Deliberation 2022-041 of April 7, 2022National Commission for Computing and LibertiesNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Wednesday May 18, 2022NOR: CNIX2214639XDeliberation No. 2022-041 of April 7, 2022 providing an opinion on a draft decree amending the decree of August 10, 2016 authorizing the creation of an automated processing of personal data called "DOCVERIF" (request for opinion no. 21021419)The National Commission for Computing and Liberties,Saisie by the Minister of the Interior of a request for an opinion concerning a draft decree amending the decree of August 10, 2016 authorizing the creation of an automated processing of personal data called "DOCVERIF"; Having regard to law no. ° 78-17 of January 6, 1978 amended relating to data processing, files and freedoms, in particular its article 89-I; After having heard the report of Mrs. Sophie LAMBREMON, commissioner, and the observations of Mr. Benjamin TOUZANNE , Government Commissioner,Issues the following opinion:The National Commission for Computing and Liberties has been seized by the Ministry of the Interior of a draft decree amending the decree of August 10, 2016 authorizing the creation of an automated processing of personal data called "DOCVERIF". This processing, on which the Commission has already ruled in 2016 and 2018, is intended to facilitate the control of the validity of documents issued by the French authorities in order to fight against documentary fraud. It can be questioned by the services of the national police and gendarmerie (users of "scope 1") as well as by public administrations, bodies entrusted with a public service mission and credit institutions (users of "scope 2") and allows these users to access data relating to the status of a document ("valid", "invalid", or "unknown"). To ensure access to this information, "DOCVERIF" is fed by an interconnection with two other processing operations: for data relating to national identity cards and passports: processing "secure electronic documents" (TES); for data relating to residence permits: the application for managing the files of foreign nationals in France (AGDREF). The draft decree submitted to the Commission for its opinion allows the development of several characteristics of the processing. It provides for: the systematic reporting, and not conditional on the status of the document, of civil status data contained in the TES processing; the extension of the perimeter of users of "perimeter 2" to municipal police officers and rural guards who are required to carry out identity statements of the offenders, to the financing companies mentioned in Article L. 511-1 of the Monetary and Financial Code, to the suppliers of means of electronic identity attesting to a substantial or high level of guarantee , and to the agents of the services of the General Secretariat of the Ministry of the Interior and the National Agency for Secured Documents (ANTS) responsible for project management and project management of the processing "Guarantee Service of the digital identity" (SGIN); the recording of the reason for consultation and communication and the extension of the

retention period for traceability data; the removal of the linking of "DOCVERIF" with, on the one hand, the system th Schengen Information and, on the other hand, the "Stolen and Lost Travel Documents" (SLTD) database managed by Interpol. criminal offenses and falls, as such, under Title III of the law of January 6, 1978 as amended and must be the subject of an order, issued after a reasoned opinion and published by the Commission in accordance with the provisions of Article 89- I of the amended law of January 6, 1978. The data controller is the Ministry of the Interior. On the general economy of the system Article 2 of the draft decree modifies article 4 of the decree of August 10, 2016 to allow the systematic reporting of data from marital status contained in the "TES" processing. While currently this information is only recorded for invalid titles, they would now be recorded for all titles, at least partially. Thus: "Scope 1" users, who until now can only access surnames, first names, date and place of birth if they are attached to an invalid document, will be able to consult the surname and first first name when the title is valid; "Perimeter 2" users, who have not yet had access to civil status data, will be able to consult the partially masked first and last name, regardless of the status of the identity document. specifies that this solution aims to fight against fraud consisting in the presentation of a title containing a valid number but whose civil status elements have been falsified. Indeed, the query of "DOCVERIF" only allows today to know if the title number is valid or not, without coupling with the associated civil status elements. As a result, each time a pass is falsified or used by a person other than its holder, without it having been invalidated following a declaration of loss or theft by the latter, the verification carried out does not does not detect fraud. However, according to the Ministry, elements of the civil status of the title can be falsified and the comparison with the civil status data of the real title would make it possible to identify the fraud. On a preliminary basis, the Commission considers that the fight against fraud documentary must be the subject of a set of measures intended to counter the various strategies of fraudsters, while limiting the risks for the persons concerned. It also recalls the importance of civil status data associated with identity document numbers for each individual and the need to prevent any risk of misuse of this data. Beyond the nature of the data processed, it emphasizes that the planned development will lead to the processing of part of the civil status data of almost the entire French population. Furthermore, the Commission considers that the security of identity documents is based on two main elements: the security of the issuing process on the one hand, and the security of the title itself, on the other hand. In this respect, the issuance, until 2021, of identity documents whose design dates from the 1980s constitutes an opportunity for significant fraud, which may call for additional measures such as the "DOCVERIF" service. The Commission considers that the objective must be that in the long term the verification of identity documents can be carried out by directly ensuring that the

