Deliberation 2021-022 of February 11, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Tuesday March 16, 2021NOR: CNIX2105676VDeliberation n° 2021-022 of February 11, 2021 providing an opinion on a draft decree amending decree no. 55-1397 of October 22, 1955 establishing the national identity card and decree no. 2016-1460 of October 28, 2016 authorizing the creation of a processing of personal data relating to passports and to national identity cards (request for opinion no. 20015262)The National Commission for Computing and Liberties, Seizure by the Minister of the Interior of a request for an opinion concerning a draft decree amending decree no. ° 55-1397 of October 22, 1955 establishing the national identity card and decree n ° 2016-1460 of October 28, 2016 authorizing the creation of a processing of personal data relating to passports and national cards national identity cards; 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 (GDPR); Having regard to Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and residence documents issued to Union citizens and family members exercising their right to free movement; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 32; Having regard to Decree No. 55-1397 of October 22, 1955 establishing the national identity card; Having regard to decree n° 2016-1460 of October 28, 2016 authorizing the creation of a processing of personal data relating to passports and national identity cards; After having heard Mrs. Marie-Laure DENIS, president, in her report, and Mr Benjamin TOUZANNE, Government Commissioner, in his observations, Issues the following opinion: residence documents issued to Union citizens and their family members exercising their right to free movement. This regulation, applicable from August 2, 2021, requires Member States of the European Union (EU) to put into circulation identity cards incorporating a highly secure electronic component containing biometric data, namely a digitized image of the face. of the cardholder and that of two fingerprints in interoperable digital formats. Article 3-5 of regulation 2019/1157 of June 20, 2019 referred to above, also imposes the compulsory collection of fingerprints. Only minors under the age of six are exempt from collecting fingerprints under the terms of this regulation. and people who are physically unable to have them taken, with Member States retaining the possibility of exempting minors under the age of twelve from having to take fingerprints. In this respect, the Commission notes that in France, national provisions have been adopted to this effect. It is in this context that the Commission is seized of a draft decree

amending the provisions relating to the national identity card (CNI) as well as those relating to the conditions for implementing the processing referred to as Secure Electronic Securities (TES). It recalls that this processing, which brings together, in a centralized database, the digitized image of the face and the fingerprints of two fingers of all CNI and passport applicants, makes it possible to issue and renew these documents, but also to prevent and detect their falsification and counterfeiting. In order to better combat document fraud, particularly when renewing the document, the TES system automatically compares the fingerprints of each applicant with those previously registered under the same identity, in order to verify that the identity of the applicant for title is the one it claims to have (person authentication function). It emphasizes that to date, the TES remains a singular file, given both its scope of unparalleled magnitude, and the particularly sensitive nature of the biometric data it contains. Since the creation of this processing, the Commission has thus always shown itself to be particularly attentive with regard to the substantial safeguards to be implemented to regulate the use of this processing and intends to show increased vigilance in the context of the modifications which are submitted. It recalls that, more particularly with regard to sovereign uses, the use of biometric recognition devices is considered legitimate to ensure the identity of a person, as soon as the biometric data is kept. on a medium for which the person has exclusive use, as is the case for the biometric passport. The Commission considers in this respect, as it has recalled in numerous deliberations, that the establishment and maintenance of a central biometric database can only be accepted insofar as imperative requirements in terms of security or public order justify it. The processing of biometric data (image of the face and fingerprints), in a centralized form, in fact generates more risks from the point of view of the protection of personal data, taking into account both the characteristics of the element of physical identification retained, the possible uses of this processing and the risks of serious breaches of privacy and individual freedoms resulting therefrom. a centralized database of fingerprints collected for electronic passports, called Secured Electronic Titles (TES), by the decree of April 30, 2008, then regretted its extension to fingerprints collected for identity cards by the decree of 28 October 2016. Seized in litigation, the Council of State validated the principle of the constitution of a centralized database, limited to the fingerprints of two fingers for s authentication, both for passports (CE, Ass., 26 Oct. 2011, No. 317827, Rec.) and for identity cards (CE, 10/9, 18 Oct. 2018, No. 404996) , even though for passports biometric data already appears in the individual component inserted in the title. solutions that it considers to be more protective of citizens' privacy should continue to be considered. In this regard, it invites the Ministry and the National Agency for Secure Documents (ANTS) to continue their work in order to study the possibility, in particular, of keeping the photograph of fingerprints in the form

