Deliberation 2018-359 of December 13, 2018 National Commission for Computing and Liberties Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Wednesday March 23, 2022 Deliberation No. 2018-359 of December 13, 2018 providing an opinion on a draft decree in Council of State of the Ministry of Solidarity and Health relating to medical information departments (request for opinion no. 18023418) health of a request for an opinion concerning a draft decree in Council of State relating to medical information departments; Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automated 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 individuals with regard to the processing of personal data nel and the free movement of such data, and repealing Directive 95/46/EC; Having regard to Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms; 2018-493 of June 20, 2018 relating to the protection of personal data; Having regard to the public health code, in particular its articles L. 6113-7, L. 6145-16 and R. 6113-1 and s. ;Given the commercial code, in particular its articles L. 823-9 and s. ; Considering the decree n° 2005-1309 of October 20th, 2005 modified taken for the application of the law n° 78-17 of January 6th, 1978 relating to data processing, files and freedoms; Considering the file and its complements; On the proposal of Mr. Alexandre LINDEN, commissioner, and after having heard the observations of Mrs. Nacima BELKACEM, government commissioner, Issues the following opinion: Article 11-4°-a) of Law No. 78-17 of January 6, 1978 as amended, of a request for an opinion on a draft decree from the Council of State relating to medical information departments. In October 2013, following a series of checks carried out by the Commission, several healthcare establishments received formal notices for having organised, as part of a so-called coding optimization service, the access by external service providers to the medical files of patients cared for in these establishments. series of checks revealed that, within the framework of the analysis of the medical activity incumbent on them, the health establishments, by soliciting external service providers, had recourse to practices disregarding the provisions of the law "Informatique et Libertés" and those of the public health code relating to the organization of the medical information department (DIM). On the occasion of the adoption of law n ° 2018-493 of June 20, 2018 relating to the protection of personal data, a modification was made to article L. 6113-7 of the public health code (CSP) to give competence to the regulatory power to determine "the methods of organization of the medical information function, in particular the conditions in which personnel placed under the authority of the responsible practitioner or statutory auditors acting under the legal mission of certification of the accounts (…) may contribute to the processing of data". The draft decree submitted is being examined by the Commission

aims to clarify these organizational methods. In particular, it authorizes and supervises access to patients' medical records for the benefit, on the one hand, of external service providers, for their missions of developing the program for the medicalization of information systems (PMSI) and optimizing the coding of acts and, on the other hand, auditors.On the authorization of access by external service providers and auditors to the medical files of patientsArticle 1 of the draft decree aims to authorize access by service providers external auditors and auditors to patients' medical files for the purpose of analyzing the activity of health establishments, "within the strict limits of what is necessary for their missions". The Commission recalls that the information contained in the files medical data constitute personal health data in accordance with the provisions of Article 4-15) of the aforementioned Regulation (EU) 2016/679 (hereinafter GDPR). It observes that under Article L. 1110-4 of the CSP, these categories of data collected by professionals in health establishments, during an act of prevention, diagnosis or treatment are protected by medical secrecy, except in the cases of derogation expressly provided for by law. It emphasizes that only a legislative measure is likely to render inapplicable the provisions of the Criminal Code relating to the penalties attached to the disclosure of information of a secret nature by a person who is the depositary thereof, either by status or profession, or because of a temporary function or mission. The Commission notes that Article L. 6113-7 of the CSP, in its version resulting from the law of June 20, 2018 referred to above, provides a legal basis for the determination, by regulatory means, of the methods of organization of the medical information department. Consequently, it considers, subject to the assessment of the Council of State, that the draft decree, insofar as it authorizes access by external service providers and commissioners accounts to health data contained in medical files, provides a legal basis for this access. The Commission considers that external service providers and auditors are therefore persons authorized to to process health data and to access it exclusively for their missions, in compliance with the provisions of the GDPR and the law n ° 78-17 of January 6, 1978 as amended. On the terms of access for external service providers and commissioners accounts data from patients' medical recordsArticle 1 of the draft decree regulates the terms under which access by external service providers and auditors to the health data contained in medical files must take place:external service providers and the auditors have access to the data, within the strict limits of what is necessary for the exercise of their missions; the traces of any access and consultations, creations and modifications of data relating to patients are kept for a period of six month by the establishment. Regarding the access of auditors, the Ministry of Solidarity and Health specified that, in accordance with the provisions According to Article L. 823-9 of the Commercial Code, their mission is to certify, by justifying their assessments, that the annual accounts are regular

