Deliberation 2022-042 of April 7, 2022Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday September 06, 2022NOR: CNIX2224126VDeliberation n° 2022-042 of April 7, 2022 providing an opinion on a draft decree relating to access to non-identifying data and the identity of the third-party donor taken pursuant to Article 5 of Law No. 2021-1017 of August 2, 2021 relating to bioethics (request for opinion no. ° 21022168) The National Commission for Computing and Liberties, Seizure by the Minister for Solidarity and Health of a request for an opinion concerning a draft decree relating to access to non-identifying data and identity the third-party donor taken pursuant to Article 5 of Law No. 2021-1017 of August 2, 2021 relating to bioethics; 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 or GDPR); Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms (data-processing law and freedoms); Having regard to article 5 of law n° 2021-1017 of August 2, 2021 relating to bioethics; Having regard to the Public Health Code; After having heard the report of Mrs. Valérie PEUGEOT, commissioner, and the observations of Mr. Benjamin TOUZANNE, government commissioner, CONSIDERING THE FOLLOWING CONTEXTUAL ELEMENTS: Article 5 of law no. 2021-1017 of August 2, 2021 relating to bioethics (law relating to bioethics) allows any person conceived by medically assisted procreation (MAP) with a third party donor, if they so wish, to access their majority at the identity, non-identifying data of the third party donor or all of its information. The following categories of people will be concerned by this system: persons born from an ART with a third-party donor; beneficiaries of an ART with a third-party donor; third-party donors, for whom a sub-distinction can be made between: third-party donors who were not subject to the provisions of the law on bioethics at the time of their donation (former third-party donors). For these, there is provision for a system allowing them to consent or not to the transmission of their data to persons born from ART; and third-party donors subject to the provisions of the new bioethics law at the time of their donation (new third-party donors). The donation of gametes and embryos will therefore henceforth be subject to the consent of the third-party donor so that his identity and non-identifying data may be revealed to the person born of assisted reproduction who has reached the age of majority. Third-party donors not subject to the new legislative provisions at the time of their donation may also consent to the communication of their data. These can appear spontaneously or be recontacted when a person born from an AMP requests access to their origins. The draft decree organizes access to their origins for people born

from an AMP with a third party donor by creating two separate data processing operations. A first processing operation, for which the Biomedicine Agency (ABM) is responsible pursuant to Article L. 2143-4 of the Public Health Code (CSP), allows the collection and the conservation of the data necessary for access to the origins of the persons concerned. to grant requests for access to origins made pursuant to Article L. 2143-5 of the CSP. CAPADD is responsible for this processing pursuant to Article L. 2143-6 of the CSP. These processing operations come under the GDPR. MAKES THE FOLLOWING OBSERVATIONS ON THE DRAFT DECREE On the general structure of the text: The law on bioethics has intended to allow people born from assisted reproduction with a third-party donor to have access to certain information relating to the latter, which requires the processing of data relating to health. In particular, concerning third-party donors, article R. 2143-12 provides in particular for the collection of: their height and weight; their general condition at the time of the donation, including their psychological condition. The draft decree specifies that the two envisaged processing, necessary for the performance of a task in the public interest or relating to the exercise of official authority vested in the data controllers, is based on Article 6-1-e) of the GDPR. In addition, the processing of health data that they involve is justified by reasons of important public interest, within the meaning of the provisions of Article 9-2-g) of the GDPR. The Commission agrees with this analysis. With regard to each of the processing operations implemented by the ABM and by the CAPADD: On the information and methods of consent of third-party donors to the communication of their so-called non-identifying data and their identity :The methods of consent of third-party donors to the communication of their so-called non-identifying data and their identity are detailed in section 4 of the draft decree. The draft article R. 2143-6 of the CSP, which draws the consequences of article L. 1244-2 of the same code, thus provides that the consent of the donor to the communication of his data to persons born of donation does not cannot be revoked as soon as the donation is granted. In the event that they have given their consent to the transmission of their data, this principle also applies to former third-party donors who have contacted CAPADD or who have been contacted again, in application of 5° and 6° of article L. 2143-6 of the CSP. Thus, their consent is no longer revocable from the effective communication of their data to the center where the donation was made. According to the details of the Ministry, third-party donors will be informed at the time of the donation of the processing of data concerning them, as well as of the impossibility of revoking their consent to the communication of the latter after attribution of the donation. The Commission invites the Ministry to provide for the transmission of this same information to former third-party donors by CAPADD, prior to the collection of their data by the donation center. On the rights of the persons concerned: With regard to the limitation of the rights to deletion and

