistics in connection with this strategy; carry out expert appraisals on request ministries, the Court of Auditors and Parliament on issues relating to oncology; making PDC data available to third parties for carrying out research, studies or assessments in the field of oncology and to respond to the national strategy for "health industries and technologies". The purposes of the processing are determined, explicit and legitimate, in accordance with the provisions of Article 5.1.b of the GDPR. The Commission notes that INCa undertakes to: not process or make available the data of the warehouse for the purpose of promoting health products to health professionals or health establishments, or for the purpose of excluding guarantees from insurance contracts and modifying insurance contributions or premiums an individual or a group of individuals presenting the same risk; not allowing the reuse of data from the PDC in the context of research involving the human person as defined in articles L. 1121-1 to L. 1128-12 of the Public Health Code (CSP); publish the results of studies conducted on the basis of the PDC. The Commission considers that the provisions of Articles 44-3° and 66-III of the Law No. 78-17 of 6 January 1978 amended relating to data processing, files and freedoms (hereinafter the amended "Data Processing and Freedoms" law), which requires its authorization for processing involving data relating to health and justified, as in this case, by the public interest. 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 amended "Informatique et Libertés" law, which impose that each processing is justified by the public interest and is the subject of its own formalities. On the legal basis of the processing The processing has as its legal basis the performance of a public interest mission entrusted to the data controller, at the meaning of Article 6.1.e of the GDPR. The processing of sensitive data is necessary: for the purposes of scientific research, in particular with regard to the provision of PDC data to third parties for the performance of research, studies or evaluations in the field of oncology (art. 9.2.j of the GDPR); for a reason of important public interest for the other objectives pursued by the PDC, provided that the subsequent processing is carried out under the responsibility of the INCa (art. 9.2.i of the GDPR). On the data processed The warehouse will consolidate data from: components of the main database of the national health data system (SNDS), within the limits of the permanent access available to INCa pursuant to Articles R. 1461-11 et seq. of the CSP and subject to their availability; cancer registers; studies for which INCa is responsible or joint responsible for treatment; summaries of visits to the emergency room (Oscour database); research, studies or assessments carried out by health manufacturers as part of the artificial intelligence and cancer sector project; medical files making up the cancerology

communicating file; regional cancer screening coordination centers. The historical depth of the data processed will be nineteen years , in addition to the current year. Data relating to patients: Only data from people who have or have had cancer, people entering a prevention or screening system or people suspected of being affected cancer will be brought together within the PDC. People suspected of having cancer are people at high risk, either because of a positive screening test or because they have a genetic predisposition. The following data will be processed in the PDC: identification: first name, last name, contact details (telephone, electronic, postal), permanent patient identification number (IPP), care episode identification number (IEP), national health identifier (INS), date full birth, sex and gender; health data: medical, medico-social and medico-economic information relating to the health course, medico-social information relating to the situation of people with disabilities, information relating to work stoppages and benefits in cash, information relating to vital status and causes of death; data relating to personal life: information relating to place of residence, lifestyle, professional life, social deprivation; data relating to insurance organizations compulsory health insurance and complementary health insurance bodies, limited to those contained in the main SNDS database. Identification data (first name, last name, IEP, EPP, INS), contact details (postal, electronic, telephone) and complete date of birth will come exclusively from the medical records making up the communication file in oncology. The identification data and contact details of the persons will be deleted as soon as the pseudonymisation is carried out at short notice in the PDC. The Commission notes that the INS will be the subject of a pseudonymisation operation at short notice as soon as the data from files communicating in oncology in the PDC. Data relating to healthcare professionals: identification data: surname, first names, ADELI number, number of the shared directory of healthcare professionals (RPPS); data relating to professional life: function , place and mode of exercise. 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. recipients Only designated and authorized INCa personnel can access the data under this authorisation. The recipients of the data are: the designated and authorized personnel of subcontractors working on behalf of INCa; of INCa who conduct a research, study or assessment project in the field of oncology, provided that a contract of joint responsibility, within the meaning of article 26 of the GDPR, or of subcontracting, within the meaning of Article 28 of the GDPR, has been concluded with the INCa. The Commission notes that the categories of recipients and accessors are subject to professional secrecy governed by the provisions of Articles 226-13 and 226- 14 of the penal code.Information of personsThe Commission takes note of the INCa's commitments according to which:a list of the existing databases collected within the PDC

