DELIBERATION n°2018-296 of JULY 19, 2018National Commission for Computing and LibertiesNature of the deliberation: AuthorizationLegal status: In force Date of publication on Légifrance: Tuesday, October 23, 2018Deliberation n° 2018-296 of July 19, 2018 authorizing the NOVARTIS laboratory Pharma SAS to implement automated processing of personal data with the aim of guaranteeing the traceability of the personalized medicine KYMRIAH, entitled CELLCHAIN LINK. (Application for authorization no. 2185121)The National Commission for Computing and Freedoms Seizure by the company NOVARTIS Pharma SAS of a request for authorization concerning the automated processing of personal data with the aim of guaranteeing the traceability of the personalized medicine KYMRIAH, entitled CELLCHAIN LINK; Having regard to convention n ° 108 of the Council of the Europe for the protection of individuals with regard to the automatic processing of personal data; Having regard to the regulation nt (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); Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular article 8-II 8° and 54; Considering the modified decree n° 2005-1309 of October 20, 2005 taken for the application of law n ° 78-17 of January 6, 1978 relating to 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: Data controller Novartis Pharma SAS (hereinafter, NOVARTIS). On the legal basis and purpose The Novartis Pharma SAS laboratory wishes to implement automated processing of personal data as part of the provision for patients of the drug called Kymriah. This medicine is intended to treat children and adults suffering from certain forms of leukemia and lymphoma. The drug Kymriah is an autologous drug, made from cells taken from the patient for whom the treatment is intended. It is exempted within the framework of a temporary authorization of use (ATU). The processing of the data thus aims to: guarantee a rigorous chain of identification throughout the manufacturing process of the personalized drug; ensure the absence of any possibility of interchangeability of the cells collected or of administration of the drug to another patient. Furthermore, as the drug does not benefit from marketing authorization (AMM) in France, its use is subject to a close monitoring procedure by the ANSM, particularly in terms of pharmacovigilance. is accompanied by a protocol for therapeutic use and collection of information to enable: monitoring and monitoring of patients treated; the relevant information on the use of this medicinal product in order to ensure its proper use, with in particular the summary of product characteristics (SPC) which sets the criteria for use of the

medicinal product, the procedures for informing patients about the medicinal product and on the ATU; the definition of the criteria for the use and dispensing of the medicinal product as well as the procedures for monitoring the patients treated; the definition of the role of all the actors of the device.The legal basis of the treatment is the respect of legal and regulatory obligations, which aims to ensure the traceability of the process and to better monitor the undesirable effects.Thus this basis is the guarantee of standards high standards of quality and safety of health care and medicines, within the meaning of Article 6-1-c of the GDPR. The Commission considers this purpose to be determined, legitimate and explicit 5-1-b of the GDPR. It considers that the provisions of article 8-II 8° and 54 of the law of January 6, 1978 should be applied. amended, which require authorization for processing involving data relating to health and justified, as in this case, by the public interest.On the data processedThe data processed concern patients in a therapeutic impasse to whom the medicine has been prescribed. The data collected from patients are: name; first name ; date and place of birth; professional status; weight; pathologies and conditions; data relating to care; biological data relating to the collected cells. Specific identifiers are used during transport: transport document (“Waybill”); batch number (“Batch ID”); serial number of the Dewar container. These data are essential for the implementation of automated processing to ensure that the cells taken from the patient, transported again in order to be reinjected into him, are inseparably linked to a single and unique patient. The information collected in the context of pharmacovigilance is: surname; first name; postal and electronic addresses; gender; weight; height; date of birth or age at the time of the effect; information relating the administration of the drug; the adverse effect and its development. In addition, the identity of the doctor or health professional who observed the event will be collected as far as possible, as well as his e-mail address, telephone number telephone and fax number using the form provided by the ANSM. Concerning the request for a therapeutic use protocol and collection of information are collected: surname, first name, specialty, establishment, address, postal code, city, telephone, fax, email of the prescribing doctor and the hospital pharmacist. The Commission considers that 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 Article 5-1-c of the GDPR. On recipients Novartis Pharma SAS does not have default access to personal data. Novartis Pharma SAS may have access to the data in order to manage potential complaints related to the product or in the event of the exercise of rights over said personal data. Within Novartis will have access to the data, the authorized persons and insofar as their missions l require the following entities: Novartis Pharmaceuticals Corporation: who will have access to the data and T cells in order to manage the manufacturing process of Kymriah / CTL019; Novartis Pharma AG:

