Deliberation SAN-2021-016 of September 24, 2021 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday September 30, 2021 Deliberation of the restricted committee n°SAN-2021-016 of 24 September 2021 concerning the Ministry of the InteriorThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, president, Philippe-Pierre CABOURDIN, vice-president, of Mesdames Anne DEBET and Christine MAUGÜE and of Messrs Alain DRU and Bertrand du MARAIS, members; Having regard to Convention No. 108 of the Council of Europe of 28 January 1981 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 relating to the protection of personal data and the free movement of such data; Having regard to Directive (EU) 2 016/680 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 by the competent authorities for the purposes of prevention and detection of criminal offenses, investigations and prosecution in this area or the execution of criminal penalties, and the free movement of such data; Having regard to law no. 78-17 of 6 January 1978 relating to data processing, files and freedoms, in particular its articles 20 et seq.; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. July 4, 2013 adopting the internal regulations of the National Commission for Computing and Liberties; Considering decision no. 2019-004C of December 20, 2018 of the President of the National Commission for Computing and Liberties to instruct the Secretary to proceed or to carry out a verification mission of the "Automated fingerprint file" processing implemented by the central service of the technical and scientific police at the Ministry of the Interior; Having regard to the decision of the President of the National Commission for information technology and freedoms appointing a rapporteur before the restricted committee, dated February 26, 2021; Having regard to the report of Mrs. Sophie LAMBREMON, reporting commissioner, notified to the Ministry of the Interior on April 9, 2021; Having regard to the written observations submitted by the Ministry of the Interior on May 25, 2021; Considering the oral observations made during the restricted training session, on July 1, 2021; Considering the other documents in the file; Were present, during the restricted training session: - Mrs. Sophie LAMBREMON, Commissioner, heard in her report; As representatives of the Ministry of the Interior:- […] As Government Commissioner:- […] The training res Treinte heard, pursuant to Article 42 of Decree No. 2019-536 of May 29, 2019, […], representatives of the Ministry of Justice, Department of Criminal Affairs and Pardons (by videoconference); The Ministry of

Committee having spoken last;The Restricted Committee adopted the following decision:I. Facts and procedure1. The automated fingerprint file (hereinafter "the FAED") is a judicial police identification file listing the fingerprints of persons implicated in criminal proceedings as well as the "traces" of fingerprints found on the scenes. of felony or misdemeanor. It is managed by the Ministry of the Interior and used by the police, gendarmerie and customs services, allowing them to link a person to several identities or aliases and to link this person to previous procedures in which their fingerprints have been raised.2. In accordance with the provisions of article 2 of decree no. 87-249 of 8 April 1987 relating to the automated file of fingerprints managed by the Ministry of the Interior (hereinafter "decree no. 87-249" or "decree relating at FAED"), it is "implemented by the central technical and scientific police service at the Ministry of the Interior" .3. The FAED contains, on the one hand, "signals", which are fingerprints and palm prints taken directly from the persons concerned and accompanied by various information relating to the person to whom they belong and the context in which they were collected (sex, name , first name, date and place of birth, filiation, department that carried out the notification, date and place of establishment of the file, nature of the case and reference of the procedure, photographs of the person) and, on the other hand hand, "traces" (complete or partial fingerprints recorded at the place of commission of an offence), also accompanied by various information relating to the collection (place and date of the recording, service which carried out the recording, date and place of establishment of the file, nature of the case and reference of the procedure). Each fingerprint (recorded during a signaling operation or noted at the place of commission of an offence) accompanied by the additional information mentioned constitutes an independent "file" recorded in the FAED.4. In December 2018, the file contained nearly 6.3 million fingerprints and palm prints of people identified as suspects for crimes and/or misdemeanors, as well as 240,000 unidentified traces.5. The President of the Commission, by Decision No 2019-004C of 20 December 2018, initiated a review procedure against the Ministry of the Interior. The purpose of this procedure was to verify compliance by the Ministry of the Interior with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the Regulation") or "the RGPD"), of the amended law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter "the law of January 6, 1978" or "the Data Protection Act" ) and Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the Police-Justice Directive") in the implementation of the FAED by the central technical and scientific police service . As part of this procedure, several checks were carried out, and more specifically on the premises of the central service of the technical and scientific police (hereinafter "the SCPTS"), which ensures the daily management of the file, at the

