Deliberation 2018-342 of October 18, 2018Commission Nationale de l'Informatique et des LibertésNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Friday May 17, 2019NOR: CNIX1911892XDeliberation No. 2018-342 of October 18, 2018 providing an opinion on a draft decree authorizing the creation of automated processing to authenticate a digital identity electronically called "Application for reading the identity of a citizen on the move" (ALICEM) and modifying the entry and residence of foreigners and the right to asylum (request for opinion no. 18008244) The National Commission for Computing and Liberties, Seizure by the Minister of the Interior of a request for an opinion concerning a draft decree authorizing the creation of automated processing allowing the delivery of a digital identity called Application for reading the identity of a citizen on the move (ALICEM); Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to the automatic processing of personal data; 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; Having regard to Regulation (EU) 910/2014 of the European Parliament and of the Council of July 23, 2014 on electronic identification and services of trust for electronic transactions within the internal market and repealing Directive 1999/93/EC (e-IDAS); Having regard to Commission Implementing Regulation (EU) 2015/102 of 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, paragraph 3, of the aforementioned Regulation (EU) No 910/2014; Having regard to Directive (EU) 2016/680 of the European Parliament and of the Council of April 27, 2016 re on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties ;Having regard to the code for the entry and stay of foreigners and the right to asylum, in particular its articles R. 311-13-1, R. 611-1 and following;Having regard to the postal and electronic communications code, in particular its article L. 102; Having regard to law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms; Having regard to decree n° 2005-1309 of October 20, 2005 modified taken for the application of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to Decree No. 2016-1460 of October 28, 2016 authorizing the creation of a processing of personal data relating to passports and national identity cards (TES); Considering the decree of July 24, 2015 creating processing of personal data by the interministerial department of information and communication systems of a teleservice called FranceConnect; Having regard to the decree of August 10, 2016 authorizing the creation of

automated processing of personal data referred to as DOCVERIF; Having regard to deliberation no. 2015-254 of July 6, 2015 providing an opinion on a draft order establishing an automated processing of personal data by the interministerial department of information and communication systems of a teleservice called FranceConnect; Considering the deliberation n° 2016-292 of September 29, 2016 for opinion on a draft decree authorizing the creation of a processing of personal data relating to passports and national identity cards (TES); deliberation no. 2016-218 of July 21, 2016 giving an opinion on a draft decree authorizing the creation of an automated processing of personal data called DOCVERI F; After hearing Mr. François PELLEGRINI, commissioner, in his report, and Mrs. Nacima BELKACEM, government commissioner, in her observations, Issues the following opinion: The Commission has been seized by the Minister of the Interior of a request for an opinion on a draft decree by the Conseil d'Etat authorizing the creation of an automated process allowing the issuance of a digital identity called Application for reading a citizen on the move (ALICEM). This processing, implemented by the Department of Modernization and Territorial Action, should allow adults holding a biometric passport or an electronic foreign residence permit to create a digital identity from their permit. of identity on its mobile application and then to identify and authenticate itself to online service providers. It notes that the planned processing is based on a facial recognition system making it possible to verify the accuracy of the identity alleged by the person using this device, the digital identity thus created can be used to identify and authenticate themselves with online services. Given its purposes, the Commission considers that the ALICEM processing falls within the scope of the Regulation (EU) 2016/679 of April 27, 2016 referred to above (hereinafter GDPR) and must be examined in the light of these provisions. It also recalls that Article 9.4 of the GDPR provides that national law may introduce additional conditions with regard to the processing of biometric data. The processing of personal data, which must be considered taking into account the general economy of the device described below as implemented on behalf of the State acting in the exercise of its prerogatives of public power, relates to biometric data necessary for the authentication or the control of the identity of the people. It must therefore be the subject of a decree in the Conseil d'Etat, issued after a reasoned opinion and published by the Commission in accordance with the provisions of article 27 of the amended law of 6 January 1978. It also notes that the this draft decree, which was accompanied by an impact analysis, also modifies the code for the entry and stay of foreigners and the right to asylum (CESEDA). In particular, it is planned to modify article R. 611-1 of the CESEDA to allow the linking of the AGDREF 2 processing (Application for managing the files of foreign nationals in France) with the DOCVERIF processing and thus allow the transmission to DOCVERIF of data relating to the titles of foreign nationals.

