DELIBERATION n°2018-369 of DECEMBER 20, 2018Commission Nationale de l'Informatique et des LibertésNature of the deliberation: AuthorizationLegal status: In force Date of publication on Légifrance: Wednesday March 27, 2019Deliberation n° 2018-369 of December 20, 2018 authorizing the company Compugroup Medical Solutions to implement automated processing of personal data for the purpose of a health data warehouse (Request for authorization no. 2135377) The National Commission for Computing and Liberties, Entry by the company Compugroup Medical Solution a request for authorization concerning automatic processing of personal data for the purpose of a health data warehouse; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing 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 with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC" (general regulation on data protection); Having regard to Law No. 78-17 of January 6, 1978 amended relating to data processing, files and freedoms, in particular its articles 8-II-8° and 54; Considering decree n° 2005-1309 of October 20, 2005 amended taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to the file and its supplements, in particular the impact analysis relating to data protection; On the proposal of Mrs Valérie PEUGEOT, commissioner, and after having heard the observations of Ms. Eve JULLIEN, Deputy to the Government Commissioner, Makes the following observations: Data controller The company Compugroup Medical Solutions, a simplified joint stock company (hereinafter, the company CGM or CGM), offers prescription assistance software intended to health professionals. On the legal basis and purpose CGM plans to create a pseudonymised health data warehouse for public or private organizations for the purpose of conducting observational studies in the field of health. The repository is intended to allow observational studies to be carried out on pathologies or care practices commissioned by public (such as institutes or research centers) or private (such as pharmaceutical laboratories) organizations from CGM. More specifically, observational studies will focus on the evaluation of care practices, the effectiveness of a drug over a defined period or the establishment of statistics from previously anonymized data in order to produce activity indicators. warehouse is made up of data transmitted, in pseudonymised form, by health professionals using the AxiSanté or HelloDoc software packages published by CGM. CGM generates from this data aggregated and anonymized results, intended for public or private organizations wishing to carry out observational studies in the field of health. A committee is responsible for examining the research projects of CGM's customers. in order to guarantee the character of public interest of the future uses of the data. This committee will be managed

by a healthcare professional, a CGM employee, and will be made up of people from outside the company. The legal basis for processing is Article 6, 1. f) of the General Data Protection Regulation (hereinafter GDPR), legitimate interests pursued by the controller. The Commission considers that the purpose of the processing presented is determined, explicit and legitimate, in accordance with the provisions of Article 5-1-b of the GDPR. It considers that it is necessary to apply the provisions of article 8-II 8° and 54 of the law of January 6, 1978 as amended, which subject to authorization processing involving data relating to health and justified, such as in this case, by the public interest in that the warehouse would make it possible to know the evolution of the care of the population suffering from the same pathology and to act on the practices of care in terms of policy of health. The Commission would like to point out that the future uses of the data contained in this warehouse fall within the framework of the provisions of Chapter IX of the law, which also requires that each request for research, study or evaluation meet a requirement of public interest. Thus, the Commission considers that the use of the data contained in the processing that will be implemented by CGM cannot, by analogy with the "prohibited" purposes of use of the national health data system (SNDS), be exploited for purposes of promoting health products to 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 group 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 (art. L. 4113-7 of the Public Health Code). Finally, the Commission recalls that the processing of personal health data which will be implemented subsequently, for research, The study and evaluation in the field of health are separate processing operations which must be subject to specific formalities under section II of chapter IX of the "IT and Freedoms" law. On the data processed The data in the warehouse relate to patients cared for by health professionals using, as part of their activity, the software published by the data controller, as well as to health professionals. to patients are the following: identification data: gender, age group, unique identifier generated from surname, first name, date and rank of birth, sex and department; health data: biology data, pathologies, prescription information, date of last consultation with a specialist, smoking status, physical activity, vaccination. Data relating to healthcare professionals is the surname, first name, professional address and RPPS number. The Commission notes that the file specifies that no processing of the NIR is envisaged by the company CGM. The Commission considers that the data whose processing is envisaged is 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 regulations. On the recipients The customers targeted by CGM are industrialists in the health or public research organisations. The Commission notes that CGM's customers will not receive any individual data relating to healthcare professionals' patients. Only CGM will be able to analyze this data in pseudonymised form and only envisages communication of results in anonymised form within the meaning of the criteria of the G29 opinion. authority of CGM and CGM's subcontracting company. The Commission considers that the categories of recipient do not call for observation. On information and the right of access With regard to patients: Health professionals will be responsible for contractually to inform their patients of the processing of data concerning them within the framework of the warehouse, as well as to allow the exercise of the rights of access, rectification and opposition which are recognized to them. It is expected that the persons be informed individually by giving each of the patients concerned a leaflet and by posting a document in the waiting or reception room of the medical office. The Commission notes that the exercise of the patient's rights of access, rectification and opposition will be exercised with the health professional in charge of their monitoring or with the company Compugroup. It takes note of the deletion of all the data collected in the event of the exercise of the right of opposition. With regard to healthcare professionals: The software published by CGM provides for the prior information and collection of the healthcare professional's consent before the installation of the module allowing pseudonymization and the transfer of data to the warehouse. The rights of persons concerned exercise with the data protection officer of the controller by sending an e-mail or letter. GDPR. Subject to this reservation, it considers the methods of information and exercise of rights satisfactory. On security measures The data collected by healthcare professionals is uploaded to the warehouse from a module specifically developed in conjunction with the practitioners' software. The data that is extracted and sent to the centralized database on the CGM Data server is pseudonymized. A unique identifier associated with the patient was constructed from several fields added to a random variable with an SHA 256 type hashing method. The pseudonymized database is centralized and hosted by a subsidiary of the data controller whose infrastructure has obtained HDS approval. The data is transmitted to the warehouse via an encrypted communication channel (HTTPS). The data is then subject to anonymization (generalization technique by aggregation and k-anonymity). The Commission recalls that, to avail itself of the anonymity of a data set, the data controller must comply with the three criteria of Opinion No. 05/2014 on anonymization techniques adopted by the group of Article 29 (G 29) on April 10, 2014. This compliance needs to be reviewed regularly in light of developments in anonymization and re-identification techniques. In addition, the Commission calls on the

data controller to be vigilant as to the presence of identifying data that may be found in documents held in non-text formats. Users are authenticated by means of a password. The Commission recalls that, in accordance with its deliberation n°2017-190 of June 22, 2017 modifying the recommendation relating to passwords, it requests that the latter be longer minimum of twelve characters and are composed of uppercase letters, lowercase letters, numbers and symbols or between eight and eleven characters, are composed of three of the four aforementioned possibilities and associated with an access restriction in the event of successive errors (temporary account blocking, possibility of new attempts after an incremental waiting period, etc.). clear. The actions of users accessing the warehouse are subject to traceability measures. A partitioning of processing is achieved in particular by means of a separation of network communications. A backup policy is implemented. 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 other characteristics of the processing The data are kept for 6 months following the end of the research project carried out and then archived for 10 years. The Commission considers that these data retention periods do 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, in accordance with this deliberation, the company Compugroup Medical Solutions to implement the processing described above, and recalls that the processing of personal data which will be implemented subsequently for the purposes of research, study or evaluation in the field of health are separate processing operations which must be subject to specific formalities provided for in section 2 of chapter IX of the law.For the President The Deputy Vice-PresidentMarie-France MAZARS