will be published on the INCa website. This list must be updated regularly as soon as a data provision contract is concluded or terminated in order to provide transparent information to people concerning the databases gathered within the PDC; a reference to the data support information for data controllers of the databases collected within the PDC (data providers) will be provided from the INCa website; a dedicated telephone line will be set up by INCa to inform people about the PDC. The Commission requests that: the information relating to the implementation of the PDC be accessible on the websites of the controllers of the databases gathered within the platform; a period of one month be respected between the delivery of information to the persons concerned or their legal representatives or the updating of the list of databases published on the INCa website and the effective entry of the data into the PDC; it is communicated to it every three n a report on the operation of the PDC and on the research carried out using the data it contains. processing of the databases collected within the platform an information note intended for patients, their legal representatives and healthcare professionals in accordance with the provisions of the GDPR and to ensure that this information will be given to them. The information media must include all the information provided for in Article 14 of the GDPR. The Commission also recalls that, when the controller wishes to adopt a multi-level approach to informing individuals, the first information should contain, in accordance with the guidelines on transparency within the meaning of the GDPR of 29 November 2017 of the "Article 29" working group (G29), information relating to the purpose of the processing, the identity of the controller, a description of the rights of the data subjects, as well as any information on the processing which would have a significant impact on the data subject. In this case, the Commission asks that all information media indicate that the exercise of rights by people, in particular their right to object, will have no consequences on their medical care and mention a referral to the web page dedicated to information relating to the PDC. It is recalled that the information relating to the constitution and modifications of the PDC does not replace: the information incumbent on data providers for the processing of personal data that they implement in their capacity as data controller, in particular with regard to processing relating to the keeping and management of medical records, processing relating to the creation of a pseudonymised database with a view to their reuse for research, study or evaluation purposes and the processing carried out for research, study or evaluation purposes; the information incumbent on any data controller who proceeds with the reuse personal data from the PDC, in particular for research, study or evaluation purposes. Article L. 1461-3 of the CSP makes access to data from the SNDS and its components subject to communication to the Health Data Platform (PDS) of several elements by data controllers, before and after the studies. Research, study or evaluation projects carried out

using PDC data must be registered in the public directory of the PDS. The Commission recommends that the PDC be also registered in the public directory of the PDS. With regard to people whose data comes exclusively from the SNDS and people already included in the PDC whose medical follow-up is no longer in progress: In application of Article 69 of the "Informatique et Libertés" law and Article 14.5.b of the GDPR, the obligation to provide individual information to the data subject may be subject to exceptions, in particular in the event that the provision of such information would prove impossible, would require disproportionate efforts or would seriously compromise the achievement of the objectives of the processing. In such cases, the controller shall take 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 this case, an exception is made to the principle of individual information and appropriate measures will be implemented, in particular by: posting an information note on the PDC on the INCa website; posting on the INCa social network pages of an information note relating to the PDC; the insertion in the practical guides "patient guides", available on the INCa website, of an information note dedicated to the PDC; the distribution via the letters of information (newsletter) from patient associations or the posting within these associations of an information note dedicated to PDC. With regard to people whose data comes from regional cancer screening coordination centres: These people will receive a first level of information referring to the PDC website, included in the invitation letter to organized screening for breast cancer, colorectal cancer and cancer of the cervix. the data comes from a cancer registry:These people will receive a first level of information referring to the PDC website, integrated into the information note relating to the cancer registry concerned.As regards people whose data are taken from the communication file in oncology:These people will receive a first level of information referring to the PDC website, which will be integrated:in the welcome booklet mentioned in article L. 1112-2 of the CSP;in the documents submitted to the person when announcing a diagnosis ("patient kit"). The Commission points out that each of these first levels of information must include the information mentioned by the G29 in its guidelines on transparency. Articles 12 and following of the GDPR. Rights of persons The Commission notes that, the purposes pursued by the PDC not requiring the processing of directly identifying data, the data of the PDC will be pseudonymized by the data controllers of the databases collected within the PDC or, in the case of data from medical records making up the communication file in oncology, as soon as they are received. Individuals may exercise their rights (access, rectification, opposition or deletion) by directly contacting the data controllers of the organizations at the origin of the collection of the data concerned. INCa is committed to facilitating the exercise of these rights by referring to these different structures. Individuals