of a template. Having recalled these general elements, the Commission considers that the implementation of a high-level State digital identity, respectful of the Data Protection principles, must be encouraged. It considers in this respect that the implementation of a national electronic identity card (CNIe) is intended to meet sovereign uses (travel document, proof of identity during checks, fight against documentary fraud) which are the subject of the draft decree submitted to the Commission, but also, eventually, to digital identity services which are not described in the draft decree but could be the subject of future legislative or regulatory texts. The Commission encourages the development of these secure identities, which make it possible in particular to eliminate the circulation of photocopies of civil status documents when carrying out certain administrative or commercial procedures requiring them, while recalling that such a level of certification identity is not necessary for many other procedures. It also wishes to make some observations on the considerations to be taken into account in this regard. With regard to the development of digital identity solutions, the ministry specified that the electronic component of the CNIe would be integrated into the electronic identification scheme composed of 'ALICEM (Application for reading the identity of a citizen on the move) and FranceConnect. The Commission considers that the deployment of this card is an opportunity to extend very widely access to a secure device allowing the benefit of digital identity services and that a reflection should be carried out in order to take into account the issues related to digital inclusion. It will be incumbent to maintain physical access to the services in question, in particular to public services or essential services. Also, the planned device must be adapted in order to guarantee accessibility for people with disabilities to the devices for collecting biometric data and digital recording of CNIe requests. On this last point, it refers to the recommendations made by the Defender of Rights in its decision 2020-027 of 20 May 2020 relating to the difficulties encountered by adults under guardianship when issuing or renewing their national residence permit. identity. The Commission also considers that the design of this new CNIe is an opportunity to integrate additional tools to guarantee the best possible protection of privacy in the context of its use as a digital identity medium. Thus, it is possible to provide identification devices carrying out the selective disclosure of the information present on the card (functionality included in the German identity card). This could allow the card to be used for certain specific purposes without having to reveal all of the identity data (for example to certify one's municipality of residence when one wishes to benefit from a reduction on entry to a municipal equipment, without revealing all the elements of identity present on the card; or to certify his age to play a game of money or buy alcohol by giving these elements of information alone). Similarly, it would be possible to use or derive separate sector identifiers (functionality included in the Austrian identity card) according to the purposes pursued,

like what the Commission recommends for e-government teleservices and could be implemented, for example, in the multi-service maps developed at the level of the territories under the name of daily life maps. The Commission encourages the Ministry, through the interministerial mission on digital identity, to reflect on future developments of the CNIe in this direction. Given the purposes pursued by the TES processing, which fall within the scope of the GDPR, and insofar as the processing is implemented on behalf of the State acting in the exercise of its prerogatives of public power, whether it relates to biometric data necessary for the authentication or the control of the identity of the persons, it must be authorized by a Conseil d'Etat decree, issued after a reasoned opinion and published by the Commission in accordance with article 32 of the law of 6 January 1978 as amended. of decree provides, in particular for a new purpose (to fight against identity theft), to extend the data currently transmitted to the national file for checking the validity of titles (DOCVERIF processing) as well as e the transfer of information to the software for drafting the procedures of the national police and gendarmerie in the event of a declaration of theft of title. In accordance with the aforementioned European requirements, this draft decree also provides for the removal of the optional nature of the collection of fingerprints, in order to record them in the identity card. The draft decree calls, under these conditions, for the following observations. On the purpose of combating identity theft The Commission recalls that under the terms of Article 1 of Decree No. 2016-1460 of 28 October 2016 referred to above, the TES file must allow the establishment, issuance , the renewal and invalidation of national