Boulogne police station. -Billancourt, where the data feeding the FAED are collected, as well as to the court of law and the Paris Court of Appeal, whose decisions have implications for the future of FAED data. Finally, questionnaires were sent to the courts of Angers, Fort-de-France and Lons-le-Saunier as well as to the Court of Appeal of Versailles. All of these checks made it possible to verify the FAED data collection methods, their daily management, as well as their future after court decisions.6. For the purposes of examining these elements, the President of the Commission, on February 26, 2021, appointed Mrs. Sophie LAMBREMON as rapporteur, on the basis of Article 22 of the law of January 6, 1978.7. At the end of her investigation, the rapporteur, on April 9, 2021, served a report on the Ministry of the Interior detailing the breaches of the Data Protection Act that she considered constituted in this case. The rapporteur proposed to the restricted formation of the Commission to issue an injunction to bring the processing into compliance with the provisions of Articles 4, 89, 97, 99 and 104 of the Data Protection Act, as well as a reminder . It also proposed that this decision be made public and no longer allow the ministry to be identified by name after the expiry of a period of two years from its publication.8. On the same day, the Ministry of the Interior was informed that this file was on the agenda of the restricted training session of July 1, 2021.9. On May 25, 2021, the department filed observations.10. The Ministry and the rapporteur presented oral observations during the session of the Restricted Committee.II. Reasons for decisionA. On the applicable law11. Article 1 of the Police-Justice Directive defines its scope and covers any "processing of personal data by the competent authorities for the purposes of the prevention, detection, investigation and prosecution of criminal offences. matter or execution of criminal sanctions, including the protection against threats to public security and the prevention of such threats" .12. The first paragraph of article 87 of the Data Protection Act, first article of title III of the law, provides "this title applies, without prejudice to title I, to the processing of personal data implemented, for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the protection against threats to public security and the prevention of such threats, by any authority competent authority or any other body or entity entrusted, for the same purposes, with the exercise of public authority and the prerogatives of public power, hereinafter referred to as the competent authority". This Title III therefore applies to processing that meets a dual characteristic relating to its purpose, on the one hand, and to the quality of the data controller, on the other.14. Article 1 of Decree No. 87-249 sets out the purposes of FAED. According to the latter, the purposes of the processing are to: "facilitate the search and identification […] of the perpetrators of crimes and misdemeanors and to facilitate the prosecution, investigation and judgment of criminal and misdemeanor cases […] ]";"facilitate the search for and discovery

of missing protected minors and adults as well as those of adults whose disappearance is of a worrying or suspicious nature [...]";"facilitate the identification in a legal framework of deceased persons as well as the "identification of persons found seriously injured whose identity could not be established"; "facilitate the identification in an extrajudicial framework of deceased persons"; "allow the identification of a foreigner under the conditions provided for in Article L. 611 4 of the code for the entry and stay of foreigners and the right to asylum"; "allow the identification of persons within the framework of the identity verification procedure of article 78-3 of the code of procedure criminal" .15. In this case, the checks carried out concerned the use of the FAED in the context of police and judicial activities during criminal proceedings. The Restricted Committee considers that these activities fall within the scope of the purposes referred to in Article 87 of the Data Protection Act.16. The Restricted Committee also considers that, within the framework of these missions, the Ministry of the Interior must be regarded as the competent authority, with regard to Article 1 of Decree No. 2020-874 of July 15, 2020 relating to the powers of the Minister of the Interior (previously decree no. 2017-1070 of 24 May 2017).17. Consequently, the Restricted Committee considers that in this case, the FAED, when it is implemented by the Ministry of the Interior for the various purposes mentioned above, must comply with the provisions of Title III of the law Computing and Liberties.B. On breaches1. On the breach relating to the lawfulness of the processing18. Article 4 of Decree No. 87-249 draws up the exhaustive list of information that may accompany, in the FAED, the recording of a fingerprint or trace. With regard to fingerprints, this information is the sex of the person and, when known, his surname, first names, date and place of birth and elements of filiation, the department that carried out the signaling, the date and place establishment of the data sheet, the nature of the case and the reference of the procedure and the anthropometric shots. With regard to traces, this information is the place where they were recorded, as well as the date of the record, the service that carried out the record of the traces, the date and the place of establishment of the file supporting the reproduction of the traces. papillary, the nature of the case and the reference of the procedure and the origin of the information and the date of its recording in the treatment.19. Firstly, the delegation noted that additional information is processed in the FAED, such as the name of the victim or the registration number of a vehicle.20. The Restricted Committee notes that this information is recorded in the form of an image and therefore cannot be searched. It also notes, as specified by the Ministry of the Interior in the response to the sanction report, that they are only present in the "traces" sheets and not in the "signalling" sheets .21. The Restricted Committee nevertheless finds that the Ministry of the Interior processes data not covered by Decree No 87-249 and concludes that this processing is unlawful. The Restricted Committee notes, moreover, that