document itself is not physically falsified. In particular, for permits with an electronic chip (i.e. all passports in circulation, national identity cards issued since August 2021 and residence permits issued since 2011), the solution the most respectful of the principles of data minimization and privacy protection by design to achieve the objective of verifying the match between the first and last names and the identity document presented, is based on offline reading of the content of the chip. It is only in a residual way, to remove a doubt or when the electronic component is damaged (intentionally or by wear), that a comparison with a central base should be maintained. Thus, when all French documents (passports, national identity cards and residence permits) have an electronic chip, consultation of the "DOCVERIF" database will no longer be useful for documents that can be checked using this chip. It will then be necessary to reassess the proportionality of the risks generated by the "DOCVERIF" database and to consider an alternative architecture allowing to proceed, in a residual way, to the only validity checks which cannot be made directly on the title. firstly, with regard to the architecture of the system, the Commission had observed, in its deliberation no. 2021-022 of February 11, 2021 issuing an opinion on a draft decree amending decree no. to "TES" processing, that the planned modification, which would lead to a very significant increase in the volume of data transmitted to "DOCVERIF" processing, "should not lead to DOCVERIF processing, which pursues purposes distinct from those of TES, becomes a mirror base of the latter". It had invited the ministry to identify solutions making it possible to meet the objective pursued without transmitting all the civil status data to "DOCVERIF". The Commission then envisaged a scenario in which the "DOCVERIF" "perimeter 1" and "perimeter 2" databases would only retain, for valid documents, a digital signature of the surname and first name. Thus, "DOCVERIF" would be queried on the basis of the same elements as the system implemented before this modification but, in the case of a "valid" return for which the verification agent would have a doubt, the surname and first name present on the title could be verified with regard to the stored signature. To respond to this request, the ministry explored two different scenarios for minimizing the data transmitted from the "TES" processing to "DOCVERIF". It emerges from the details provided by the Ministry that the two scenarios assessed were ruled out for users of "perimeter 1" since they would not allow them to have access to the identity of the true holder of the document registered as valid in DOCVERIF but falsified. However, the ministry considers that this information is essential to the exercise of the missions of the police and gendarmes, in particular to be able to contact the real holder of the title in order to warn him, or for investigation purposes. The ministry would therefore like the database used by "perimeter 1" to contain a direct copy of the surname and first name in "DOCVERIF" and not a signature or fingerprint resulting from the combination of these data. For "perimeter 2", the draft order

provides that "DOCVERIF" will be queried based on the type of document, the document number and the date of issue to transmit in return the status of the title as well as two elements of civil status (the name and the first name) in a partially masked format. However, the Commission notes that the Ministry undertakes to modify the draft decree in order to provide for the querying of "DOCVERIF", by users of "perimeter 2", based on the type of document, its number , its date of issue as well as, optionally, the surname and first name presented by the person. Only the status of the title will be transmitted in return. Finally, the Commission observes that, with regard to "perimeter 1", the choice of the ministry is guided by operational constraints aimed at limiting the manipulations to be carried out by users. Indeed, the use of a signature or fingerprint query system requires the user to fill in all the civil status data, and not just the title number, thus increasing the risk of error. While it is certain that the data entry error rate depends on the amount of information to be entered and that this is greater in the scenario suggested by the Commission than in those studied by the Ministry, it is also possible to reduce the risk of input error by automating the reading of the information (or, at the very least, of the majority of it), in particular with the title's MRZ strip. The Commission takes note of the Ministry's comment on the short-term operational difficulty of making available to the whole of "perimeter 1" devices allowing this automatic reading and that their absence would make it difficult to use, in practice, a server-side data verification system because of the number of errors that would be made when typing the identity data and therefore the large number of "unknown" answers that would be returned in the state of practice, because of these errors. Consequently, it recommends that, as soon as these means are available or deployable, the device relating to "perimeter 1" be reviewed to allow the implementation of a solution which will be limited to confirming or invalidating a scanned identity and which would not store more nominative data in the database or, at the very least, more clearly. perimeters 1 and 2 must be justified by a specific and relevant operational need with regard to the purposes of the processing and be proportionate with regard to its objectives. fraud schemes. On the other hand, it is difficult to assess the extent of it today, especially for recently designed tickets, since the police and gendarmes cannot currently, in a large number of cases, detect that there is counterfeiting or falsification of the document that is marked as valid by "DOCVERIF". A quantified assessment of the number of frauds of this type, for each category of security, must be carried out to confirm the scale of the operational need. With regard to the objectives pursued by the reform of "DOCVERIF", the Commission notes that the risks incurred real and considers that supervision and control measures should be put in place. Indeed, copying civil status data and title numbers for the entire French population with a title will increase the attack surface for this data. Through "DOCVERIF", a very large