This connection does not in itself call for any particular observation. As regards the AGDREF 2 processing, the Commission recalls that its main purpose is to guarantee the right of residence of foreign nationals in a regular situation and to fight against illegal entry and stay in France of foreign nationals . This processing thus constitutes the main file for the administrative management of foreigners in France and in particular allows the management, by the prefectures, of the files of foreign nationals, the production of residence permits and the management of removal measures. With regard to these elements , the Commission considers that the AGDREF 2 processing falls under the provisions of Articles 70-1 et seq. of the Data Protection Act which transposed the aforementioned directive of 27 April 2016 and that this amendment falls under the said provisions in that it falls fully in the prevention and detection of criminal offences. In accordance with article L. 611-5 of the CESEDA and article 30-II of the amended law of January 6, 1978, the changes made to this processing must be subject of a decree in Council of State taken after opinion of the CNIL. In general, it also recalls that pursuant to Article 70-4 of this same law, processing that is likely to create a high risk for the rights and freedoms of natural persons must be subject to an impact assessment on the protection of personal data (DPIA). The Commission also recalls that the processing operations presenting a high risk having been the subject of a prior formality before 25 May 2018 are not however immediately subject to the performance of a DPIA, unless the conditions for implementing the this processing has subsequently been the subject of one or more substantial modifications. In this respect, it notes that with regard to its purposes and the biometric data it contains, the AGDREF 2 processing is, by entail high risks for the persons concerned. On the other hand, it considers that the modification examined (addition of a link with DOCVERIF processing) is not substantial. The Commission therefore considers that the modification of the processing submitted to it does not require, at this stage and given the circumstances of the case, the performance of an impact analysis in the context of this referral. purpose and functionalities of the processing Article 1 of the draft decree provides that the purpose of the processing is to offer French nationals holding a biometric passport and foreign nationals holding a residence permit comprising an electronic component to identify themselves and to authenticate with public or private bodies, using a mobile phone with an Android operating system and equipped with contactless technology. The Commission notes that Article 1 of the aforementioned draft decree does not mention the creation and delivery of the digital identity (or means of electronic identification) from the mobile application, even though this constitutes one of the final characteristics of the planned processing and that it is from the creation of the digital identity that an individual will be able to identify and authenticate himself to access online services. Article 1 should therefore be amended in order to mention, under

the purposes pursued, the creation of a digital identity. Firstly, with regard to the creation of a digital identity, the Commission notes that this is subject to the creation of an account on the ALICEM application. It specifies that the creation of this account requires the entry, by the person concerned, of his e-mail address and his mobile telephone number, which are verified by sending a unique activation link to the e-mail address and a single-use password by a short message to the mobile telephone number. Article 2 of the draft decree specifies in this respect that the processing mentioned in Article 1 applies to French nationals holding a biometric passport and to foreign nationals holding a residence permit comprising an electronic component in accordance with article R. 311-13-1 of the CESEDA. The persons concerned with their document - a biometric passport for French nationals and a electronic foreign residence permit for foreign nationals - then proceed to the optical reading of the data of the MRZ strip of the title by photographing it using their mobile equipment. Contactless technology t must allow the reading of the title data recorded in the electronic component, namely the civil status data, the address and the photograph of the user. The Commission notes that the digitized image of the fingerprints is not read by the device and will therefore not be used or recorded in the planned processing.A query of the DOCVERIF processing, which is the subject of a separate referral , is carried out in order to confirm the validity of the identity document. In this respect, the Commission notes that a user with an invalid title will not be able to proceed with the creation of a digital identity. Finally, it notes that access to the ALICEM application is secured by a password code. security (PIN code) defined by the user of the application and which will be required to access the application and to authenticate with the online services concerned. The Commission notes that once the account has been created, its activation is subject to a verification process of the alleged identity in order to ensure that the person who created the account corresponds to the one holding the title. It notes that this verification takes the form of a biometric processing of facial recognition from a video taken in real time by the user who must perform a series of challenges imposed by the application (blinking of the eyes, movement of the head, facial movement, etc.). This video is then sent to the servers of the National Agency for Secure Titles (ANTS). The Commission notes that these challenges are used to verify that it is indeed a person in possession of the mobile phone (so-called dynamic facial recognition phase). Finally, a photograph is extracted from the video to make a comparison with the portrait extracted from the title (so-called static facial recognition phase). Following the satisfactory completion of the activation phase, the digital identity is generated. Access to the ALICEM account can therefore be done via the mobile application or the website dedicated to the application.Secondly, the Commission notes that once created and activated, users of the device will be able to identify themselves and authenticate