will have access to the data the customer service, ordering/planning departments as well IT department (for IT support reasons); Novartis Pharma Gmbh: will have access to data to manage customer service and ordering processes and who will be responsible for bringing the product to market for EU countries; Novartis Pharma SAS: may have access to the data in order to manage potential complaints related to the Product or in the event of the exercise of rights over said personal data les.Within each subsidiary entity of Novartis SAS, access is defined according to the role of the employees. There is no default access; you must justify the need for this access, follow the required training and complete an access form. The scope of access will then depend on operational needs. The third parties who may have access to the data: the establishments where the patient is treated and who enter the data into the Novartis IT system in order to ensure the maintenance of the identification chain; the approved/certified health data host; Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V., as a corporate entity for the Fraunhofer Institute for Cell Therapy and Immunology ("IZI"), which manufactures Kymriah/CTL019 on behalf of Novartis, will have access to patient data for product manufacturing and storage of Cells T and samples; Accenture AG Fraumünsterstrasse 16, 8001 Zürich, Switzerland and Accenture HDC 4 - Mantri Cosmos SEZ, Nanakramguda Village, Gachibowli, Serilingampally Mandal, Randa Reddy District, Telangana 500008: will access the data to provide IT support in their capacity as 'system administrator. They will only be able to access the data upon justified change request, documented and approved by Novartis. In the event of access by an administrator, he must enter the VPN, use the privileged access tool (PAM) recording the operations and authenticate himself. The administrator will not see the patients' personal data, which remains in the Cell Chain solution. Concerning data access authorizations: authorization profiles define the functions or types of information accessible to a user; persons justifying their need to access the data benefit from an authorization; with regard to third parties, the “Cell & Gene Therapy” department of Novartis identifies, approves and certifies external users. Certified users are then provisioned and de-provisioned into the system at the request of Novartis operational managers, using the integrated security architecture between Novartis and Salesforce. The Commission considers that the categories of recipient do not call for observation. On information and the procedures for exercising rights With regard to patients: the patient will be given an information and consent form by the doctor prescriber with the explanations necessary for their proper understanding. The form after a careful reading of the patient (his legal representative or the trusted person he has designated) must, to consent, date and sign at the bottom of the form; the form contains the following information: the identity of the data controller; the data collected; the purposes of the processing; the persons having access to the data; information relating to national or

international data transfers; the security measures put in place; the storage of the data and the medicinal product; the form contains the following indications: the right to access his personal data and, if he considers that information concerning him/her child is incorrect, obsolete or incomplete, to request its rectification or updating; the right to request the erasure of their personal data or the limitation of their use for specific processing purposes; the right to withdraw consent to the use of their personal data and cells at any time, without affecting the validity of the process prior to such withdrawal; the right to object, in whole or in part, to the processing of their personal data. To exercise their rights, the patient will have access to an e-mail address, a postal address and may, if necessary, send a request to the data protection officer. Finally, the patient will be able to exercise his rights through the prescribing doctor. As regards health professionals (prescribing doctors and dispensing pharmacists), they are informed of the processing of their personal data in the e-mail sent to them at the time of the implementation training in the center to which these health professionals are attached. The information issued to them includes the information provided for by Regulation 2016/679 of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and by the Data Protection Act, in particular the procedures for exercising the rights of access and rectification. that these information and exercise of rights measures are satisfactory. On security measures The Commission notes that the data controller undertakes to host all health data with an approved or certified host in accordance with the provisions of the Public Health Code. The Commission considers that the nature of the data requires that they be subject to encryption measures in accordance with Appendix B1 of the general security reference system both at the level databases than backups. The Commission requests that access permissions be granted for a determined and limited period, after hierarchical validation, that they be deleted as soon as a user is no longer authorized and that a review of the authorizations granted is carried out regularly. The Commission also requests that specific authorizations be provided for non-professional health personnel, so that they can only have access to non-identifying patient data. The Commission notes that the new Article L. 1110-4 of the public health code resulting from the law of 26 January 2016 on the modernization of our health system no longer provides for authentication by CPS or equivalent device approved by ASIP health and that the new article L. 1110-4-1 of the same code refers these authentication methods to compliance with interoperability and security reference systems approved by the Minister responsible for health after consulting the CNIL. Pending publication of the regulatory texts allowing the entry into force of these new provisions, the Commission requests that the authentication of health professionals take place by means of a CPS or an equivalent device approved by ASIP santé.The

Commission reminds the responsible nable to processing the need to set up a logging system making it possible to keep a trace of personal data consultation operations. to guarantee the confidentiality of data for the provision of files to external recipients. These conditions must be based on means ensuring the authentication of the recipients, the confidentiality and the integrity of the transmissions as well as a management of the authorizations allowing to attribute to the recipients the right to access only the data which are necessary for them. .On the other characteristics of the processingNovartis wishes to keep the health data for a period of 30 years. This duration is based on the European regulations applicable to this type of therapy. Initially, access to the data will be restricted to the Audit and Pharmacovigilance departments, if necessary, as well as any other person capable of justifying the need beyond a period of 3 years which corresponds to the duration life of a cell during which medical acts can be carried out. Secondly, the personal data, in particular all the identifiers used in the process, are kept to ensure the traceability required by the regulations. This traceability will make it possible to manage adverse events occurring in patients and any internal or external audits. Novartis also wishes to keep the data of healthcare professionals for a period of 15 years. The Commission considers that these data retention periods do not exceed those 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 NOVARTIS Pharma SAS to implement the aforementioned processing. For the President Deputy Vice-President Marie-France MAZARS