identity cards […] and passports […], as well as preventing and detecting their falsification and counterfeiting. The Council of State considered that […] this processing is only intended to allow the processing of applications relating to these titles and to prevent and detect their falsification and counterfeiting. The creation of such processing, intended to preserve the integrity of the personal data necessary for the issue of identity and travel documents for the purposes of securing the issue of these documents and improving the effectiveness of the fight against fraud and which, moreover, facilitates, by the centralization of the data collected, the procedures of the users, is thus justified by a reason of general interest (Council of State, 10th - 9th chambers combined, 18/10/2018 , 404996). Article 9 of the draft decree completes the purposes pursued by the TES processing in order to make it possible to fight against identity theft, which is an extension of the current purposes. The Commission notes that this formulation of the purposes of the processing , which corresponds to uses that have existed since the beginning, had been mentioned in its previous opinions. However, it calls on the ministry to clarify that this is identity theft in connection with the fraudulent use of identity documents. It also stresses that, insofar as the TES processing is intended to collect the biometric data of nearly the entire French population, it is

important that the Ministry and the ANTS, now joint controllers of the processing, be particularly vigilant as to compliance with the purpose of authentication of this processing and that access to it can only be done by the identity of the holder of the identity document. It recalls that the Council of State has ruled that in accordance with its purpose of authentication, access to this processing can only be done by the identity of the holder of the identity document, excluding, because of the the very operating methods of the processing, of any research based on the biometric data themselves . On the retention period of fingerprints Article 10-3 of Regulation 2019/1157 of 20 June 2019 referred to above provides that unless they are necessary for the purposes of the processing in compliance with Union law and national law, the biometric identification elements stored for the purpose of personalizing identity cards or residence documents are kept in a very secure manner and only until the date of delivery of the document and, in any case, no more than four -ninety days from the date of issue of the document. After this period, these biometric identification elements are immediately erased or destroyed. As a preliminary point, the Commission observes that other European countries (such as Belgium and Germany), some of which have several years' experience in the use of cards fitted with electronic components, store biometric data in a central database for a period not exceeding the ninety days provided for by the aforementioned Regulation 2019/1157 and do not use a centralized database containing fingerprints to combat fraud and identity theft. The French Government has chosen to keep the currently existing database and to provide, by regulation, that all personal data relating to the CNIe is kept for a period of fifteen years (article 14 of the draft decree). . This choice is not contrary to Article 10-3 of the European Regulation, clarified by its recital 22, which reserves the possibility of longer storage when this is necessary for the purposes of processing the same data provided for by law. national. In doing so, the draft decree lowers the retention period of this data, to align it with the validity period of the new identity cards. Asked about the proportionality of this new retention period, the ministry specified that the retention biometric data in the TES database beyond the issuance of the identity document to the applicant is justified by the need to fight against the improper obtaining of a title and, in particular, against the phenomenon of identity theft as part of the issuance process. He also indicated that the possibility for an individual to usurp an identity and use an authentic document represents a serious risk which should be taken into account by transmitting several examples of possible scenarios (request for a document by presenting a civil status obtained fraudulently and by usurping the identity of the person concerned, request for renewal of a lost or stolen title by alleging a usurped identity, mimetic fraud, etc.). While the Commission notes that the retention periods provided for by the draft decree correspond to the period of validity of the title, as is already the case since 2016, it stresses that the use of a new type