with online service providers. It thus notes that people can opt for the ALICEM digital identity directly with online service providers or through the FranceConnect device, previously examined by the Commission. Initially, the user will only be able to select the ALICEM digital identity to access a service provider via FranceConnect. The Commission notes that identification and authentication to online services do not include by themselves for the processing of biometric data, both for access to a service requiring a high level of security within the meaning of the aforementioned e-IDAS regulation and for access to a service requiring a substantial or low level of security within the meaning of this same regulation. The Commission notes that an RGAA (General Administration Accessibility Framework) audit was carried out in 2017. Subject to the foregoing, the Commission considers that the purposes pursued by the ALICEM processing are determined, explicit and legitimate, in accordance with the provisions of Article 5-1-b) of the GDPR. On the processing of biometric data The Commission notes that the ministry intends to apply the consent under the legal basis allowing the implementation of the ALICEM system. presented, that a distinction should be made between the creation of an ALICEM digital identity and the step of verifying the identity claimed by the person to activate the ALICEM account, this activation being subject to the processing of biometric data .In this respect, the Commission considers that if there is indeed express consent to the creation of an ALICEM identity, the mobilization of consent to base the use of biometrics e for the purpose of verifying the accuracy of the identity alleged by the person creating his digital identity, and thus activating the ALICEM account, raises questions. The Commission recalls that Article 9.1 of the GDPR poses a principle of prohibiting the processing of certain categories of so-called sensitive data, including biometric data. Article 9.2 specifies that the aforementioned prohibition may be waived in certain cases, in particular when (a) the data subject has given his explicit consent to the processing of such personal data for one or more specific purposes or (g) where the processing is necessary for important reasons of public interest. Firstly, it recalls that to be valid, the consent in question must be free, specific, informed and unequivocal in accordance with Article 4-11) of the GDPR. In this respect, the Commission notes that in the context of of the planned processing, people are invited prior to the process of creating the digital identity to consent or not to the processing of their biometric data. It also notes that the refusal to carry out facial recognition at the stage of the ALICEM account activation procedure prevents the creation of the ALICEM digital identity. In view of the above, the Commission recalls that consent does not is likely to constitute the legal basis for the processing of biometric data only in the event that the person concerned has control and a real choice concerning the acceptance or refusal of the proposed conditions or the possibility of refusing them without suffering any prejudice. In this respect, the Commission

considers, in accordance with the position adopted by the Article 29 Working Party (G29) and taken up by the European Data Protection Board (EDPB) in the context of its guidelines on consent that, in the event that the provision of a service is subject to consent to the processing of personal data, this consent is only voluntary if the processing of these gifts born is strictly necessary for the provision of the service requested by the person, or if an alternative is actually offered by the data controller to the person concerned. In this case, the refusal to process biometric data prevents the activation of the account, and nullifies the initial consent to the creation of the account. However, the need to use a biometric device to verify the identity of a person in order to achieve the high level of guarantee of digital identity, within the meaning of the e-IDAS regulation, has not been established. , given in particular the possibility of using alternative verification systems (see below). Furthermore, the Commission notes that the Ministry does not, in this case and at present, offer an alternative to facial recognition to create a high-level digital identity within the meaning of the e-IDAS regulation. As a result, the creation of an ALICEM digital identity is subject to a facial recognition process without any other equivalent alternative being provided to allow the issuance of a digital identity by this application. above, the consent to the processing of biometric data cannot be regarded as free and as therefore likely to lift the prohibition imposed by Article 9.1 of the GDPR.Secondly, the Commission notes that in this case, it has not been argued or demonstrated that the proposed processing would be necessary for reasons of substantial public interest. It considers in particular that while it cannot be ruled out from the outset that this processing may be in the context of important public interest reasons by promoting, at the initiative of the State, the securing of electronic identification, the characterization of such a reason, as well as the assessment of the necessity mentioned in (g) of Article 9.2. in any event, would require additional demonstration elements from the Ministry. verify the accuracy of the identity claimed by the person creating his account, and thus ensure the effective freedom of consent of the persons concerned to the processing of their biometric data at the time of activation of their ALICEM account. These alternative solutions could in particular take the form of a face-to-face meeting (such as a trip to the prefecture, to the mayor, or to another public service welcoming the public directly), manual verification of the video and the photograph on the title (such as a sending of the video to the ANTS server and verification of the identity operated by an agent) or a live video call with an ANTS agent. The Commission considers, moreover, that the development of these alternative solutions is also likely to enable a greater number of people to use the ALICEM system and, in particular, with regard to those who would not be able to meet the various challenges proposed.On the data processedArticle 7 of the draft decree lists the categories of data recorded in the planned processing, namely: data allowing

