Deliberation 2021-025 of February 25, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday June 22, 2021NOR: CNIX2118707XDeliberation n° 2021-025 of February 25, 2021 providing an opinion on a draft decree amending the decree of 1 September 2016 creating by the Directorate General of Public Finances an automated processing of personal data for managing the file of capitalization and life insurance contracts called Ficovie (request for Opinion No. 1942384) The National Commission for Computing and Liberties,

Seized by the Ministry of Economy, Finance and Recovery,

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 general tax code, in particular its article 1649 ter;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 31-I;

After having heard Mr. Philippe-Pierre CABOURDIN, commissioner, in his report, and Mr. Benjamin TOUZANNE, government commissioner in his observations, Issues the following opinion: The Commission was seized on the basis of I of article 31 of the amended law of January 6, 1978, a request for an opinion on a draft decree amending the decree of September 1, 2016 establishing by the Directorate General of Public Finances (DGFiP) an automated data processing management of the file of capitalization and life insurance contracts called Ficovie. The draft order has several objectives. It integrates the management of authorized third parties with the purposes pursued by Ficovie, expands the persons who can access this processing and modifies the provisions relating to the exercise of the rights of the persons concerned with regard to changes in the regulations relating to the protection of personal data. staff made by the entry into force of the European data protection package in 2018. The Commission notes that, with regard to the changes made to the categories of staff who can access Ficovie, these aim to draw the consequences of the changes made by the legislator to several articles of the book of tax procedures, the customs code and the labor code, mainly within the framework of the law of October 23, 2018 relating to the fight against fraud. It recalls that it ruled in its deliberation No. 2019-080 of June 20, 2019 providing an opinion on a draft decree relating to the procedures for authorizing and designating agents of several organizations and administrations to access information from the

automated processing called Patrim, FICOBA, FICOVIE and BNDP, on the methods of authorization and designation of these. Under these conditions, it considers that these changes do not call for comment. The Commission recalls, however, that the necessary consequences should be drawn from this by updating the security measures for the processing to be implemented. On the applicable legal regime and the rights of the persons concerned The Ministry considers that the purpose of FICOVIE processing is, in the tax field, the prevention, detection and prosecution of criminal offenses by a competent public authority, thus falling within the scope of application of article 87 of the law of January 6, 1978 relating to data processing, files and freedoms. The Commission recalls that for processing to be partially or totally within the scope of Directive (EU) 2016/680 of 27 April 2016, known as the Police-Justice Directive, as transposed in Title III of Law No. 78-17 of January 6 as amended, data processing must meet two cumulative conditions. It must, on the one hand, pursue one of the purposes mentioned in its article 1 relating to the prevention and detection of criminal offences, as well as investigations and prosecutions in this area, and on the other hand, be implemented by a competent authority within the meaning of this directive. With regard to the criterion of the purpose pursued by the processing, the Commission notes that Article 2 of the decree of 1 September 2016 establishing by the Directorate General of Public Finances a processing automated personal data management of the file of capitalization and life insurance contracts called Ficovie provides The purpose of the processing is to identify, on computer media, the declarations of the contracts and investments provided for in I and II of Article 1649 ter of the General Tax Code (…). However, with regard to the applicable legal regime, the Council of State considered in its decision n ° 424216 of July 19, 2019 that a processing of data of a p personnel falls, depending on its purpose, within the scope of the regulation of April 27, 2016 or that of the directive of the same day: Even though, as stated in point 8, the disputed processing has several purposes, which include the prevention, detection and repression of criminal offences, its purpose is to allow, by combating tax fraud and tax evasion, improved compliance with their tax obligations by French and American taxpayers. It follows that it falls within the scope of the regulation of April 27, 2016 and not that of the directive of the same day. It follows that the mere fact that a processing operation, which was created for other purposes, also serves to detect possible infringements, is not sufficient to bring it within the scope of the police-justice directive. In the present case, the Commission considers that the aforementioned processing falls within the scope of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 referred to above (GDPR), without there being any need to examine the criterion relating to the competent authority within the meaning of Article 3.7 of the so-called Police-Justice Directive. It therefore considers that the draft decree will have to be

