

Deliberation 2022-009 of January 27, 2022 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° 2022-009 of January 27, 2022 authorizing the company Clinityx to put implements automated processing of personal data for the purpose of setting up a health data warehouse, called "Magellan" (authorization request no. 2224905)The National Commission for Computing and Liberties, Seized by the company Clinityx of a request for authorization relating to the automated processing of personal data for the purpose of setting up a health data warehouse, called Magellan; 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 the free movement of such data data, and repealing Directive 95/46/EC (RGPD); Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms (Data Protection Act), in particular its articles 44 -3 and 66-III;After hearing the report of Ms. Valérie PEUGEOT, commissioner, and the observations of Mr. Benjamin TOUZANNE, government commissioner,On the data controller:Clinityx is a design office that carries out research in the field of health, in particular based on data from the National Health Data System (SNDS). It develops tools to enable the use of health data under enhanced protection conditions. On the purpose of the processing, its lawfulness and the conditions for processing data concerning health: The company Clinityx wishes to constitute a data warehouse in order to be able to feed a tool intended to automatically calculate predetermined public health indicators relating to the populations of patients, the use of care, and the use of health products. This tool - called Magellan - aims to allow :evaluate the representativeness of a registry or a cohort;evaluate access to health products and care for the population;evaluate the contribution of a new technique, technology , health product or medical practice on the care of a population; to assess the impact of health and social protection policies on the population; to carry out feasibility studies in the framework of research involving or not involving the human person. This warehouse will be supplied with certain personal data from the SNDS. The Commission notes that the creation of the Magellan warehouse aims to: firstly, make available to certain actors in the field of health (patient or health professional associations, small or medium-sized enterprises, etc.) aggregate public health indicators relevant to their activities, calculated from SNDS data; hand, to limit the number of individual SNDS data processing operations necessary for the construction of simple aggregated indicators in a logic of protection of privacy from the design stage. It also notes that the company Clinityx transmitted, in support of its authorization request, a description of the use cases for the Magellan tool. 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. The processing implemented by Clinityx is necessary for the purposes of the legitimate interests it pursues. , taking into consideration the very indirectly identifying nature of the data and the guarantees, particularly in terms of individual rights, provided for by the texts governing the provision of SNDS data. This processing is, as such, lawful with regard to the article 6-1-e of the GDPR and fulfills a condition allowing the processing of data concerning health with regard to article 9-2-i of the GDPR. The Magellan warehouse is subject to the provisions of articles 44-3° and 66-III of the amended law of January 6, 1978 which provides, in the absence of compliance with a reference system, that processing involving data relating to health and justified, as in this case, by the public interest cannot be implemented only after authorization from the Commission. The data contained in this repository may not, in accordance with the principle of the prohibited purposes of use of the SNDS, be used for the purposes of promoting health products to health professionals or establishments. of health, 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 – CSP). The Commission recalls that future uses of the data contained in this warehouse will fall within the framework of the provisions of Articles 66, 72 and following of the Data Protection Act, which require that each research project, study or evaluation be justified by the public interest and be subject to its own formalities.

On the governance of the warehouse: Clinityx has set up a governance system for the Magellan warehouse consisting of a committee in charge of: proposing the strategic orientations of the Magellan tool; deliver an opinion on the relevance of the indicators produced and the data used to calculate these indicators; review the annual report on the use of the tool prior to its publication. The Commission notes that this committee will notably be made up of members qualified in SNDS data processing.

On the nature of the data processed: The following data may be fed into the Magellan warehouse: consumption data individual data (from the inter-scheme consumption datamart – the DCIR) from the National Inter-scheme Health Insurance Information System (SNIIRAM); data from the Information Systems Medicalization Program (PMSI); the reference beneficiaries (IR_IMB_R); the pharmacy repository (IR_PHA_R). The SNDS data that can be processed in the context of this request relate to data whose maximum historical depth is five years. The Commission notes that this historical depth has been scientifically justified in the application file. The Commission also notes that the company Clinityx will process approximately 240 variables

from the SNDS for the purpose of building a data lake intended to bring together all the data relating to the same patient from different sources. After this step, the warehouse will only contain the data strictly necessary for the operation of the Magellan tool. The variables or the joins intended to gather the data of the same patient, to calculate the cost of a care or to detect anomalies, will then be destroyed. The Commission notes that less than 35% of the variables transmitted by the CNAM will therefore be fed into the Magellan warehouse. Finally, it notes that it submitted, in support of its request, an expression of needs specifying in particular the list of these variables. The Commission considers that the data whose processing is envisaged are adequate, relevant and limited to this which 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 retention period of the data: The personal data of the SNDS cannot be the subject of outside of Clinityx's secure bubble. Only anonymous results can be exported. The retention period of the data in the secure bubble must be limited to the period necessary for the implementation of the processing, which cannot be more than five years, from the effective access to data. Each time the data is updated, the oldest data will be anonymized or deleted. The Commission considers that this data retention period does 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 the data: Only the data controller and the persons authorized by him have access to the data within the framework of the implementation of this processing. The data controller keeps up-to-date documents indicating the competent person(s) within it to issue the authorization to access the data, the list of persons authorized to access this data, their respective access profiles and the procedures for allocation, management and control of authorizations. These categories of persons are subject to professional secrecy under the conditions defined by Articles 226-13 and 226-14 of the Criminal Code. The qualification of authorized persons and their access rights must be regularly reassessed, in accordance with the procedures described in the authorization procedure established by the data controller.