the identification of the user, data allowing the identification of the title held by the user , the data relating to the history of transactions associated with the ALICEM account and the unique identifier of the notification service for the purposes of identifying the mobile telephone. The Commission notes in this respect that certain personal data are recorded on the equipment mobile of the user and others on the central server of the ANTS. This sharing allows in particular that only the identification data be kept on the user's mobile equipment and therefore under his exclusive control. As data allowing the identification of the user, civil status data will be recorded (name, if applicable surname, first name, date and place of birth, nationality, sex, size and color of eyes and postal address) as well as the photograph of the person. The Commission notes that this data comes directly from the contactless reading of the electronic component of the ticket during the enrollment phase. It considers that these data, making it possible to certify the identity of the holder of a title, are relevant, adequate and not excessive with regard to the purpose relating to the creation of the digital identity of the person concerned. notes that the digitized image of the fingerprints contained in the electronic component of the title will not be saved either in the mobile application or in the central server of the ANTS in accordance with Articles 5 and 6 of the draft decree. the person's e-mail address and mobile phone number are also collected. These data, making it possible to initiate the process of creating the ALICEM account, do not call for any specific observations from the Commission. The Commission also notes that the biometric data relating to the user's video and photograph taken with his equipment are required for facial recognition biometric processing. They are therefore adequate, relevant and not excessive. It acknowledges that this data will be erased as soon as the comparison is completed. With regard to data relating to the history of transactions, carried out via FranceConnect and recorded in the processing, the Commission recalls that this system guarantees a principle of strict separation between the identity provider and the service provider, so that the identity provider does not know which service provider has used the identity. The Commission notes that the data mentioned in a) to d) of 3° of article 7 of the draft decree, which correspond to the data relating to the history of transactions making it possible to know the service provider, will not be transmitted and therefore kept in the processing when the transactions are carried out by the intermediary of FranceConnect . Finally, the data allowing the identification of the pass held by the user and the unique identifier of the notification service for the purpose of identifying the mobile telephone do not call for any particular observations by the Commission. Subject to what foregoing, the Commission considers that the data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in accordance with the provisions of Article 5-1-c of the GDPR.On retention periods Article 11 of the

draft decree provides for different retention periods depending on the data concerned. The data stored on the mobile equipment of the data subject, i.e. data relating to identification and data relating to transaction history, are deleted when the application is uninstalled, which does not call for any particular observation. Article 11. II of the draft decree specifies that the data recorded es on the central server are kept until the application is uninstalled by the user or seven years from the last use of the ALICEM account. The Ministry indicated on this point that this seven-year period complies with ANSSI requirements pursuant to the e-IDAS regulation. Finally, said article provides for two specific retention periods in the event of non-completion of the creation activation of the ALICEM digital identity (twenty-four hours if the creation of the account has not been completed and seven days if the account has not been activated), which do not call for any observation on the part of the Commission. On the authorized persons and the recipientsArticle 8 of the draft decree specifies that the agents of the services of the Ministry of the Interior responsible for the project management of the processing, as well as the agents of the ANTS responsible for the control of processing, individually designated and duly authorized by their director, can access all or part of the data and information recorded in the processing, by reason of their attributions and within the limit of the need to know. the access of these persons to the data seems justified by the operational implementation of the ALICEM system, the Commission recalls that the identification data mentioned in article 7 1° of the draft decree are exclusively kept on the mobile equipment, which cannot, in principle, access the persons mentioned above. It therefore considers that the draft decree should be amended in order to explicitly exclude access to the data contained in the user's mobile equipment. The Commission takes note of the modification of the draft decree in this sense. With regard to recipients, Article 9 of the draft decree provides that FranceConnect, the teleservice providers bound by agreement to FranceConnect and the teleservice providers bound by agreement at ANTS may be recipients of the data. The Commission notes that the FranceConnect system is not a recipient strictly speaking, but a processing operation allowing intermediation between ALICEM and the service provider concerned: by transmitting the necessary identification elements to the service provider, it guarantees the identification and user authentication. It considers that the draft decree should be clarified on this point. In this respect, it takes note of the upcoming change, namely the mention of the Interministerial Directorate for Digital and the State Information and Communication System (DINSIC) instead of FranceConnect. Article 9 II of the draft decree lists the data transmitted by ALICEM to the recipients. The Commission recalls on this point that each of the recipients can only receive the data strictly necessary to allow verification of the identity or identity attributes required to access the service concerned, and not all of the data listed in that article . It