opposition: The draft articles R. 2143-16 and R. 2143-21 of the CSP rule out a priori the option for the persons concerned to exercise their rights to the deletion of data and to opposition to processing. Asked about this point, the Ministry specified that it intended to apply Article 23-1-i) of the GDPR. In this respect, Article 23 of the GDPR requires a text in the law of the Union or of Member State to limit the scope of the rights provided for in Articles 12 to 22 of the GDPR, provided that such a limitation respects the essence of the fundamental rights and freedoms and that it constitutes a necessary and proportionate measure in a democratic society for guarantee in particular the protection of the data subject or the rights and freedoms of others (article 23-1-i) of the GDPR). The Ministry clarified that, in accordance with Article 23-1 of the GDPR, the rights to oppose and erase data may be waived to the extent that their limitation is necessary for the purposes of guaranteeing the right of access to origins. people born from assisted reproduction with a third-party donor. He underlined that: for third-party donors, the exercise of these rights is incompatible with the making of the donation, insofar as the latter is now subject to consent to the communication of its data to people born of an MAP; for ART beneficiaries, the exercise of these rights is incompatible with the realization of ART, and would require the revocation of consent to ART with a third-party donor. Thus, according to the Ministry, the exclusion of these rights makes it possible to guarantee the effectiveness of the right of access to origins. The Commission does not call this analysis into question since the exercise by the donor of the rights of erasure and opposition would indeed be such as to defeat the application of the law, which is to allow the person born of an AMP with a third-party power giver, if they so wish at some point in their life after reaching majority, gain access to their origins. However, in the absence of details from the Ministry, the Commission understands the project that the limitation of rights will also apply to persons born from an ART with a third-party donor. Aware of the consequences that the exercise of these rights by the person born of an ART with a third party donor, which would have the effect of a definitive renunciation of the right of access to his origins, the Commission takes note of this. It nevertheless recalls that this limitation must meet the conditions provided for in Article 23 of the GDPR and that the draft must be supplemented in order to contain the specific provisions provided for in 2. of this same article. The Commission further notes that the Ministry has undertaken to modify the decree so that it specifies that the persons concerned must be informed of the limitations made to their rights. Regarding the right to limitation of processing: Contrary to what is mentioned in the analysis of impact relating to data protection (AIPD) which excludes the option for data subjects to exercise their right to limitation, the draft decree does not provide any information on this point. According to the details of the Ministry, the exercise of this right, which would partially render data inaccessible for a certain period, would have

the effect of temporarily preventing the addition of a third-party donor to the ABM database and could lead to the refusal of a new donation or the use of a donation, since the ABM would not be able to ensure that the use of donation(s) from the same donor will not deliberately lead to the birth of more than ten children, in accordance with the provisions of Article L. 1244-4 of the CSP. the persons concerned for this reason. For example, the right to limitation could allow a third-party donor who considers that his data are inaccurate to have them rectified before communication to the person born of an ART. The Commission takes note of the ministry's commitment to clarify the draft decree in this regard. With regard to the rights of access and rectification: The draft articles R. 2143-16 and R. 2143-21 of the CSP provide for the exercise of the rights of access and rectification by the persons concerned. The Commission takes note of the fact that people born from assisted reproduction with a third-party donor and third-party donors making use of their right of access can only access, outside of the mechanism for access to origins, only the information that is own and which they themselves communicated. The ministry clarified that these methods also concerned the beneficiaries of an ART with a third-party donor. The Commission notes that the Ministry has undertaken to modify the draft decree on this point. It also invites it to add to draft articles R. 2143-16 and R. 2143-21 of the CSP the terms, where appropriate, following third-party donors and persons born from medically assisted procreation with a third-party donor making use of their right of access can only access the personal data which concerns them, insofar as the persons born of an AMP with a third-party donor will not themselves have communicated data concerning them beforehand to exercise their right. With regard to access to data and recipients: The draft articles R. 2143-14 and R. 2143-19 of the CSP specify the persons who can access the data for registration purposes , processing and storage. The Commission notes that the Ministry has undertaken to modify the draft decree, so that it specifies that the persons who may, under the authority of the data controller, record, consult and process the data are persons accessing to the processing and not to the data, insofar as they have writing rights. On the data processing implemented by the ABM: On the purposes of the envisaged processing: Article L. 2143-4 of the CSP provides for the implementation by the ABM of processing of personal data relating to third-party donors, their donations and persons born as a result of these donations as well as the identity of the recipients or couples. According to the draft article R. 2143-10, this processing, called Register of gamete and embryo donors, is intended to allow the persons concerned to access their origins and to allow statistical analyzes to be carried out at from the data included in the processing and previously pseudonymised. The Commission considers these specific, explicit and legitimate purposes within the meaning of Article 5 of the GDPR. Regarding the performance of statistical analyses, according