updated taking these elements into account and takes note of the ministry's commitment on this point. With regard to its characteristics, the Commission also notes that this processing complies with the formalism imposed by Article 31 of the aforementioned law. In this context, the Commission intends to make observations in particular on Articles 4 and 5 of the draft. Article 4 mentions the rights of access, rectification, erasure and limitation as provided for by the so-called Police-Justice directive transposed in articles 105 and 106 of the law of January 6, 1978 as amended. Article 5 excludes the application of the right of opposition under article 110 of the law of January 6, 1978. Article 4 of the draft decree provides in particular for a differentiation of the exercise of the right of access depending on the quality of the person concerned (subscriber, insured, beneficiary, beneficiary who would not be able to provide proof of his acceptance of the benefit of the contract). The DGFiP intends in particular to eliminate any possibility for the beneficiary who does not accept to exercise his right of access. In this respect, the Commission recalls that the right of access is composed of at least two parts. The first part allows the data subject to know whether data concerning him or her are processed by the controller, without the provisions of Article 15 of the GDPR providing for possible derogations on this point. In the event of a positive response, the second part of the right of access allows the person to obtain communication of the data concerning him. The Commission notes that if the differentiation in the provision of the copy of the data according to the quality of the data subject appears to be in accordance with paragraph 4 of Article 15 of the GDPR in order to preserve the privacy of others, the exercise of the right to Differentiated access must be modulated in proportion to the invasion of the privacy of others that it may cause. all the identification data concerning him but also the identity (surname and first name) of the subscriber and the insured, and the data of the contract referred to in 2° of I of the decree of September 1, 2016 mentioned above in the extent that this information is not likely to infringe the rights of these third parties. The Commission notes, however, that restrictions on the right of access may be made when it is exercised by the beneficiary who has not yet accepted or the good beneficiary who would not be able to provide proof of his acceptance of the benefit of the contract. Consequently, he must have access only to his identification data: surname, first names, date and place of birth, sex, address, technical identifier from the DGFiP information system (ITIP number) and individual national tax identifier used by tax administrations in their internal processing and in their relations with taxpayers (SPI number) for natural persons. Indeed, these data do not infringe the rights and freedoms of others, since they only relate directly to the person concerned. The Commission reminds the data controller that it is up to him to indicate to a beneficiary who would not be able to provide proof of his acceptance of the benefit of the contract whether personal data concerning him are processed or not on the date of

the consultation, with regard to the modifications which may be made by the subscriber until at his death. It takes note of the ministry's commitment to study such a possibility, in conjunction with the insurers. The draft decree provides that the persons concerned exercise their rights with the personal tax service on which the applicant depends. The request can be made by post, by e-mail via the secure messaging service of your personal space or directly at the reception of the personal tax department. The Commission draws the attention of the DGFiP to the case of a foreign beneficiary who does not reside in France and who does not have a tax number and, consequently, no personal tax service with territorial jurisdiction. It notes that the draft decree will be supplemented on this point. The Commission therefore requests that the statements relating to the rights of individuals (right of access, rectification, erasure, etc.) be modified to correspond to the rights provided for by the GDPR. On the security measures implemented Two main applications allow the consultation of processing data: the FICOVIE-Agents system, intended for administration agents and the FICOVIE-Notaries subsystem, intended for notaries. The Commission recalls first of all that the processing being a teleservice within the meaning of the law, it is subject to the prescriptions provided for by the ordinance n° 2005-1516 of December 8, 2005, must comply with the general security reference system (RGS) provided for by Decree No. 2010-112 of February 2, 2010. The Commission also recalls that, in this respect, the processing must be subject to a risk analysis including the risks weighing on the persons concerned. It also recalls that it is up to the data controller to formally attest to the acceptance of the security level of the teleservice through an RGS approval and to publish the approval certificate on its site. The Commission takes note that access to the FICOVIE-Notaires application, the only application accessible via the Internet, is secured by the TLS 1.1 protocol but it recommends, on this point, to use, as much as possible, the version of TLS the most up-to-date. The Commission notes that the FICOVIE-Agents and FICOVIE-Notaires applications are only accessible to authorized persons and agents and that the latter are required to enter a personal identifier and password in order to to log in. At this stage, the processing provides for a password of between eight and twelve characters, which does not comply with the criteria defined in its deliberation no. 2017-012 of January 19, 2017 adopting a recommendation relating to passwords. It recommends modifying the processing to bring it into line with this recommendation. On the management of application traces and technical logs The Commission notes that various traces are generated by the processing (FICOVIE-Agents application and FICOVIE-Notaries application) and that the duration storage of the latter varies according to the population concerned, as well as the type of trace. Thus, the storage period of the technical logs of the FICOVIE-Agents system (logs) is thirty-one days and of the functional traces of the agents is one year. In addition,

the FICOVIE-Notaires subsystem generates and stores the functional records of notaries for a period of three years. It should be noted that this subsystem does not keep technical logs. The Commission recalls that its recommendation, on the management of traces and logs, is to implement a retention period of 6 months, except to prove that certain risks can only be covered by an extension of this duration, and to implement a system of centralization of traces in order to be able to ensure the integrity and availability of the management of traces and logs. The Commission therefore considers that it is necessary for the FICOVIE-Notaries subsystem and the FICOVIE-Agents system to allow the retention of technical logs, the retention period of which, adapted to the context, should be six months. Similarly, the Commission recommends that, subject to necessity and the implementation of the aforementioned systems, the functional traces relating to the FICOVIE-Notaries subsystem and the FICOVIE-Agents system, be kept for an equivalent period, which taking into account particular risks presented by the processing may be extended to one year. The Commission notes that no log monitoring tool, either technical or application, is deployed. It recalls that the implementation of a proactive mechanism for the automatic control of logs contributes to the detection of abnormal behavior by the automatic generation of alerts and is therefore, consequently, necessary and more appropriate than an extended retention of logs. Finally, the Commission encourages the Ministry to implement, as it is already done for the FICOVIE-Notaries subsystem, organizational measures, on a regular basis, having as their object the analysis of the logs in the to detect suspicious behavior or usage anomalies.The PresidentMarie-Laure DENIS