the Ministry of the Interior does not dispute the unlawful nature of this processing since it is announcing a modification of the regulatory framework in order to allow it, in the future, to regularly process this data which it considers necessary.22. Secondly, the delegation noted that around seven million "signalling" sheets, most of them old (sometimes dating back several decades), are kept in paper format in a dedicated room in the central department. This physical file, called "manual file", has not been updated since 2017. It includes both old files (created before the computerization of the file) and the original paper of more recent files intended to be scanned and inserted in FAED.23. The Restricted Committee notes that Article 1 of Decree No. 87-249 provides for and authorizes "the automated processing of traces and fingerprints and palm prints" and therefore does not refer to the "manual file", the latter not being automated. This processing had been created by law no. 667 of 27 November 1943 establishing a technical police service, published in the Official Journal of 28 November 1943 and article 4 of which provided for the creation of a "judicial identification service essentially responsible for searching for and recording traces and clues in the places where a criminal act was committed, for establishing and classifying the data sheets. This text was repealed by the fifth paragraph of article 58 of law no. 2001-1062 of 15 November 2001 relating to daily safety, without this text, or a subsequent text, authorizing equivalent processing.24. Therefore, the Restricted Committee notes that the retention of "signaling" sheets in paper format is not provided for by any legislative or regulatory provision and concludes that it is unlawful. The Restricted Committee considers that a breach of Article 89 of Law no. 78 17 of 6 January 1978 has thus been established.25. While it takes note of the announcement of the complete destruction of the "manual file" within the next four years, the Restricted Committee notes that no precise timetable has been announced by the Ministry of the Interior for achieving this goal and that his assertions are not supported by any evidence. It also considers that the four-year period put forward by the Ministry of the Interior cannot be accepted, given the age of the files concerned, the duration of the breach and the nature of the data concerned.26. In this regard, the Restricted Committee notes that the Ministry of the Interior has made significant efforts to sort the files to be destroyed without delay from those to be scanned and inserted into the automated processing before destruction. Nevertheless, if these operations led to the preparation for destruction of 430,000 files dated from 1962 to 1996, the Restricted Committee notes that this number remains low with regard to the total number of files included in the "manual file" and that the destruction has not yet been carried out for the forms in question.27. Finally, the Ministry of the Interior announced, during the meeting of July 1, 2021, the destruction of the only paper sheets whose data can no longer be legitimately included in the automated file. The Restricted Committee considers that the absence of a legal basis

for the "manual file" prevents the retention of "signalling" sheets in paper format, even in the event that the data they contain can legitimately appear in the automated file after having been scanned. It therefore considers that the destruction of the paper files of the "manual file" cannot be limited to the files whose data can no longer be included in the automated processing. The Restricted Committee also notes that the Ministry of the Interior announced, in its response to the sanction report, the "total deletion of the manual file […] 100% accomplished at the latest within four years" .28. It appears from all of these elements that the conditions for the lawfulness of the processing implemented are not met and that a breach of Article 89 of the Data Protection Act has been established.2. On the breach relating to the retention period of the data29. Under the terms of article 4 of law no. 78-17 of 6 January 1978 "personal data must be: […] 5° Kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary in relation to the purposes for which they are processed […]" .30. Article 5 of the decree relating to the FAED sets the retention periods for traces and fingerprints. The principle retention period is fifteen years (ten years for the fingerprints of minors). It can be increased to twenty-five years (fifteen years for the fingerprints of minors) by decision of the judicial authority or with regard to the qualification of the offence.31. These durations result from an amendment to decree no. 87-249 by decree no. 2015-1580 of December 2, 2015 and which entered into force on March 1, 2017. Prior to this date, the data was kept for a period of twenty-five years