to the details of the Ministry, these analyzes will only be used for counting and statistical elements (for example , the number of donors enrolled during a study), from the raw data in the database. No extraction of personal data is envisaged at this stage. Access to these indicators must be subject to compliance with the right to know of authorized users and the authorizations put in place for each profile, as well as functional traces recording the author, the date and time of the operations carried out. In general and apart from these statistical analyses, if the processing data were to be extracted in order to reuse them for research, studies or evaluations in the field of health, these must be subject to prior formalities as provided for by the Data Protection Act. The Commission notes that the ABM has undertaken to submit a request for authorization to the CNIL if such research were to be considered. On the data whose processing is envisaged: The draft article R. 2143 -11 of the CSP describes the categories of personal data that will be processed by the ABM.Concerning the data relating to the identity of the persons concerned: The ministry has specified that their name at birth, first name, date of birth will be collected , sex, as well as their country of birth. The Commission requests that the exact nature of the data that will be collected be specified in the decree.Concerning the so-called non-identifying data of third-party donors:I of draft article R. 2143-12 lists the non-identifying data of the third-party donor that may be communicated to people born of donation if they so request. This data includes in particular the motivations for their donations. In its deliberation no. the data processed, admittedly non-nominative, is, in reality, indirectly identifying, both for third-party donors and for persons outside the MAP procedure who could be mentioned in the reasons for the donation (third party to the donation). Therefore, the transmission of this information alone to the person born from ART with a third-party donor is likely to enable him to re-identify the third-party donor and/or third parties to the donation. The Commission notes that measures aimed at preventing the risk of re-identification have been considered: firstly, third-party donors will be informed by the physician in charge of ART of the risks of re-identification attached to the completion of free text fields, as well as the associated verification procedure; secondly, by the verification by the ART center doctor of the form completed by the third-party donor at the time of the donation; finally, by the possibility for the doctor to enter the CAPADD in the event of doubt concerning the potentially re-identifying nature of the data (draft article R. 2143-9 of the CSP). The Commission welcomes the fact that the draft decree creates such a procedure to avoid the risks of re-identification, particularly with regard to third parties to the donation, which could be mentioned in the document detailing the reasons for the donation written by the third-party donor. It stresses the need to raise the awareness of doctors as well as people working within CAPADD on the notion of identifying data within the meaning of the applicable data protection texts. On the conditions for

