Deliberation 2020-025 of February 6, 2020 National Commission for Computing and Liberties Nature of the deliberation: Opinion Legal status: In force Date of publication on Légifrance: Saturday July 11, 2020 Deliberation No. 2020-025 of February 6, 2020 providing an opinion on the request for approval presented by the Hospital IT Purchasing Center, candidate for the hosting of personal health data

(Request No. 18004560)

The National Commission for Computing and Liberties, Seizure for opinion by the Minister for Solidarity and Health of the application file for approval of the Hospital Computing Purchasing Center, candidate for the hosting of data from personal health; 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 , and repealing Directive 95/46/EC (General Data Protection Regulation); Having regard to the Public Health Code, in particular its Articles L. 1110-4, L. 1111-8 et seq. and R. 1111-1 to R. 1111-15-1; Having regard to the social security code, in particular its article L. 161-36-1; Having regard to law n° 78-17 of January 6, 1978 as amended relating to data processing, files and to freedoms; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to the data processing, files and freedoms; Considering the file and its supplements; On the proposal of Mrs Valérie PEUGEOT, Commissioner, and after having heard the observations of Mrs Nacima BELKACEM, Government Commissioner, Makes the following observations: The National Commission for data processing and freedoms is seized for opinion by the Minister of Solidarity and Health, in accordance with the provisions of Article R. 1111-10 of the Public Health Code, of the application for approval presented by the Centrale d purchase of hospital IT, a candidate for the hosting of personal health data. The Commission must decide, in accordance with said provisions, on the guarantees presented by the candidate for approval in terms of with regard to the processing of personal health data and the security of this data. The Commission recalls that whatever its opinion, issued in view of the file communicated to it, It has the power to carry out checks with any data controller in order to carry out any necessary verification operation, in accordance with the provisions of articles 19 of the law of January 6, 1978 as amended and 16 and following of decree n ° 2019-536 of the May 29, 2019 taken for application of this law. Issues the following opinion under these conditions: Candidate host: The candidate for approval is the Central Purchasing Center for Hospital Computing (CAIH), an association under the law of 1901 bringing together health establishments, social and medico-social establishments, groups formed by these establishments, or public agencies and establishments operating in

these sectors. It has 1,150 members. The applicant for accreditation offers a personal health data hosting service from Microsoft's Office 365 software suite. Microsoft Ireland Operations Limited (MIOL) is identified as a subcontractor by the applicant. The Office 365 services covered by this application for approval are:Exchange OnlineSharePoint OnlineSkype Enterprise OnlineProject OnlineMicrosoft TeamsOne Drive EnterpriseAs well as the Azure technology bricks to ensure the proper functioning of these services with the exception of the Active directory service Directory. The host offers this service to its members, which are public health establishments. The candidate does not offer a feature for direct access to data by the persons concerned. Commission requirements: the hosted data is generally stored on Microsoft servers with HDS certification. However, this is not the case for data linked to the Office Exchange service which is stored in Finland and Austria and therefore does not fall within the scope covered by Microsoft's HDS certification; the scope explicitly excludes the service of 'Azure Active Directory (Azure AD) to provide Microsoft cloud-based identity and access management. However, the Office 365 services offered by the candidate directly use Azure AD. Its absence from the perimeter raises questions concerning the associated measures, in particular the location of authentication data linked to the Active Directory; the candidate does not sufficiently fulfill its duty to advise concerning the configuration of the Active Directory, telemetry and generally on the measures to improve security and to configure the security modules provided by the subcontractor. Indeed the candidate appears as a simple interface between the Microsoft subcontractor and the end customer. However, the services made available by Microsoft seem relatively generic and the candidate does not seem to bring additional elements to the technological bricks provided by the subcontractor. This results in many questions concerning the duty of advice of the candidate who transfers many security requirements to his client but does not seem able to support him in the implementation of these measures; for example, the candidate transfers to his client the implementation of an identification and authentication policy, appropriate training, data traceability, a backup, restoration and archiving policy, a continuity policy of activity and recovery of activity, of an operational security policy applicable to its bastion; the candidate does not present an organization chart specific to its organization. The presence of an information systems security officer (RSSI) within the candidate's organization or that of the subcontractor is mentioned without further details. Organizational charts presenting the organization of the staff of the subcontractor in charge are presented but these appear to be a generic team associated with Office 365 and do not include the doctor of the host. The candidate's staff in charge of supporting the client is not presented, which reinforces doubts about the candidate's ability to support his clients; The information systems security policy complies with the criteria

required by the Commission. procedure for managing personnel and authorizations complies with the criteria required by the Commission, subject to the following reservations: the candidate transfers to his client the responsibility of defining the policy for managing authorizations; the candidate indicates that Microsoft personnel do not access not to customer data, nor to hosted health data. This point is applicable to C.A.I.H. . However, the applicant indicates in its documentation that such access may be permitted in the event of a technical or security incident. The candidate presents numerous guarantees making it possible to supervise this type of access (fine management of authorizations, reinforced traceability, regular audits, etc.); such access is the subject of information from the doctor of the host who also has access to associated traces. However, such measures seem too permissive. Any access to data by the staff of the host in the event of a technical or security incident must be the subject of prior information from the host's doctor and be carried out under his direct supervision; the candidate presents different categories of people who may have access to the data under the conditions mentioned above. The terms of access and in particular the place(s) from which this access takes place are not specified. The Business Continuity Plan complies with the criteria required by the Commission subject to the following reservations: the candidate put in place backup encryption mechanisms to ensure the confidentiality and integrity of the data. The documentation seems to indicate that encryption key management is devolved to the customer, but this deferral is not done contractually. The hosting company's duty to advise does not seem to be fulfilled in this regard; the backup hosting location is not explicitly mentioned in the file. The candidate only indicates that the backups are located within Microsoft data centers; a crisis unit is present within Microsoft teams. This works in conjunction with a crisis unit within the candidate. However, the activities and missions of this last committee are not presented. The traceability procedure complies with the criteria required by the Commission. The rights of the persons concerned are respected in accordance with the requirements of the Commission, subject to the following reservations: the candidate must take into account in all contractual documents, the new wording of article L. 1111-8 of the public health code, modified by law n° 2016-041 of January 26, 2016 on the modernization of our health system , which replaced the collection of the express consent of the person concerned for the hosting of their health data by information accompanied by a right of opposition. the candidate must attach to the contract a model information note in accordance with Articles 13 and 14 of the General Data Protection Regulation and mentioning the procedures for exercising the rights of the data subject. The staff concerned are not trained in accordance with to the requirements of the Commission: training followed by Microsoft staff is presented but these do not mention the specific nature of health data; the candidate passes on to his client

the responsibility for setting up suitable training for his users but does not seem to propose a duty to advise in this respect.Opinion of the Commission: UnfavourableFor the President

Deputy Vice-President Sophie LAMBREMON