number of people will have access to title numbers and civil status data certified as valid, liable to misuse. Under these conditions, the Commission recommends that the processing be deployed as experimental in order to assess the reality of the need invoked. Its maintenance or perpetuation should be conditional on a combined demonstration of a specific operational need, a determined level of fraud and the effectiveness of the system within a set deadline. In this perspective, the Commission wonders about the advisability of limiting in "DOCVERIF" the information concerning the valid titles to the only titles which can be the subject of a doubt concerning their authenticity (such as for example the fact that the chip has been destroyed or the presence of the number on the lists of numbers of titles offered for sale) and invites the Ministry to experiment to determine whether it is possible to have sufficient efficiency with an alternative system where a database of only titles in doubt would be used. It takes note with satisfaction of the Ministry's commitment to modify the draft decree in order to provide for the communication of civil status data to users of "perimeter 1" for valid permits on an experimental basis and that the possible sustainability of this development, justified by its effectiveness, will require a modification of the text and a new referral to the Commission.Thirdly, it appears from the impact assessment relating to data protection (DPIA) transmitted that a development of II of article R. 611-1 of the code of entry and residence of foreigners and the right of asylum (CESEDA) is envisaged to allow the reporting of elements of civil status resulting from the "AGDREF" processing for invalid and valid residence permits. Without prejudice to the comments previously made on registration not conditional on the status of the civil status data document in "DOCVERIF", comments which are also applicable for residence permits, the Commission notes that the timetable for implementing role of this development has not yet been defined and will be depending on the deployment of the "Digital Administration for Foreigners in France" (ANEF) program. In any case, it recalls that it must, if necessary, be kept informed and seized, under the conditions provided for in article 33-II of the law of January 6, 1978 as amended, of any substantial modification affecting the characteristics of the processing . In the same way, it recalls that the DPIA transmitted to it, under the conditions provided for in Article 90 of the aforementioned law, must be updated. On the purposes of the processing and the categories of data processedIn the first place, the proposed modification, namely the processing of civil status data for valid documents, aims to allow "to fight against the improper use of such documents, their falsification and their counterfeiting", as well as the provides for article 1 of the decree. The ministry stresses that the information delivered by "DOCVERIF" concerning civil status for valid documents to users of "perimeter 1" and "perimeter 2" will not allow to make the link with a natural person or to carry out an identity check within the meaning of article 78-2 of the code of criminal procedure.

Thus, the changes envisaged, having the sole objective and consequence of strengthening the fight against the improper use of identity documents, their falsification and their counterfeiting, fall within the purposes of the processing provided for in Article 1 of the aforementioned decree. .Secondly, the draft decree extends the access of "DOCVERIF" users to new categories of data. ), date and place of birth in the event of an invalid title, will have access to the surname and first name in the event of a valid title. of "perimeter 1", that only agents with the role of verifying the identity of persons and verifying the validity of documents can have access to the processing. On the other hand, it does not have any information on the existence of other frameworks in which "DOCVERIF" could be queried. In the event that the civil status data from the "TES" processing would already be accessible to users of the "scope 1", the Commission considers, without calling into question the use of "DOCVERIF" to obtain the status of the title, that the consultation of these same civil status data from "DOCVERIF" would not be necessary.D n the other hand, the draft decree provided that users of "perimeter 2" could, with regard to valid and invalid titles, access to partially masked surnames and first names. The Commission notes that it is not excluded that , despite the planned masking, it is possible, for a user of "perimeter 2", to find the surname or first name of the person concerned. , for "perimeter 2" users, a query of "DOCVERIF" based on the type of document, its number, its date of issue as well as, optionally, the surname and first name presented by the person. Only the status of the title will be transmitted in return. Finally, with regard to the accuracy of the data processed, particular vigilance is required in terms of updating the data, given the significant consequences that, for the persons inspected, possible errors on the status of the document presented during an inspection. On accessors and recipients of the processing The draft decree extends the list of users of "scope 2" without modifying the scope of users of "perimeter 1". As a preliminary point, the use of "DOCVERIF" is an option left to the discretion of the users, except for the suppliers of means of electronic identification aiming at the substantial or high level. In the event of an invalid title or a valid title containing data falsified, the users of "perimeter 2" are not competent to carry out an investigation procedure. Although the Commission takes note that the follow-up to the procedure will, in these circumstances, be carried out by the competent police or gendarmerie services and that the construction of a chain of reporting users to the police and gendarmes is under study, it nevertheless regrets that it does not have information on the purpose, terms and conditions of the introduction of such reports. Firstly, the draft decree adds municipal police officers and country guards to users of "perimeter 2". With regard to the assignments within the framework of which these new recipients will be able to access "DOCVERIF" data, the Commission notes that they will have access to the processing solely within the framework of their identity statement