at from the establishment of the sheet.32. The Restricted Committee notes that, at the time of the audit in January 2019, the terms and conditions for storing FAED data did not take into account the modification that came into effect in 2017. Thus, the reports were kept for twenty-five years without distinction according to the age of the person concerned, the starting point of this period being further calculated from the last signaling of the person concerned, and not from the establishment of each record. As a result of this choice, each new report by the person concerned caused a new period of twenty-five years to run for all of his previous reports, leading to this data being able to be stored without limitation in the event of regular reports. Reduced durations were planned for certain "traces" files (twelve years for traces linked to unsolved crimes and three and a half years for traces linked to offences). An automatic purge took place after twenty-five years if a person had not been flagged again.33. The Restricted Committee notes that the findings of the delegation showed that the FAED contained, on the day of the inspection, more than two million records kept beyond the retention periods provided for by the applicable provisions. It notes that this breach is not disputed by the data controller, who indicated during the meeting of July 1, 2021 that more than three million records had been deleted since the checks carried out in order to respect the old retention periods. 34. In view of these elements, the Restricted Committee

considers that a breach of Article 4 of Law No. 78-17 of January 6, 1978 has been established.35. The Ministry of the Interior announced, during the session, that a sorting of the manual file had been fully carried out so that all files dating back more than twenty-five years are prepared for destruction, thus respecting the retention periods prior to the 2015 reform. The Ministry of the Interior indicated that, in order to comply with the retention periods arising from decree no. The author must be carried out, and has announced a four-year deadline for this work to be completed, certain files whose data can legitimately appear in the FAED having to be identified then scanned for feeding into the automated file.36. With regard to automated processing, the Ministry of the Interior indicated during the meeting that the work of qualifying the files using the NATINF code of the offense had been carried out, making it possible to define, for each of them , its maximum retention period, also taking into account the possible minority of the person concerned. All files whose retention period had expired were deleted, i.e. more than three million reports concerning 790,000 people. No more automated processing records would therefore be kept today beyond the duration provided for by the text. In addition, a purge is now carried out monthly so that all records whose retention period has expired in the month are deleted. Work is currently underway to have this process automated and taking place on a daily basis. Tests are announced in the weeks following the meeting, and the system should be generalized from the fall.37. While it notes the efforts undertaken to ensure that all of the FAED files are qualified, allowing precise and automated management of retention periods, the Restricted Committee notes the particularly substantial delay taken by the Ministry of the Interior in the application of a reform of retention periods that took place in 2015 and entered into force in 2017. It also notes that no precise timetable has been announced by the Ministry of the Interior in order to achieve compliance with the new retention periods.38 . It appears from all of these elements that a breach of Article 4 of the Data Protection Act has been constituted.3. On the failure relating to the accuracy of the data39. Under the terms of article 97 of the Data Protection Act "the competent authorities take all reasonable measures to guarantee that personal data which are inaccurate, incomplete or no longer up to date are erased or rectified without delay or are not not transmitted or made available" .40. Article 7-1 of Decree No. 87-249 provides for the procedures for erasing data after certain stages of the legal procedure. Thus, the fingerprints and the information accompanying them must be erased in the event of release or final acquittal. In the event of a decision of non-suit, of classification without further action for absence of an offense or insufficiency of charges or for an unknown author, the data must in principle be erased "unless the public prosecutor considers that their conservation appears necessary for reasons related to the purpose of the file with regard to the nature or circumstances of the commission of the offense or the personality

of the person concerned". Finally, the data can be erased at the request of the person concerned "when their conservation no longer appears necessary for reasons related to the purpose of the file".41. The Restricted Committee notes that the decisions of release, acquittal, dismissal and dismissal of charges are rendered by the judicial authorities and that they must then be sent to the FAED managing department using shuttle forms in order to that the decisions be passed on and that the data to be erased.42. The checks carried out, and more particularly the questionnaires sent to the courts, revealed the significant differences that may exist in the practices of the courts and courts of appeal. Thus, on the day of the review, some courts did not transmit any decision to the FAED and others only transmitted some (partial acquittal, correctionalization or dismissal