of identity card including the integration of an electronic component, which will a priori make it possible to reduce the hypotheses of documentary fraud, could have led to a reassessment of this duration. However, it takes note of the clarifications provided by the Ministry according to which it is possible that identity theft is based, in practice, on the presentation of a stolen or found ticket whose electronic component has been deliberately damaged and whose photograph looks like the usurper. The Commission also takes note of the clarifications provided relating to the fact that in the event of suspicion of fraud, the documents required to study a usurpation file include the fact that previous titles may have been invalidated or refused. The Commission also notes that these retention periods have been admitted to litigation by the decisions of the Council of State already mentioned (CE, Ass., 26 Oct. 2011, No. 317827, Rec.; CE, 10/9, 18 Oct. 2018, No. 404996). It also points out that the draft decree, which reduces the period of validity of the CNI in accordance with the provisions of the aforementioned European regulation of 20 June 2019, also provides that the retention periods for data in the TES processing relating to the permits already issued , remain unchanged. However, it highlights the difficulties related to a good overall understanding of the retention periods adopted insofar as it is necessary to refer to the provisions of the draft decree appearing under the transitional provisions. In this context, the Commission draws the attention of the ministry as well as of the ANTS to the need to ensure the legibility of the system envisaged for the persons concerned. On the possibility of requesting the deletion of the digitized image of the fingerprints under digital form The Commission notes that Article 3 of the draft decree provides for the possibility for the person concerned to request that the digitized image of their fingerprints not be kept for processing beyond a period of eighty - ten days from the date of issue of the permit or the date of refusal of this issue by the examining body, the paper copy of the fingerprints then being kept by the ANTS for a period of fifteen years. The Commission notes that Although the retention in paper format of the applicant's fingerprints is not new, it calls for the following observations in the context of the amendments envisaged. On the one hand, the Commission accepts favorably the possibility of shorter storage of biometric data in a centralized database. To allow the expression of this choice, a specific form will have to be proposed to the applicant (on paper or put online) and will have to be adapted to the new regulatory context. The Commission recalls that the information to the persons concerned must be delivered, in accordance with Article 12 of the GDPR, in a concise, transparent and easily understandable way, in particular for any information intended specifically for a minor. It recalls, in any case and to the extent that personal data will be collected through this form, that it must include information relating to the applicable regulations on the protection of personal data. On the other hand, the Commission notes

that Article 15 of the draft decree, which relates to the nature of the information provided to the applicant when applying for a title, is intended to inform him of the possibility actually offered to him of refusing the conservation in TES of the digitized image of his fingerprints beyond a maximum period of ninety days, does not refer (including by the subject of a reference) to the provisions of the decree of October 22, 1955 referred to above relating to the conservation, of a paper copy of these same data. It considers that for purposes of better readability of the system as a whole, the draft decree could be supplemented in this sense. Finally, it notes that the removal of fingerprints at the end of the ninety-day period , when the applicant has requested it, is carried out manually by authorized agents of the ANTS. The Commission recommends that this solution remain transitional and that the necessary modifications be planned and implemented to allow automated deletion of data at the end of the retention period. On the interconnection with the national file for checking the validity of documents (DOCVERIF) Article 12 of the draft decree provides that the TES processing transmits to the national document validity check file, the numbers of the documents issued, the type of document, the surname, first names, date and place of birth of the holder as well as the date of issue and mention of the valid or invalid nature of the document and, where applicable, the reason for its invalidity with mention of the date of the event. Although the transmission of data resulting from TES processing to DOCVERIF has already been planned and regulated since 2016, the Commission recalls that it is currently limited to the numbers of the documents issued as well as the indication relating to the type of document. It also recalls that the civil status data of the holder of the document (surname, first names, date and place of birth) are only transmitted to DOCVERIF in the event that the identity document is declared lost, stolen or invalidated in TES. It also notes that no biometric data is intended to be transmitted in this context. In general, the Commission recalls that to ensure the strict proportionality of this transmission, only the data useful for the achievement of the pursued purpose must be recorded. It notes that the proposed modification leads, in a systematic way, to the transmission of information to the DOCVERIF file, by removing any criterion as to the status of the title (deletion of the mentions lost, stolen or invalidated). Questioned on this point, the ministry specified that the only confirmation of the validity of the number of a title does not make it possible to guarantee that the title was not falsified and that the envisaged modification aims to allow, with the aim of fighting against documentary fraud, to check that the civil status data appearing on the suspect title correspond to those of the authentic title recorded in TES and transmitted to DOCVERIF. The Commission notes that the systematic transmission of data from the TES would, for example, make it possible to detect any falsifications of the civil status appearing on an identity document whose number is still valid. Without calling into question the principle of these