and sincere. The auditors must, for the collection of income related to the stay, base their assessment on the procedures for implementing internal control and, in particular, ensure that the billable activity is taken into account in an exhaustive manner and that it is valued correctly; due to activity-based invoicing, medical care serves as the basis for coding pathologies, which involves checking the medical files in which these elements are collected. The Ministry also indicated that, to carry out this work, the auditors may be assisted, under their responsibility, by experts of their choice and, in particular, call in an expert medical information doctor, as well as an expert in information systems. He also specified that the auditors will not be empowered to create and modify data relating to patients. If the Commission therefore does not question the need for the auditors to verify the fair valuation of the medical activity in the context of the audit assignments they carry out – and, to do this, to access health data –, she wonders about the methods adopted, in particular the interest that they access to directly identifying data appearing in patients' medical files. is not sufficiently supervised. It requests that the auditors not have access to the patient's identification data (surname, first name, age, date of birth, address) and that they only have access to pseudonymised data within the meaning of the 4-5) of the GDPR. The Commission also requests that the access permissions put in place be effectively restricted to reading and, consequently, that the draft decree expressly mention the impossibility for the to create and modify data relating to patients. On the qualification of external service providers and auditors and their obligations The Ministry indicated that external service providers for their missions of developing the PMSI and optimizing the coding of acts, and auditors for the review of the revenue cycle, may process directly or indirectly identifying personal health data transmitted by health establishments requesting them. Article 1 of the draft decree provides, in this respect, the framework for this processing by imposing: a prohibition on keeping the data made available by the establishment, beyond the duration strictly necessary for the missions which have been entrusted to them within the limits of their contract; the use of an approved or certified health data host, when health data is hosted. With regard to external service providers, the Commission indicates that these , by contributing directly to the coding of acts or to operations to optimize this coding, intervene on behalf of healthcare establishments. As such, it considers that they fall within the category of subcontractors within the meaning of Article 28 of the GDPR. The Commission points out that, given the sensitivity of the data, they will have to put in place sufficient guarantees as to the implementation of technical and organizational measures so that the operations of analyzing medical activity on behalf of healthcare establishments meet the requirements of the GDPR and guarantee the protection of the rights of the patients concerned by the processing of their data. CSP, the legislator opened the possibility for the ministry to

allow the latter, under their legal mission of certification of accounts, either to access the medico-administrative databases of health establishments, or to obtain an extraction from them. , the Commission considers that they are responsible for the processing of personal data thus implemented. Nevertheless, it indicates that the processing operations, taking into account the general principles applicable to the protection of the processing of personal data, must as a priority be carried out in the form of a simple consultation of the medico-administrative databases. As such, the Commission recalls that the statutory auditors must comply with all the general principles applicable to the protection of the processing of personal data, as they result from Article 5 of the GDPR, and in particular those relating to minimization and safety. In accordance with the provisions of Articles 24 and 25 of the GDPR, the auditors must implement all appropriate technical and organizational measures, both when determining the means and when implementing the processing itself, to meet GDPR requirements and protect the rights of individuals; they must ensure that only data strictly necessary for the exercise of their account certification missions is processed. As soon as the processing operations concerned are likely to create a high risk for the rights and freedoms of natural persons, an analysis impact on data protection must be carried out by the auditors in application of the provisions of Article 35 of the GDPR. The Commission also draws attention to compliance with the following security requirements: the processing must be implemented works within the framework of an information systems security policy; data exchanges must be encrypted; processing must provide for a procedure for managing personnel and authorizations in order to allow the processing of only data strictly necessary for the purpose , as required by Article 32-4 of the GDPR; the data must be deleted from the systems when they are no longer subject to processing nt, in accordance with the duration of the contract; a traceability procedure must be implemented in order to allow the identification of the people who have accessed the data over a period of six rolling months (this is to allow the collection, exploitation , the securing of traces, the taking into account of all events, the management of traces, in particular with regard to their integrity and their backup as well as their regular use). In this respect, the Commission notes that the draft decree provides that the hosting of data by a third party must comply with the conditions set out in Article L. 1111-8 of the CSP (use of an approved or certified health data host). Finally, the Commission notes that the draft decree mentions that the statutory auditors cannot keep the data made available beyond the duration strictly necessary for the missions entrusted to them within the limits of their contract. Insofar as the Ministry indicates that the contractual duration of data retention may vary, the Commission wonders, in view of the particularly sensitive nature of the data and the need to retain a duration that complies with the requirements of Article 5-1 -e) of the GDPR, on the advisability of

adopting a shorter retention period, providing for the deletion of the data as soon as the certification procedure is completed.

The other provisions of the draft decree do not call for comments from the Commission.For The PresidentDeputy

Vice-PresidentMarie-France MAZARS