decisions were not transmitted by certain courts). The FAED management service was therefore not informed of all the releases, acquittals, dismissals and dismissals which should have led to the deletion of the corresponding files in FAED.43. The Restricted Committee observes that the updating of FAED data actually depends on the transmission, by the courts, of all the shuttle forms to the managing department, as indicated by the Ministry of the Interior in its response to the report, and as the rapporteur has already pointed out. It nevertheless considers that, in its capacity as data controller pursuant to article 2 of decree no. 87-249 of 8 April 1987, responsibility for the accuracy of the data rests with the Ministry of the Interior. processed, on the basis of article 97 of the aforementioned Data Protection Act. The Restricted Committee considers that with regard to this obligation, the Ministry of the Interior was responsible for setting up a framework to guarantee the transmission of all the data necessary for updating the file, for example by laying down operational methods or requirements in terms of human or technical resources committed.44. The Ministry of the Interior argues, in defense, the existence of a circular from the Directorate of Criminal Affairs and Pardons (hereinafter "the DACG") of August 5, 2016 and a dispatch from the Directorate of Judicial Services of the same day recalling the transmission rules. However, in view of the old nature of these documents, and especially the absence of regular referral or reminder to the heads of jurisdictions, for example, the Restricted Committee considers that the mere existence of these documents is not sufficient to consider that the Ministry de l'intérieur has implemented all the means at its disposal to ensure the transmission of all the shuttle forms, thus making it possible to guarantee the accuracy of the data it processes.45. In addition, the Restricted Committee notes that the circular of August 5, 2016 relating to the automated file of fingerprints (NOR: JUSD1622422C), which is also mentioned by the Ministry of the Interior in defence, cannot lead to a compliant processing of the data of the FAED. This circular specifies, in fact, with regard to the erasure of data as a matter of principle in the event of a decision of non-suit, of classification without action for absence of

offense or insufficiency of charges or for unknown author, unless otherwise decided by the public prosecutor of the Republic, that "it can […] be deduced from the wording adopted that the silence of the public prosecutor characterizes his desire to maintain the data in the file, in order to preserve the hypotheses of reopening of investigation or information Such an interpretation can be deduced both from the very terms of the text, which does not require any formalism in maintaining data in the file, and from the distinction made with cases of erasure by operation of law on the one hand and cases erasure at the request of the interested party on the other hand ".46. The restricted committee considers that the position adopted by the circular is not compatible with II of article 7-1 of decree no. , dismissal for lack of offense or insufficient charges or for unknown author. In these cases, the text provides that the public prosecutor may, by exception, decide on the retention of data. However, the interpretation of the text made by the circular of August 5, 2016 overturns the principle laid down, since it entails the retention of data in principle, unless otherwise expressed by the public prosecutor.47. It appears from all of these elements that the Ministry of the Interior has not implemented all the proportionate means enabling it to ensure the accuracy of the data processed in the FAED. The Restricted Committee therefore considers that a breach of Article 97 of the Data Protection Act has been constituted.48. On the whole of this breach, the Ministry of the Interior indicated that it is carrying out work to redesign the classification form without follow-up and that a reminder was sent by the DACG to the management of the National School of the judiciary. However, no justification was provided in support of this statement.49. It appears from all of these elements that a breach of Article 97 of the Data Protection Act has been constituted.4. On the breach relating to data security50. Under the terms of Article 99 of the Data Protection Act, "the data controller and its subcontractor implement the measures provided for in 1 and 2 of Articles 24 and 25 of Regulation (EU) 2016/679 of 27 April 2016 and those appropriate to guarantee a level of security adapted to the risk, in particular with regard to the processing of special categories of personal data mentioned in I of Article 6 of this law". The mentioned I of Article 6 aims in particular at the processing of “biometric data for the purpose of uniquely identifying a natural person”.51. Firstly, the Restricted Committee notes that connection to the FAED was possible on the day of the control within the Boulogne-Billancourt police station on January 29, 2019, through the CHEOPS portal (which is an internal portal for access to various processing operations implemented by the internal security forces), using the combination of an identifier […] and a password […].52. The Restricted Committee also notes that access to FAED is limited by the fact that the terminals allowing access to the CHEOPS portal are located in premises to which access is restricted (police stations, gendarmerie brigades, customs premises) . It nevertheless emphasizes that many people outside