developments with regard to the clarifications provided, the Commission notes first of all that this modification will lead to an increase in the volume of data transmitted to the DOCVERIF processing. It recalls that this modification must not lead to the DOCVERIF processing, which pursues purposes distinct from those of TES, becoming a mirror database of the latter. Under these conditions, the Commission invites the Ministry and the ANTS to take all necessary measures to ensure strict compliance with the conditions for the implementation of each of these files. Finally, if it is aware of the operational constraints linked to the implementation of technical solutions which could make it possible to meet the pursued objective of combating fraud, without however leading to all civil status data being transmitted for DOCVERIF processing, it nevertheless invites the Ministry as well that the ANTS to initiate a reflection on this point, through, for example, the generation at TES level of an electronic signature certifying the title data without transmitting a copy and to carry out a feasibility study on such a opportunity. In any case, the Commission stresses that, failing this article of the draft decree to specify the purposes for which the data will be transmitted to DOCVERIF, this Your transmission must only meet the conditions for its collection as provided for by the TES decree. It also recalls that the decree of August 10, 2016 authorizing the creation of DOCVERIF, on which it will have to decide, will have to be modified in order to provide for the collection of this data. On the transmission of data to software for drafting police procedures and the national gendarmerie Article 13 of the draft decree regulates the possibility of transmitting data resulting from the TES processing to the software for drafting the procedures of the national gendarmerie and police, in the case of the collection of declarations of theft of national cards of identity and passports. Civil status data, information relating to the issue of the permit (date, place, authority, type and number) as well as the digitized image of the face of the holder of the permit are transmitted in particular. The Ministry has also specified that only information relating to documents corresponding to the exact civil status entered by the agent in charge of the complaint will be transmitted. to be implemented by the end of 2021. It also emphasizes that the planned functionalities will require the modification, if necessary, of the regulatory acts governing this processing. It notes that these transmissions are justified in particular by the need to make the information transmitted to the Schengen Information System (SIS). Without calling into question the operational usefulness of such a development, the Commission recalls that when the Council of State, in its aforementioned decision of October 18, 2018, ruled on the legality of the decree relating to TES processing, it had specifically noted that the interconnection of the processing system is only planned with the Schengen and INTERPOL information systems and only relates to non-nominal information relating to the numbers of lost or stolen passports, the issuing country and the blank character or personalized

document. At this stage and if it takes note of the details provided by the ministry according to which the data transmission carried out must allow, during the collection of a complaint for theft of a national identity card or a passport, the software of drafting of the procedures to obtain from TES the number of the pass concerned as well as the information making it possible to verify that the complainant is indeed the legitimate holder (visualization of the photograph of the pass), the Commission nevertheless wonders about the advisability, in this situation, to transmit all the data mentioned in article 13 of the draft decree - and not only the information relating to the issue of the title - in order to subsequently transmit complete reports to the SIS. cause and more particularly with regard to the transmission of the digitized image of the face of the holder, the draft decree specifies that it is transmitted according to methods which do not allow its registration larly in the aforementioned software. Asked about this, the ministry said the photograph will be displayed as a pop-up without download or save functionality. It will allow the agent receiving the complaint to verify that the identity declared by the complainant is the one appearing on his identity document (CNIe or passport). In this respect, the Commission invites the Ministry to reinforce the information of the agents concerned as to compliance with the prohibition on recording in any way whatsoever (and for example via a screenshot) the photograph of the person concerned. . It also invites the Ministry to consider the possibility of affixing a watermark to the photograph displayed, thus making it possible to dissuade any illegitimate recording by ensuring better traceability and thus guaranteeing strict compliance with the conditions of implementation previously described. On the other interconnections The TES processing is intended to feed the national part of the second generation Schengen Information System (N-SIS