informing the people concerned: According to III of draft article R. 2143-16 of the CSP: third-party donors will be informed of the processing of their data when they are taken in charge by the ART center, and when their consent is obtained; the beneficiaries of ART are informed by the doctor when they receive treatment under ART.As regards the information of third-party donors on the risk of re-identification:The Committee considered it necessary, in its deliberation n° 2019-097 of July 11, 2019 providing an opinion on a draft law relating to bioethics, to provide clear information to third-party donors on the possible risk of re-identification of third parties to the donation based on non-identifying data and in particular when writing the reasons for the donation. According to the details of the ministry, third-party donors will be informed of the nature of all the data collected and of the distinction between data relating to identity and non-identifying data through the intermediary information brochures. The Commission notes, however, that the information brochures do not contain any information on this subject. It therefore invites the Ministry to complete them. With regard to the information of persons born from an ART with a third-party donor: As regards the processing of data of persons born from an ART with a third-party donor, the information will be issued to the beneficiaries of the ART. Article L. 2141-10 of the CSP also provides that the beneficiaries of the ART are encouraged to anticipate and create the conditions that allow them to inform the child, before his majority, because it comes from a gift. The Commission notes that no provision provides for information measures with regard to persons born from assisted reproduction with a third party donor when they reach majority. In addition, individual information on the processing of data would amount to informing the because it was born of an MPA and therefore does not seem to be in line with the will of the legislator. Collective information will be made available by the ABM and the CAPADD. The Commission invites the Ministry to ensure the completeness of this information and to implement the appropriate means to allow its wide dissemination. On the updating and the right to rectification of data: With regard to the possibility of updating of the data provided for by article L. 2143-2 of the CSP, the draft article R. 2143-13 of the same code provides that the first names and sex of the persons concerned, as well as data relating to the family and professional situation from the third-party donor, may be the subject of an update request from the ART centers or the ABM. the situation of the donor (for example change of family situation or profession). A distinction is thus made between the updating of data and the right of rectification which, in its view, concerns erroneous or incomplete data which must be the subject of a corrective measure. The Commission nevertheless recalls that the right to rectification provided for in Article 16 of the GDPR aims to allow the rectification of inaccurate or incomplete data, the inaccuracy possibly also being due to a change in the situation of the persons concerned. It notes, moreover, that according to the draft decree, the

procedures according to which a request for updating can be made differ from those laid down concerning the exercise of the right to rectification. Taking note of the Ministry's uncertainty as to the distinction to be made between the possibility of updating the data and the right of rectification, it invites it to provide for methods of processing requests that do not require the persons concerned to find themselves constrained to multiply their procedures. On the data retention periods: The draft article R. 2143-15 of the CSP provides that all the data collected as part of the processing carried out by the ABM will be kept for a period of one hundred -twenty years from the date of their registration. taking into account life expectancy. The Commission nevertheless recalls that personal data must be kept for a limited period of time to meet the purposes of the processing in accordance with the provisions of Article 5-1-e) of the GDPR D. In its previous opinion no. 2019-097 of July 11, 2019, it had suggested that scenarios in which the retention period could be reduced should be provided. In this respect, the Commission notes that the Ministry intends to specify in the decree that the data of the persons concerned will be deleted once all the donations of the same person have been used without giving rise to a birth. However, it invites him to ensure that the retention period could not be reduced in other cases. On data security and traceability of actions: The processing envisaged, carried out on a large scale and including in particular sensitive data , was the subject of a DPIA. The processing, to which third-party donors will be able to connect remotely in order to complete the consent form provided for in draft article R. 2143-6 of the CSP, constitutes a teleservice within the meaning of Ordinance No. 2005-1516 of 8 December 2005 and will be subject to security approval before it goes into production. The hosting of the processing will be internalized within the ABM, in the Agency's own data centres. According to the details of the ministry, the backup of the processing data will be carried out by a company subject to US law on servers located in France and without any transfer of data outside the European Union. It is up to the ABM, as data controller, to ensure that its subcontractor provides sufficient guarantees in accordance with Article 28 of the GDPR, in particular by verifying whether local laws and practices are likely to allow US authorities to access data stored on European Union territory. Such access, if not based on an international agreement, could constitute unauthorized disclosure under EU law, in breach of Article 48 of the GDPR. In this case, the Commission considers that the US regulations on access to data from Internet service providers and telecommunications companies by US intelligence services apply to data processed, including outside the territory of the United States, by the company involved in this data backup. As it stands, the Commission therefore considers that there is a risk of access to the data by the US authorities. Consequently, insofar as the envisaged processing is carried out on a large scale and includes sensitive data, the Commission requests that the data