may contact INCa electronically or by post. The Commission recalls that if the individuals concerned provide additional information allowing them to be re-identified, the exercise of their rights must be made possible directly with INCa, in accordance with Article 11 of the GDPR.Security measuresThe data controller has carried out and transmitted in support of the authorization request an impact analysis relating to the protection of data specific to the PDC. Approval of this warehouse was also carried out by the approval authority on October 5, 2022 in accordance with the order of March 22, 2017 relating to the security reference system applicable to the SNDS, for a period of one year, subject to the implementation of the action plan it has defined. This approval decision is only valid until October 5, 2023 and will therefore have to be renewed before this date. The security measures planned or implemented in the PDC have been compared with the security requirements mentioned in the reference system " data warehouse in the field of health" by the data controller. Discrepancies with the security requirements of this standard have been noted concerning: the pseudonymization of health data; the pseudonymized patient identifiers that may be provided by the CNAM for data relating to the SNDS or generated by the PDC. and the sensitivity of the data processed, the pseudonymization of health data must be carried out within the PDC in an integration environment comprising reinforced technical and organizational security measures, in particular in order to guarantee network, cryptographic and system partitioning specific to the integration environment, compared to the rest of the health data warehouse. This pseudonymization must be carried out as soon as possible and the directly identifying data and the contact details must be deleted as soon as the pseudonymization of the data and documents has been carried out. The Commission recalls that the various pseudonymized identifiers relating to each of the various bases hosted, the pseudonymized derived from the INS, as well as the main identifier, will have to be generated in accordance with the requirements of the aforementioned repository by a cryptographic hash function resistant to brute force attacks or a cryptographically secure pseudo-random number generator. the goal is to store the different pseudonymised identifiers of the hosted databases, and the main identifier must be partitioned from the rest of the warehouse with encryption dedicated to this single table. Specific access profiles must be implemented in order to guarantee enhanced traceability when accessing this data. Pseudonymised data will be encrypted at rest by state-of-the-art algorithms within a host certified for the hosting of health data, located in France and not subject to extra-European regulations. The security measures, which must be operational during the implementation of the processing, must meet the requirements provided for in articles 5.1. f and 32 of the GDPR, taking into account the risks identified by the data controller. It will be up to the data controller to carry out a regular reassessment of the

risks for the persons concerned and an update, if necessary, of these security measures.Transfers of dataThis authorization does not constitute an authorization for transfer outside the European Union. On the retention period The identification data and contact details of people from the medical files making up the communication file in oncology will be deleted as soon as they are entered into the PDC. The person's INS will be deleted as soon as the pseudonymization operation is carried out. Personal data from the SNDS are kept for a period in accordance with the provisions of Article R. 1461-13.I. 1° of the CSP. Personal data other than those from the SNDS will be kept for twenty years from the last inclusion of data concerning the person in the warehouse. The Commission considers that these data retention periods do not exceed not the duration necessary for the purposes for which they are collected and processed, in accordance with the provisions of Article 5.1.e of the GDPR. Additional comments The other conditions for implementing the PDC remain unchanged. AUTHORIZES the National Cancer Institute to put implement, for a period of ten years, the processing described above. The President Marie-Laure DENIS