assignments as framed , for the former, by article 78-6 of the code of criminal procedure and, for the latter, by article L. 522-4 of the internal security code. Secondly, the financing companies mentioned in 2 ° of Article L. 511-1 of the Monetary and Financial Code are among the new buyers of "scope 2" provided for by the draft decree. Finance companies are, in the same way as credit institutions which already have access to processing, required to verify the identity of their customers on the basis of Article L. 561-5 of the same code within the framework of the fight against money laundering and terrorism. The Commission underlines that the access of these users to the processing data must be relevant with regard to the purposes of the processing, namely the facilitation of the control of the validity of the documents and the fight against the improper use, falsification or counterfeiting of such documents.Thirdly, the draft decree adds a 4° to article 6 of the decree of August 10, 2016 to include, among the users of "perimeter 2", the "providers of electronic identification means benefiting from a certification or a certificate of conformity by the National Agency for the Security of Information Systems with the requirements of the substantial or high level of guarantee within the meaning of Article I of Implementing Regulation 1502/2015 of the 8 September 2015 laying down the technical specifications and minimum procedures relating to the guarantee levels of the electronic identification means referred to in Article 8(3) of Regulation (EU) No 910/2014 on electronic identification onic and trust services for electronic transactions within the internal market". These recipients, which are listed in appendix 2 created by the draft decree, include the "Digital identity" supplier of the La Poste group. The Commission welcomes this development, necessary to set up a digital identity with a substantial or high level of guarantee. The draft decree also adds a 5° to article 6 to provide that the agents mentioned in I of article 3 of the decree authorizing the creation of a means of electronic identification called "Digital identity guarantee service" (SGIN), on which the Commission recently ruled, have access to processing. These users cover, according to the terms of I of the aforementioned article 3, the agents of the services of the general secretariat of the Ministry of the Interior and of the ANTS responsible for the project management and the project management of the processing SGIN. The Commission takes note of the clarifications provided that access by the SGIN to "DOCVERIF" will not be subject to the condition of an assent from the National Agency for the Security of Information Systems (ANSSI) at the level substantial or high, so as not to delay the technical work in progress, it being understood that the assent of ANSSI on the achievement by the SGIN of the high level is planned for the summer of 2022. It thus observes that this access , insofar as it will not be subject to the condition of an assent at the substantial or high level, differs from the access granted to the other providers of electronic identification means referred to in 4° of Article 6 created by the draft decree. The Commission wonders,