controller use a service provider exclusively subject to European law, or else implement measures preventing any access to the data by the service provider and therefore by the US authorities, such as the encryption of data saved by state-of-the-art algorithms and the non-transmission of encryption keys to the service provider. Encryption measures to ensure the integrity and confidentiality of the data processed will be put in place as part of the processing, both with regard to user workstations, access flows and data exchanges. The Commission recalls the need for encryption at rest of the stored data, which seems to be operational according to the documents provided by the ministry. It also recalls that the technical mechanisms implemented for this processing must comply with the state of the art, and in particular with the recommendations of the general security reference system (RGS). The Commission notes that third-party donors and healthcare professionals will only be able to connect to ABM processing by means of strong authentication, comprising at least two different authentication factors. If one of these factors is a password, the Commission recommends implementing a password policy in accordance with deliberation no. 2017-012 of 19 January 2017 adopting a recommendation relating to passwords , or any other subsequent update of this recommendation, and to choose a different robust authentication factor in order to ensure better authentication reliability and, therefore, to ensure adequate traceability of the access of these users. Concerning the authorization of persons who can access the data processed, the Commission welcomes the implementation of authorization profiles allowing restrictions of access to certain functionalities and to the visibility of data according to the scope of the profile and the operation carried out. The Commission notes that proactive control mechanisms for malicious behavior will be put in place by the ABM. The retention period for functional traces is currently being defined by the data controller. The Commission recalls that keeping functional traces in accordance with its recommendations consists of keeping these traces for a minimum period of six months and a maximum of one year from the generation of the functional trace, or providing specific justification demonstrating a high risk for the persons concerned requiring these traces to be kept beyond the recommended duration, in particular in the event of the possibility of misuse of the purpose of the processing. It acknowledges that these traces will not include health data or personal data. On the processing of data implemented by CAPADD: Article L. 2143-6 of the CSP provides for the implementation by CAPADD the processing of personal data for which it is responsible, the purposes of which are specified by draft article R. 2143-17 of the CSP, namely the recording, storage, and follow-up of requests and the collection and registration of certain third party consent. The Commission considers these specific, explicit and legitimate purposes within the meaning of Article 5 of the GDPR. On the data whose processing is envisaged: The draft article R. 2143-18 of the CSP describes the

categories of personal data which will be processed by CAPADD. In addition, the AIPD on the processing of CAPADD data details the data processed for each of the categories of data subjects. By way of example, the data relating to the identity of persons born from ART with a third-party donor will include: French nationality, civility, birth and usual names, first names, date and place of birth as well as contact details (postal and electronic). The Commission wonders whether it is necessary to collect the French nationality of the persons concerned, insofar as the whole system for donating gametes and embryos is not conditional on the nationality of the persons concerned. that the ministry has undertaken not to collect this information. It also requests that the exact nature of the data that will be collected be specified in the decree. With regard to the collection of data from former third-party donors: According to the AIPD transmitted by the ministry, the national directory for the identification of natural persons (RNIPP) and the national inter-scheme directory of health insurance beneficiaries (RNIAM) will be consulted as part of the procedure for recontacting former third-party donors. According to the ministry, the identification numbers, and more particularly the registration number in the national identification directory of natural persons (NIR) of former third-party donors, will be exchanged between CAPADD and the National Institute of Statistics and economic studies (INSEE), the National Health Insurance Fund and the primary health insurance funds via secure messaging. It is also provided that the data will be deleted at the end of the recontact procedure. The Commission, which recalls that any processing of the NIR must be carried out in accordance with the provisions of Article 30 of the Data Protection Act, invites the ministry to specify in the decree that this data will be processed. It also requests that former donors recontacted be informed that the RNIPP and the RNIAM have been consulted in order to use their NIR to find them. Finally, according to the ministry's details, only the date and the result of the recontact procedure will be kept (consent, refusal or lack of response from the third-party donor). The Commission asks that this be clarified in the decree. With regard to the collection of data from new third-party donors: The Ministry, questioned about the persons concerned by the processing of CAPADD data, confirmed that would also be processed, in the event of a request for access to origins, data relating to new third-party donors. The ministry has undertaken to complete the draft decree on this point. The Commission takes note of this. On the conditions for informing the persons concerned: According to the details of the Ministry, general information will be made available to the public on the CAPADD website and will provide information on the characteristics of the data processing implemented by the latter. The Commission recommends that the collective information campaign highlight the possibility for people to obtain the transmission of a complete information note and the procedures for this request, which should not refer exclusively to electronic means. The