therefore considers that the draft decree should be supplemented in this sense.On information and the rights of the persons concernedArticle 13 of the draft decree provides that information for the user concerning the use of a device static facial recognition and dynamic facial recognition will be delivered to the data subject at the time of opening the account. The Commission notes that the data subject is informed by the provision of general conditions of use of the application and that these must be expressly validated to proceed with the creation of the account. The data subject is also informed of the processing of his data with each request for identification and authentication from a service provider. The Commission also notes that the content of the information was not brought to its attention. precisely and that the draft decree is limited to information on the use of facial recognition. It therefore draws the Ministry's attention to the importance of providing information in a concise, transparent, understandable and easily accessible manner, in clear and simple terms, in accordance with Article 12 of the GDPR. In addition, the Ministry has indicated the introduction of specific information concerning consent to the processing of biometric data, which the Commission takes note of. Article 14 of the draft decree provides that the rights of access, rectification, limitation and erasure are exercised with the ANTS, which does not call for any specific comments from the Commission. Finally, the Commission notes that there is provision for a mechanism aimed at the portability of data for the persons concerned. She nevertheless wonders about the effectiveness of this in the event of renewal of a title. Indeed, the renewal of the title implies the loss of the traces relating to the old title and this, without possibility for the user to recover them. In this context, the Commission invites the Ministry to consider a solution to allow the user to recover his data in this case. It takes note of the Ministry's commitment to reflect on this point, which could usefully be brought to its attention. On security measures As a means of identification and high-level authentication, the impact of security incidents on the persons concerned can be particularly serious. In this specific context, the Commission notes that the data controller implements a set of measures to reduce the likelihood of such incidents. The Commission notes that the data stored by the application, with the exception of preference data (in particular resulting from a configuration by the user), are encrypted with algorithms and key management procedures in accordance with appendix B1 of the general security reference system. In addition, data exchanges between the application and the ANTS servers are carried out via encrypted communication channels and ensuring both the integrity of the data and the authentication of the source and the recipient. authorization profiles are planned in order to manage the administration of the system while respecting the principle of access to data as needed, which does not call for any particular observation. The Commission notes that the data controller implements a password policy, for users as well as

for administrators, in accordance with deliberation n° 2017-012 of January 19, 2017 adopting a recommendation relating to passwords modified by deliberation n° 2017 -190 of June 22, 2017, in particular with regard to the storage of passwords. In addition, administrator access to the system is implemented in accordance with the Ministry's security reference system on remote access. Article 12 of the draft order provides that information relating to creation, consultation, updating update and deletion of data are kept for seven years from their registration. The Commission notes that two types of information are kept as logs: on the one hand, data relating to transactions carried out by the user and, on the other hand, those relating to enrolment. demonstrate the proper enrollment of the user (SOD), the Commission considers that the expected duration of seven years is a security requirement formulated by the National Agency for Information Systems Security (ANSSI) which does not call for observation on his part. On the other hand, the Commission considers that keeping the traces of access to the ALICEM application, as well as the history of the transactions carried out for the same duration, is manifestly disproportionate. It therefore recommends keeping this data for a maximum period of six months. administrator privileges available to users, thus excluding so-called rooted equipment. The Commission nevertheless wonders about the need for such a restriction, the choice of users to have administrator rights on their equipment can also be motivated by the need to increase its security. In this regard, the Ministry indicated that while for a minority of users having rooted equipment can increase security, for the majority of users having such equipment can constitute an additional security risk, which the Commission takes note.The Commission notes that to limit the likelihood of identity theft by falsification of enrolment, the system implements various guarantees, including analysis of the video stream or random challenges of facial recognition dynamic.Finally, the Commission notes that obtaining qualification of the ALICEM device with regard to the e-IDAS regulation is currently being assessed by ANSSI.Subject to the previous observations, the security measures described by the person in charge processing comply with the security requirement provided for in Articles 5.1.f and 32 of the GDPR. The Commission recalls, however, that this obligation requires the update of the AIP D and its security measures, to take into account the regular reassessment of the risks.The PresidentI.FALQUE-PIERROTIN