the police force are likely to be legitimately in these premises (cleaning staff, lawyers, doctors, etc.).53. […]. It considers, on the other hand, that Article 99 of the aforementioned Data Protection Act imposes a reinforced security obligation on data controllers when the latter process so-called sensitive data within the meaning of Article 6 of the same text, for example fingerprints and palm prints, which are “biometric data for the purpose of uniquely identifying a natural person” .54. The Restricted Committee notes that, given the particularly serious consequences that could have an illegitimate access to FAED data, and given the absolute need for strict logging of the data contained in the file, the fact of allowing connection to FAED simply combining a username and password cannot be considered an appropriate measure to guarantee a level of security commensurate with the risk.55. With regard to the implementation of reinforced security measures, the Restricted Committee recalls, on the one hand, that each official is already equipped with a unique and identifying agent card allowing access to the file. The generalization of this already functional mode of connection would therefore not be disproportionate. It recalls, on the other hand, that the CNIL had already brought to the attention of the Ministry the weakness of the current authentication method, and this as early as 2013. In response, the Ministry of the Interior already affirmed, in 2014, that strong authentication by card-agent would be imposed for any connection to the CHEOPS.56 portal. While the Restricted Committee takes note of the statements made by the Ministry of the Interior during the meeting that strong authentication using the agent card has been imposed since that day for any connection to FAED, it notes that these statements do not are supported by no element or part.57. Secondly, the Restricted Committee notes that during signaling operations, certain data is stored locally in a computer terminal present in the police custody premises in the form of Excel spreadsheets and other computer files, or in files in the paper format. Photographs also remain stored in the devices enabling identification photos to be taken.58. Keeping this data outside of the FAED centralized file does not guarantee the application of security rules essential for highly sensitive processing, such as access restrictions, access logging, protection against modification or deletion, compliance with retention periods and guarantee of the rights of individuals.59. Although the Ministry of the Interior mentions, in its response to the report, the drafting of notes reminding the services supplying the FAED of the security rules to be applied, these notes were not provided and no document in the file shows that the Ministry gave instructions to put an end to this practice.60. It appears from all of these elements that the security measures taken by the Ministry of the Interior concerning the FAED do not guarantee a level of security adapted to the risk. The Restricted Committee therefore considers that a breach of Article 99 of the Data Protection Act has been constituted.5. On the failure to inform individuals61. Under the terms of Article 104 of the

Data Protection Act, "the data controller provides the data subject with the following information: 1° the identity and contact details of the data controller and, where applicable, those of his representative; 2° where applicable, the contact details of the data protection officer; 3° the purposes pursued by the processing for which the data are intended; 4° the right to lodge a complaint with the National Data Protection Commission; 'Informatique et des Libertés and the contact details of the commission; 5° the existence of the right to ask the data controller for access to personal data, their rectification or erasure, and the existence of the right to request a limitation the processing of personal data relating to a data subject" .62. The Restricted Committee notes that on the day of the check carried out at the Boulogne-Billancourt police station on January 29, 2019, no information relating to the FAED was displayed in the police custody premises. It also notes that the agents of the Paris Judicial Court and the Paris Court of Appeal informed the control delegation that no information was communicated to the persons concerned, either by the police services or by the public prosecutor's office, neither at the time of pronouncement or service of the decision, nor at any other time.63. The Restricted Committee notes that, if Article 107 of the Data Protection Act allows, under certain conditions, restrictions on the rights of individuals and in particular the right to information, these restrictions must be "provided for by the act establishing the treatment" . In the present case, no article of Decree No. 87-249 restricts the right of data subjects to information about processing.64. The Ministry of the Interior indicated, both in its response to the sanction report and during the restricted training session, that information was provided on the websites of the Ministry of the Interior and "public service". It also indicates that information will be produced by posting in the police custody premises. This general information will relate to all the processing implemented by the Ministry of the Interior and will refer, for complete information, to the two websites mentioned.65. With regard firstly to the information on the websites of the Ministry of the Interior and "public service", the Restricted Committee considers that this information cannot, on its own, constitute sufficient information to meet the obligation imposed by article 104 of the law.66. On the one hand, the Restricted Committee notes that the communication of information on a website, which can certainly be complete, is not directly made available to the person concerned and that its consultation requires an active approach by the on the part of the data subjects, which is only possible if the data subjects are aware of the existence of the processing. However, the persons whose data are processed in the FAED may even be unaware of the very existence of the processing when, as in the present case, no information is communicated to them directly, either at the time of the data collection or at that of the pronouncement of the decision, as to the existence of this processing and the identity of its person in charge. In addition, the Restricted Committee notes that some people whose data is