II), as well as the Stolen and Lost Travel Documents (SLTD) processing managed by Interpol, of data relating to lost, stolen or invalidated. This input, which is carried out automatically, implies that the TES processing transmits data, with the exception of biometric data, as soon as a declaration of loss or theft is recorded. In this observation, the Commission nevertheless underlines that, with regard more particularly to the SLTD database, data may be transmitted outside the European Union. It recalls that data transfers to third countries can only be carried out subject to compliance with the conditions set out in Articles 45 and following of the GDPR. In the absence of an adequacy decision adopted by the European Commission, such transfers may only be made subject to appropriate safeguards being implemented in accordance with Article 46 of the GDPR, taking into account the circumstances of the transfer. as well as the recommendations of the European Data Protection Board on the measures that complement the transfer tools to ensure compliance with the EU level of protection of personal data.On the security of the processingGenerally, the Commission underlines that the renewal of the

format of the identity card used for approximately thirty years will bring a significant reinforcement of the security of the title, in particular by the addition of the secure electronic component. It also points out that in its opinion of February 23, 2016, the Council of State recalled that, given the scope and the particularly sensitive nature of the TES, which could collect data relating to the identity as well as the photographs digital fingerprints of several tens of millions of people, the implementation of this computer processing of data had to comply with strict security rules. The Commission points out that the implementation of adequate security measures requires in particular to ensure the effectiveness of the access restrictions provided for by the normative framework in force, the traceability of consultations as well as the prevention of any misappropriation of data. It notes that with regard to the electronic component recording identity data, that -this is similar to the one used for the passport since 2008 according to the specifications of the ICAO (International Civil Aviation Organization) standard for documents travel.The Commission also notes that the National Information Systems Security Agency (ANSSI), during the audits it carried out concerning TES processing, issued a certain number of recommendations.Among the recommendations implemented implemented, the Commission notes that a log of legal requests has been made. In the state of the documentation, it is not indicated that the agents authorized to respond to legal requests cannot also be authorized to manage these traces. The Commission considers it essential that such a rule be made explicit and implemented if this were not the case. The Commission includes documentation that some of the recommendations have otherwise not been implemented and thus: the recommendation 1 advises not only to encrypt the biometric data in base, which has been implemented by the ministry, but also to entrust the means of decryption to a third party so that neither the ministry nor the third authority can, alone, have the means to decipher the data to respond to legal requisitions. This second part of the recommendation does not seem to have been implemented by the ministry at this stage or provided for in the action plan. This recommendation makes it possible both to raise the level of data security and protection of privacy, as well as to limit the risk that the processing is transformed into a basis for identifying individuals. Given these elements, the Commission considers it necessary that such a measure, also recommended by ANSSI, be implemented; recommendation 4 provides for raising the level of security requirements for service contracts. Its implementation having to be integrated during the renewal of the contract, the Commission understands that this is provided for in the ministry's action plan. The Commission considers it essential that these specific recommendations be taken into account and notes that it is what the Ministry provides for almost all ANSSI's recommendations. It also considers that the scope of security audits should be extended, so as to include the interconnections, links and reconciliations

implemented. The Commission notes that several measures of the action plan were indicated for the end of 2020 in the version of the data protection impact assessment (DPIA) of December 2020. While it notes a certain delay in their implementation, it recommends that the ministry update the planned deadlines and plan an evaluation of their implementation at the end of 2021. Finally, the Commission notes that traces, both systems and applications, are generated are processed and kept for a period of five years. The Commission recalls that its recommendation on the management of logs and technical logs is to implement a retention period of six months, except to be able to prove that certain risks can only be covered by an extension of this period. .Similarly, in order to be able to ensure the integrity and availability of the data, a system of centralization of the traces is recommended as well as the implementation of a proactive mechanism of automatic control of the logs contributing to the detection of abnormal behavior by the automatic generation of alerts.The PresidentMarie-Laure DENIS