The Commission notes that many organizations (health authorities, public health institutions, companies in the health products sector, patient associations, federations hospitals or prevention or care establishments), with the exception of those mentioned in 1° of A and 1°, 2°, 3°, 5° and 6° of B of I of Article L. 612-2 of the Monetary and Financial Code as well as the insurance intermediaries mentioned in Article L. 511-1 of the Insurance Code, may, in compliance with the provisions of the Data Protection Act, to be recipients of the aggregate indicators calculated by the Magellan tool.

On the information of the people: The people concerned are informed of the implementation of the SNDS and the possible reuse of their personal health data according to the methods defined by

article R. 1461-9 of the CSP. The Commission recalls that the provisions of Article 69 of the Data Protection Act are applicable to all processing carried out using data from the SNDS. In accordance with the provisions of Article 14 of the GDPR, in the event that the provision of individual information proves impossible, requires disproportionate effort or seriously compromises the achievement of the processing objectives, appropriate measures must be implemented by the data controller in order to protect the rights and freedoms, as well as the legitimate interests of the person concerned, including by making the information publicly available. In this case, an exception will be made to the principle of individual information of persons and appropriate measures must be implemented by the data controller in order to make the information publicly available concerning the constitution of this warehouse. The Commission notes that a transparency portal dedicated to the Magellan warehouse (via the Semaphore tool) will be set up by the company Clinityx. An information note relating to the constitution of the warehouse and its operation will be published on this website. The Commission also notes that each user of the Magellan tool must complete an information sheet containing all the information provided by Article 14 of the GDPR and that this information sheet will be published on the transparency portal prior to requesting the tool. All the information notes published on the transparency portal will include all the information provided for by the GDPR. The Commission recalls that 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 studies. Research, study or evaluation projects carried out using data from the Magellan repository must be registered in the public directory of the PDS. The Commission also takes note of Clinityx's commitment to register the warehouse in the public directory of the Health Data Platform. Finally, the Commission asks that it be sent a report every three years on the operation of the warehouse and on the research carried out using 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 data subjects: The rights of access, rectification, erasure, limitation of processing, and opposition are exercised by the person concerned with the director of the PDS or the director of the body managing the compulsory health insurance scheme to which the person is related, in accordance with the provisions of Article R. 1461-9 of the CSP. The Commission considers that the procedures for exercising the rights of the persons concerned do not call for any other comments. The technical infrastructure of the person responsible for implementing the Magellan warehouse, used for hosting SNDS child systems, has been analyzed by the Commission on various occasions, in particular in the context of previous authorization applications. responsible for processing carried out and

transmitted in support of the authorization request an impact analysis relating to data protection specific to the creation of the Magellan warehouse, as well as a risk analysis on the security of the systems of information. An approval of the secure bubble was also carried out by the approval authority on December 20, 2021, in accordance with the decree of March 22, 2017 relating to the security baseline applicable to the SNDS. This approval decision is only valid until January 31, 2023. It must therefore be renewed before this date, if the processing were to continue beyond this deadline. Technical and organizational measures have been planned by the responsible in order to partition the different extractions of the SNDS that can be stored within their technical solution. Separate environments, based on software containerization solutions, are implemented in particular to prevent any data merger. The query tool as well as the data on which this tool is based will also be partitioned thanks to the use of these solutions. The minimized data from the SNDS will be transmitted by the National Health Insurance Fund (CNAM) via a hard disk encrypted whose algorithms and key management methods comply with Annexes B1 and B2 of the General Security Framework (RGS). Health 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 exclusively subject to the laws and jurisdictions of the European Union. This data will also be encrypted in transit. Finally, the backups will be encrypted at rest. A multi-factor authentication including a password in accordance with the deliberation n° 2021-012 of January 19, 2017 adopting a recommendation relating to passwords, or any other subsequent update of this recommendation, is required for all data access and warehouse administration. Administration bastions allow connections to be traced. The Commission also notes that technical and functional traces will be kept for a period consistent with its recommendations and backed by a proactive mechanism for regular monitoring. The export of data outside the Magellan warehouse will consist exclusively of statistical reports that do not allow any re-identification of persons, and which will be sent exclusively to data controllers following requests made via the Magellan tool. To this end, a minimum threshold of eleven individuals will be retained for each aggregation. This verification prior to the allocation of access to the query tool may be carried out via data accessible in a professional directory kept up to date, or via enrollment carried out in person. The Commission notes that users external to Clinityx will only have access to statistical reports that do not include personal data. The Commission nevertheless recalls that the data controller must carry out an analysis to demonstrate that its anonymization processes meet the three criteria defined by Opinion No. 05/2014 on anonymization techniques adopted by the Article 29 group (G29) on April 10, 2014. If these three criteria cannot be met, an in-depth analysis of the risks of identification must be carried out by the data controller in order to demonstrate that the latter,

with reasonable means, are non-existent. The security measures described meet the requirements provided for. ues by 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 latter to carry out a regular reassessment of the risks for the persons concerned and an update, if where appropriate, of these security measures. Under these conditions, the Commission authorizes the company Clinityx to implement the processing of personal data for the purpose of setting up a health data warehouse called Magellan, for a period of ten years.The

PresidentMarie-Laure DENIS