processed in the FAED may only have limited access to the Internet (people in detention or homelessness, in particular), and that their right to information would be disproportionately restricted by information provided only in this way.67. On the other hand, the Restricted Committee notes that the data of minors may appear in the FAED. It considers that minors must benefit from appropriate information, in accordance with recital 39 of the police-justice directive which states that "this information should be adapted to the needs of vulnerable persons such as children". Thus, particular attention must be paid by the data controller to ensure that they can understand the processing implemented and its implications, as well as the rights available to them and the means of exercising them. Consequently, the Restricted Committee considers that information which would necessarily be based on an active approach on their part is not appropriate in the present case.68. Secondly, with regard to the posting planned by the Ministry of the Interior, relating to all the processing implemented by the Ministry of the Interior mentioned in the written response of the Ministry of the Interior and during the meeting of July 1, 2021, the Restricted Committee notes that no precise distribution schedule has been communicated to the Restricted Committee to assess the terms of its distribution, and that no example of a poster has been communicated to it either, nor has it been communicated to it. making it impossible to assess the conformity of the modifications announced.69. It appears from all of these elements that the information provided to people solely through the websites of the Ministry of the Interior and "public service" does not meet legal requirements. The Restricted Committee therefore considers that a breach of Article 104 of the Data Protection Act has been established.III. On corrective measures and their publicity70. Under the terms of III of article 20 of the law of January 6, 1978: "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from this law, the President of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II , seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: 1° A call to order; 2° An injunction to bring the processing into compliance with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this law or to satisfy the requests presented by the person concerned in order to exercise their rights, which may be accompanied, except in cases where the processing is put implemented by the State, a penalty payment the amount of which may not exceed €100,000 per day of delay from the date set by the restricted committee (…)" .71. The rapporteur proposes to the restricted committee that a call to order be issued as well as an injunction to bring the processing into compliance with the provisions of the Data

Protection Act. It also proposes that this decision be made public.72. In defense, the Ministry of the Interior considers that the pronouncement of a corrective measure is not justified, many steps having already been initiated, and for some carried out, to achieve compliance. It also considers that significant resources have already been committed, that the system on which the FAED is based is old and that compliance requires very significant developments. It further specifies that the delays observed are explained by the numerous compliance orders to which the FAED had to respond, particularly European ones.73. The Ministry of the Interior also considers that advertising is not justified, as it has no greater effect than a simple reminder. The changes to be made having been fully measured upon notification of the sanction report, the Ministry concludes that the good faith it is demonstrating and the work already undertaken are sufficient to ensure the announced compliance. Finally, he calls on the Restricted Committee to continue the support work begun with the checks carried out.74. The Restricted Committee considers that the aforementioned breaches justify a call to order against the Ministry of the Interior for the following reasons.75. The Restricted Committee notes the particular sensitivity of the data processed in the FAED, which includes both biometric data and offense data. It considers that the combination of these two types of sensitive data should have led the Ministry of the Interior to pay particular attention to this file.76. The Restricted Committee also notes that a very large number of people are concerned by this file, the Ministry of the Interior itself evoking, in its compliance operations, the deletion of more than three million "signal" sheets involving nearly 800,000 people. The Restricted Committee notes that the checks revealed that more than two million files were unlawfully stored in the FAED. The Restricted Committee also notes that certain shortcomings have targeted all of the persons whose data are processed or have been processed