Deliberation 2018-259 of June 14, 2018National Commission for Computing and LibertiesNature of the deliberation: OpinionLegal status: In force Date of publication on Légifrance: Thursday August 09, 2018NOR: CNIX1819998X a draft decree relating to the "API-PNR France system" and modifying the internal security code (regulatory part) (request for opinion no. 18006270)

The National Commission for Computing and Liberties,

Seizure by the Minister of the Interior of a request for an opinion concerning a draft decree relating to the API-PNR France system and modifying the internal security code (regulatory part);

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Directive 2004/82/EC of the Council of Europe concerning the obligation for carriers to communicate data relating to passengers;

Having regard to Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention and detection of crime criminal proceedings, investigation and prosecution in this area or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA;

Having regard to Directive 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention and detection of terrorist offenses and serious forms of crime, as well as for investigations and related prosecutions;

Having regard to the internal security code, in particular its article L. 232-7;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms;

Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to decree no. 2014-1566 of 22 December 2014 creating a service with national jurisdiction called the Passenger Information Unit (UIP);

Having regard to deliberation no. 2013-219 of July 18, 2013 providing an opinion on a bill relating to military programming for the years 2014 to 2019 and containing various provisions concerning defense and national security;

Having regard to deliberation no. 2014-308 of July 17, 2014 providing an opinion on a draft decree relating to the creation of a processing of personal data called the API-PNR France system taken for the application of Article L. 232 -7 of the Internal Security Code and laying down the procedures for the transmission to the service with national competence Passenger Information Unit of data relating to passengers by air carriers;

Having regard to deliberation no. 2015-230 of July 9, 2015 issuing an opinion on a draft decree amending articles 5 of decree no. 2010-569 of May 28, 2010 and R. 232-14 and R. 232-15 of the homeland security;

Having heard Mr. Jean-François CARREZ, commissioner, in his report, and Mrs. Nacima BELKACEM, government commissioner, in her observations, Issues the following opinion:

The committee received a request for an opinion from the Minister of the Interior on a draft decree relating to the API-PNR France system and amending the internal security code (CSI). recalls that article L. 232-7 of the CSI, in its version resulting from law n° 2013-1168 of December 18, 2013 relating to military programming for the years 2014 to 2019, authorized, on an experimental basis and as of December 31, 2017, the processing of registration data (known as API or Advance Passenger Information) relating to passengers on flights to and from national territory, with the exception of flights connecting two points in mainland France, as well as data relating to passengers recorded in the reservation systems of air carriers (known as PNR or Passenger Name Record). This experimental system was intended to meet the needs of the operational services of national police officers, the national gendarmerie and customs as well as specialized intelligence services, within the framework of the purposes exhaustively listed in article L. 232-7 of the CSI, namely the prevention and observation of acts of terrorism, offenses mentioned in l ' article 695-23 of the Code of Criminal Procedure (CPP) and attacks on the fundamental interests of the nation, the gathering of evidence of these offenses and these attacks as well as the search for their perpetrators. For the implementation of this system , a Passenger Information Unit (UIP), a service with national jurisdiction attached to the Minister responsible for customs and created by Decree No. 2014-1566 of 22 December 2014 referred to above, was responsible for collecting the data transmitted by the airlines, to exploit them and to transmit the result of this exploitation to the requesting services. API-PNR processing, which makes it possible to carry out a reconciliation between the data collected and other files of po judicial or administrative proceedings, relating to persons or objects searched for or monitored, should also make it possible to experiment with new methods of using this data, in particular the targeting of individuals on the basis of various pre-established criteria and their classification on a scale of risks, thanks to the use of a scoring tool. 2013, n° 2014-308 of July

17, 2014 and n° 2015-230 of July 9, 2015.

Law No. 2017-1510 of October 30, 2017 strengthening internal security and the fight against terrorism, however, amended Article L. 232-7 of the CSI to perpetuate the API-PNR system and transpose Directive (EU) 2016/ 681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention and detection of terrorist offenses and serious forms of crime, as well as for the investigation and prosecution thereof matter (hereafter the PNR directive), the transposition deadline for which was set at 25 May 2018. The draft decree submitted to the committee today aims to finalize the transposition of this directive and, beyond the modifications made necessary this transposition, redefining the conditions for implementing the API-PNR system on several points.

It also notes that the draft submitted to it for opinion was subject, on the date of the referral, to the provisions of Article 26-I-2° of the law of 6 January 1978 as amended, which provides that an order, issued after reasoned and published opinion of the commission, authorizes the processing of personal data implemented on behalf of the State and which have as their object the prevention, research, observation or prosecution of criminal offenses or the execution criminal convictions or security measures. It follows from VI of article L. 232-7 of the CSI that the conditions for implementing API-PNR France processing must be defined by a decree of the Council of State, issued after a reasoned and published opinion of the commission. Given the evolution of the legal framework relating to the protection of personal data resulting in particular from the taking into account of the provisions of Directive (EU) 2016/68o of 27 April 2016 referred to above, the commission considers that the processing which submitted to it must be examined in the light of these new provisions.