specific information notices, in accordance with the provisions of the GDPR, must be able to be consulted prior to any approach with CAPADD. On the data retention periods: The Commission recalls that personal data must be kept for a period of limited to meet the purposes of the processing in accordance with the provisions of Article 5-1-e) of the GDPR. With regard to data relating to requests for access to origins by persons born from ART with a third party donor: The first paragraph of draft article R. 2143-20 of the CSP provides for the retention of data for a period of fifty years from the date of their recording. According to the Ministry's details, this duration is set taking into account the residual life expectancy of a person born from ART with a third-party donor during which he may have to make requests for access, i.e. from his majority to approximately 70 years. In addition, the Commission takes note of the clarifications of the ministry according to which it is envisaged to grant any request from persons born from an ART with a third party donor, including in the event that it has already been formulated. Recalling that the data used to respond to requests are also kept by the ABM, the Commission wonders about the need for CAPADD to keep the data relating to the requests for such a period of time. In any event, it invites the Ministry to provide for strict application of the principle of data minimization. With regard to data relating to former third-party donors: The second paragraph of draft article R. 2143-20 of the CSP provides for the retention data relating to former third-party donors for a period of one hundred years, from the date of their registration in the processing. According to the details of the Ministry, this retention period is justified with regard to the provisions of Article L. 2143- 6 (5°) of the CSP which entrusts CAPADD with the task of collecting and recording the agreement of former third-party donors to the transmission of their non-identifying data and their identity to persons born of donation. To this end, it specifies that, for the performance of this mission, CAPADD must keep the information according to which the former third-party donor consents or not to the transmission of his identity and his non-identifying data to persons born of donation, in particular so as not to repeatedly contact former third-party donors who have previously refused such transmission. so long in view of the purposes pursued. On data security and traceability of actions: The processing envisaged, carried out on a large scale and including in particular sensitive data, was the subject of a DPIA. This AIPD transmitted by the Ministry and relating to the processing of data implemented by the CAPADD seems incomplete, insofar as the likelihood of the risks has not been assessed; the Commission therefore recalls that the DPIA must be completed before the processing is implemented. Furthermore, the Commission notes that the processing will be subject to security certification before it is put into production. The processing will be hosted by an outsourced service provider certified as a health data host (HDS) and not subject to extra-European regulations. Encryption measures to ensure the integrity and

confidentiality of the data processed will be implemented as part of the processing, according to the same procedures as the processing implemented by the ABM. Sensitive data will be encrypted at rest. The technical mechanisms implemented for this processing must comply with the state of the art, and in particular with the recommendations of the general security reference system (RGS). As with the processing implemented by the ABM, the Commission notes that user access will be protected by strong authentication comprising at least two different authentication factors. The Commission recalls its above-mentioned recommendations concerning the choice of these authentication factors. With regard to the authorization of persons who can access the data processed, the Commission welcomes the implementation of authorization profiles allowing access restrictions to certain functionalities. and access to data only necessary for the user. The retention period for functional traces is being defined by the data controller. The Commission recalls that keeping functional traces in accordance with its recommendations consists of keeping these traces for a minimum period of six months and a maximum of one year from the generation of the functional trace, or providing specific justification demonstrating a high risk for the persons concerned requiring these traces to be kept beyond the recommended duration, in particular in the event of the possibility of misuse of the purpose of the processing. An operational security center will collect and analyze the traces and events produced by the network equipment of the treatment. The Commission recommends that the application traces and events collected and analyzed be kept for a period in accordance with its recommendations and notes that these traces will not include health data or personal data. It also recommends the implementation of a mechanism for proactive analysis of the functional traces generated by processing. access to the origins, will be carried out using secure health messaging systems ensuring the confidentiality of exchanges. When some of these entities are not eligible for this mode of communication, the Commission recalls that the body of the messages must not include any personal data and be limited to what is strictly necessary. It notes that the attachments will be encrypted by state-of-the-art algorithms.The other provisions of the decree do not call for comments from the Commission. The President,

M. L. Denis