in the FAED, such as the lack of information.77. It also notes that this processing concerns minors, for whom particular attention must be paid, by the data controller, to respecting all of their rights.78. Finally, the Restricted Committee recalls that the Ministry of the Interior was aware of some of the shortcomings noted in the sanction report, and that it did not, however, commit the necessary means to bring it into compliance with the legislation on the protection personal data. Thus, with regard to data retention periods, for example, the Restricted Committee notes that the Ministry of the Interior applied, on the day of the checks in 2019, retention periods prior to those defined by the 2015 reform. With regard to data security and the reinforcement of authentication to the CHEOPS portal by the agent card, the Restricted Committee notes that the CNIL had already alerted the Ministry of the Interior to this vulnerability in the past, and that the Ministry had affirmed in 2014 that the use of the agent card was going to be imposed on all users of the file.79. Although the Restricted Committee is aware of the constraints, in particular budgetary,

weighing on the Ministry of the Interior, it nevertheless considers that the latter has not committed the means necessary for its compliance, despite shortcomings identified as such.80. The Restricted Committee considers that the aforementioned elements also make it necessary for an injunction to be issued. It notes on this point that the Ministry of the Interior has announced numerous modifications to the FAED, in progress or already completed, but that these assertions are insufficiently substantiated, for lack of supporting documents. The Restricted Committee also notes that, for some of the shortcomings noted, compliance had already been announced several years ago by the Ministry of the Interior. However, the checks carried out in the context of this procedure revealed that the changes announced had not been carried out.81. Finally, and for the same reasons, the Restricted Committee considers it necessary that its decision be made public. to order for breaches of Articles 4, 89, 97, 99 and 104 of the Data Protection Act; issue an injunction against the Ministry of the Interior to bring the processing operations in question into compliance with the obligations resulting from articles 4, 89, 97, 99 and 104 of the Data Protection Act, and in particular: with regard to the breach relating to the lawfulness of the processing: - only process the information referred to in article 4 of decree no. 87-249 and only within the framework provided for by this text, and in particular ensure the deletion of data contained in the "special information" section and the destruction of the "manual file", with the exception of files that may be kept for archival purposes in the public interest or for scientific or historical research purposes; with regard to the breach relating to the duration of data retention, only keep data in a form allowing the identification of the persons concerned for the period necessary in relation to the purposes for which they are processed, by example by implementing an automated system allowing the deletion of data at the end of the periods provided for in Article 5 of Decree No. 87-249, ensuring in particular that these retention periods run from establishment of each data sheet and erase the data whose retention period has expired; o with regard to the failure relating to the accuracy of the data, take all reasonable measures to guarantee that the personal data which are inaccurate, incomplete or are no longer up to date are erased or rectified without delay or are not transmitted or made available, for example by setting up a standardized and generalized procedure for all jurisdictions aimed at ensuring that all final judicial decisions are passed on in the FAED, and in particular:- with regard to erasure as of right, ensure that all decisions of release, acquittal and correction nalization, even partial, are passed on to the FAED; - with regard to cancellation in principle, ensure that all decisions of dismissal and dismissal without action for lack of offense or insufficiency of charges or for an unknown author are passed on to the FAED, without an express decision to the contrary from the competent public prosecutor; o with regard to the breach relating to data security, implement

the appropriate measures to guarantee a level of security appropriate to the risk: - by requiring, for example, that access to the FAED requires a connection using the agent card and a PIN code; - by ensuring that personal data is only processed under the secure conditions defined for the implementation of the FAED central file following signaling operations, in particular in the signaling premises, for example by giving instructions to this effect to the departments in charge of data collection. nly relating to the information of persons, ensure that information in accordance with the requirements of Article 104 of Law No. 78-17 of January 6, 1978 is provided to the persons concerned; attach the injunctions to a compliance period expiring on October 31, 2021; by way of derogation, the compliance period relating to the breach relating to the retention period of the data of the "manual file" alone will expire on December 31, 2022; make public, on the CNIL website and on the Légifrance website, its deliberation , which will no longer identify the Ministry of the Interior by name at the end of a period of two years from its publication. The President Alexandre LINDEN This decision may be the subject of an appeal before the Council of State within two months of its notification.