The draft calls for the following observations from the commission. On the purposes of the processing and the scope of the API-PNR France system:

The purposes of the API-PNR France system are defined in I of Article L. 232-7 of the CSI, which authorizes the Minister of the Interior, the Minister of Defence, the Minister responsible for transport and the Minister responsible for customs to implement the processing of personal data for the purposes of the prevention and detection of certain offenses as well as the search for their perpetrators. The same article specifies that the offenses concerned are acts of terrorism, attacks on fundamental interests of the nation as well as the offenses listed in Annex II of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of Passenger Name Record (PNR) data for the prevention and the detection of terrorist offenses and serious forms of crime, as well as for the investigation and prosecution thereof, when punished by a custodial

sentence of an equal or greater duration imprisonment for three years or a custodial measure of three years or more. This version of Article L. 232-7 of the CSI, resulting from Law No. 1510 of 30 October 2017 cited above, no longer includes any reference to the offenses mentioned in article 695-23 of the CPP, but makes a reference to appendix II of the transposed PNR directive, which mentions twenty-six offenses or categories of offences, including participation in a criminal organisation, trafficking in human beings, corruption, fraud, serious offenses against the environment, including trafficking in endangered animal species, entry assistance illegal stay, murder, serious bodily injury, trafficking in hormonal substances, rape or even industrial espionage. the PNR directive since the API-PNR France system maintains a purpose of preventing attacks on the fundamental interests of the nation, not covered by the aforementioned directive. The committee notes that the functionalities resulting from the transposition of the PNR directive, such as the transfer of PNR data to the UIP of another Member State of the European Union or the possibility for the UIP, at the request of the authorities mentioned in article R. 232-15 of the CSI, to ask air carriers to transmit data outside the imposed transmission slots, will therefore not be implemented for the purposes of preventing attacks on the fundamental interests of the nation, gathering evidence of these breaches as well as the search for their perpetrators. In addition, the committee notes that the API-PNR France system also has a broader scope of application than that imposed by the directive insofar as it does not only concern air carriers, but also travel agencies and travel or holiday operators chartering all or part of an aircraft, to whom the last paragraph of II of Article L. 232-7 of the CSI, in the version resulting from the law of 30 October 2017 mentioned above, provides that the Minister of the Interior, the Minister of Defence, the Minister responsible for transport and the Minister responsible for customs may request (…) to transmit data relating to passengers between registered in their reservation system, and therefore PNR data. and travel or holiday operators chartering all or part of an aircraft to transmit the reservation data to the PIU, a first time 48 hours before flight departure and a second time immediately after the flight closes, by secure electronic transmission. It also notes that the obligations to which the draft decree subjects these agencies and operators are less numerous than those applicable to air carriers and that they will not, in particular, have to transmit data outside the time slots mentioned above.Finally, the draft decree submitted to the commission plans to modify several articles of the CSI relating to the API-PNR system to mention the collection and use n API data relating to crew members. These modifications are intended to supplement, on the one hand, the reference to passenger data by and crew members, in article R. 232-13 of the CSI, and on the other hand, the expression recording data by air passengers as well as crew members in b of I of article R. 232-14 of the CSI. In its current version, article R. 232-14 of the CSI, relating to data

processed within the framework of the API-PNR system, only provides for the collection and processing of data relating to passengers while mentioning within a parenthesis located at 11° of b of I of this article a status of crew member.

If this wording, according to the ministry, makes it possible to base the collection of API data relating to crew members, it remains ambiguous and a source of some confusion, which the ministry intends to resolve by expressly authorizing the collection and use of these data. The commission notes, however, that the provisions of Article L. 232-7 of the CSI on which the draft decree submitted to it is based, only authorize the collection of data relating to air passengers. It further points out that the API Directive and the PNR Directive, which these legislative provisions transpose, also only mention the collection of data relating to passengers. Lastly, it observes that the PNR Directive, in its Article 3, expressly defines the concept of passenger as excluding that of crew member. committee wonders about the possibility for the ministry to provide for the collection of API data relating to crew members. On the nature of the data processed, the conditions of their use and their retention period:

The commission recalls first of all that, in accordance with article L. 232-7 of the CSI, only data relating to journeys to and from the national territory must be transmitted to the UIP, with the exception of journeys between two points of metropolitan France. The same article of the CSI excludes the processing within the framework of the API-PNR system of personal data likely to reveal the alleged racial or ethnic origin of a person, his religious or philosophical beliefs, his political opinions, trade union membership, or data concerning the data subject's health or sex life. On this point, the committee notes that the automatic filtering system initially implemented to make inaccessible any sensitive data which may be mistakenly transmitted to the PIU will be maintained. The committee also recalls that, with regard to passengers, the data that air carriers are required to collect and transmit are both registration data relating to passengers for these journeys (API) and data relating to passengers recorded in their reservation systems (PNR data). PNR are those provided by travelers at the commercial reservation stage and correspond mainly to data relating to the identity of air passengers (nationality, surname, first name, date of birth), the route taken, the number and names of other passengers listed in the passenger file as well as other information concerning the passenger (seat number, information relating to b wages, means of payment, etc.). API data, on the other hand, is check-in and boarding data present in the information systems of airlines or airport platforms. They essentially consist of data relating to the identity of air passengers (nationality, surname, first name, date of birth, sex), the travel document used (type, number), the flight taken (number, border crossing point, transport code, date of the flight, times and point of departure and arrival, point of embarkation and disembarkation, total number of people transported) as well as other information concerning the passenger