however, with regard to the drafting of the draft decree, on the terms and conditions of the planned access. Indeed, as soon as the access of the agents in charge of the project management and the project management would be necessary for the only technical work required for the implementation of the SGIN, the Commission considers that this access should be limited in time and that the relevant provision of the draft order should be amended accordingly. However, if such access was intended to guarantee the functioning of the electronic identification means SGIN while waiting for a certificate of conformity from ANSSI, it wonders about the choice to limit this access to agents responsible for controlling and project management insofar as this access will not allow the data to be processed for the purposes pursued. On the agreements concluded between the organization concerned and the data controller Article 6 of the decree provides that access to the information contained in the processing by private users of "perimeter 2" is subject to the prior conclusion of an agreement with the processing manager. Firstly, the AIPD transmitted by the ministry indicates in particular that the agreement concluded between the users and the data controller stipulates that no decision taken by a user can be based solely on an "invalid" or "unknown" indication. It is also specified that the ministry has the possibility of periodically carrying out audits with regard to a user in order to ensure compliance with contractual commitments. The agreement provides for the possibility of immediately interrupting the service in the event of a breach, or within ten working days without justification. While the Commission notes that guarantees are provided for in the agreement, it nevertheless questions the effectiveness practice of these elements and in particular the possibility of guaranteeing that the result of each consultation of the processing will not constitute the main element on the basis of which the user of the "perimeter 2" takes a decision within the framework of his missions. It notes that mismatches would be a strong indication of fraud, likely to support the decision taken. perimeter 2" and detailed in the AIPD that input errors lead to a high rate of invalid titles (confusion of the title number and the foreign number for residence permits, and other input errors due in particular to the readability of the digitized titles ). In this regard, users are informed, via the processing user agreement, of the fact that the mention "unknown" may be caused by an input error and that they are also invited to carry out the necessary checks to limit the risk of error. The agreements include a point of attention on the distinction between permit number and foreigner's number visible on a residence permit. The aforementioned report also highlights the difficulty, for some users, of interpreting "invalid" or "unknown" returns " in the absence of additional information on the reasons and to adapt the conduct to be adopted vis-à-vis the persons concerned. In view of these elements, the Commission recommends supplementing the user agreements concluded with the organizations concerned with, on the one hand, recommendations to

reduce input errors and, on the other hand, guidelines to follow in the event of an "invalid" or "unknown" title. It also recommends that the agreements encourage the bodies concerned to use methods of direct and automatic verification of the title, by reading the electronic chip in particular when possible. In addition, the Commission recommends supplementing these agreements in order to encourage the organizations to inform the persons concerned of the fact that they are likely to perform a "DOCVERIF" query. Moreover, if it notes that it is provided for by the draft decree that "the rights of information, access, rectification, erasure and limitation provided for in Articles 104 to 106 of the same law s 'operate directly with the modernization and territorial administration", it considers that the wording of the draft decree relating to the right to information should be modified insofar as, under the terms of Article 104-I of the amended law of 6 January 1978, it is the responsibility of the data controller to provide the data subject with the information listed and not of the person requesting communication of this information. Thirdly, the Commission observes that the standard agreement for the use of "DOCVERIF" indicates that the authorization for use is given for French territory (mainland, overseas departments, overseas regions), which means, according to the details provided by the ministry, that the interrogations ns are carried out exclusively on French territory and that the answers are consulted and stored exclusively on French territory. It notes that the agreement may be modified by users on this point and that, as it stands, the agreement does not include prohibition of any transfer of data outside the European Union. of the conditions set out in article 112 of the law of January 6, 1978 as amended. Where appropriate, appropriate safeguards for the protection of personal data should in particular be provided by a legally binding instrument. In the absence of an adequacy decision adopted by the European Commission or of appropriate guarantees, and by way of derogation from the aforementioned article 112, such transfers can then only be carried out subject to compliance with the conditions set out in article 113. of the amended law of 6 January 1978.The Commission takes note that the agreement will be amended to explicitly mention the prohibition of data transfers to States that do not belong to the European Union.On security measuresFr Due to the importance of the risk for individuals in the event of misuse of the purposes of the processing and the frequency of occurrence of such practices, the retention period of certain logging data of three years is considered proportionate by the Commission. Indeed, this journaling contributes by its dissuasive capacity to the security of the processing. The Commission underlines the importance of the proactive analysis of traces to identify abnormal behavior and limit the impact on the persons concerned as soon as possible. Civil status data is stored encrypted with algorithms and key management procedures compliant with appendix B1 of the general security reference system. The Commission observes that

work is underway to ensure that key management is also in compliance with ANSSI's recommendations in the course of 2022. Most players authenticate themselves with their agent card (in particular, for national police, national gendarmerie, ANTS, CERT or Tracfin agents). The Commission approves of this choice, considering that strong authentication is essential for "perimeter 1" access. In view of the risks relating to the processing, as well as the modifications proposed by the Ministry on "perimeter 2", the Commission considers that strong authentication for this perimeter is a practice to be encouraged. The Commission observes that audits have been carried out in the framework of the certification of the device and underlines that the correction of the main deviations has been carried out or is planned by the end of 2022. To ensure a level of security adapted to the risks, regular audits as well as the implementation of the necessary corrections for any discrepancy that is at least significant are considered essential by the Commission. Subject to the previous observations, the security measures described by the data controller seem to comply with the security requirement provided for by article 99 of the "Informatique et Libertés" law ".The Commission recalls, however, that this obligation requires updating the DPIA and its security measures with regard to the reassessment. on regular risks.The PresidentMarie-Laure DENIS