(status of the person on board, number seat, passenger file reference code, number, weight and identification of baggage). Concerning the API and PNR data transmitted by air carriers relating to passengers, the draft decree does not mark any significant change compared to the experimental system previously put in place. implemented, with the exception of the addition, with regard to PNR data, of categories of data relating to minors. On this point, article 5 of the draft decree provides that all information available on unaccompanied minors under the age of 18 may be recorded in the processing, such as name and sex, age, languages spoken, the name and contact details of the person present at the start and his relationship with the minor, the name and contact details of the person present at the finish and his link with the minor, the agent present at the start and at the arrival. The committee notes that Annex I of the aforementioned Directive 2016/681 does not mention the person present as a person whose data may be collected but refers to the guardian. However, the committee notes that the same situations are covered and thus notes that these two formulations relate to the same field. of article L. 232-7 of the CSI, to ask travel agencies and travel or holiday operators chartering all or part of an aircraft to transmit PNR data, by supplementing article R. 232-14 of the CSI relating to the categories of data processed. However, the committee considers inappropriate the proposed amendment to the first paragraph of I of this article, which introduces a list comprising API data and PNR data, while the transmission by travel agencies and travel or holiday operators provided for in II of Article L. 232-7 of the CSI, unlike air carriers, only concerns PNR data. The committee therefore considers that the wording of the draft decree should be reviewed so that it appears more clearly that only PNR data can be transmitted by travel agencies and travel operators. It notes that the ministry undertakes to clarify the wording of the provisions concerned.Concerning the conditions for the use of data, the commission takes note of the clarifications made to II of article R. 232-13 of the CSI by the draft decree indicating that the data are only processed by the IPU in order to carry out an assessment of persons before their planned arrival on the national territory or their planned departure from it, in order to identify the persons for whom further examination is necessary with regard to the purposes of the processing by the authorities mentioned in Article R. 232-15 and, where applicable, by Europol. The committee also notes that this assessment will always result from the use of screening and targeting techniques. , to automatically and systematically compare them with several files relating to wanted persons or objects (FPR, FOVeS, SIS II, SILCF and Interpol's ASF-SLTD database). This function, known as screening, is intended to determine whether persons or objects registered in these files appear on a flight concerned by the processing. The commission notes that the guarantees provided on this point in the context of the experiment are maintained. It notes in particular that the screening carried out,

which therefore makes it possible to know that a person or an object is registered in a processing operation, is not carried out with regard to the entire content of the aforementioned files, but only in relation to the files relevant, in particular with regard to the offense seriousness threshold provided for in Article L. 232-7 of the CSI.

The commission also notes that the results of this connection, which reveal the registration or absence of registration of an individual in the parts of the files consulted, remain kept for a maximum period of ninety-six hours. .In addition, in the event of a positive response (hit), a copy of the search or surveillance sheet concerned is made available in order to allow the agents of the UIP to carry out the operation to remove doubts, which justifies the mention of such elements in II of article R. 232-14 of the CSI among the data likely to be recorded in the processing, for a maximum retention period of twenty-four hours. The commission emphasizes however that the draft decree submitted to it maintains the principle of the retention of a partial copy of the FPR to allow the linking mentioned above. The implementation of such a mirror database had been justified by technical difficulties and the Ministry had undertaken to implement several measures to limit the risks associated with such a method, in particular the limitation of the elements recorded to those necessary for the exercise of the missions of the UIP, the absence of direct access of the agents of this unit to the data and the updating at least weekly of the partial copy of the RPF. The commission recalls however that this process remains more risky, from a data protection point of view, only a direct consultation of the FPR and should therefore only be implemented insofar as the linking cannot be carried out otherwise. However, it notes that, since the implementation of the mirror database of the FPR within the framework of the API-PNR system, screening systems have been able to be set up with an interconnection between a database, in particular ACCRED, and the FPR , without any technical difficulties getting in the way. In this context, the commission notes that the ministry undertakes to assess as soon as possible the possibility of a direct interconnection between the FPR and the API-PNR system and that the implementation of the mirror base will only be continued if the expert's report confirmed that the FPR does not have the technical capacity to respond to the massive requests from the API PNR system. It invites the Ministry to inform it of the progress and conclusions of this expertise by sending it an annual report on the conditions for implementing the API-PNR system. The commission considers that such an assessment, beyond the issue of the RPF's mirror base, is justified by the major issues raised by the system and the need to promote regular exchanges on ways to improve the system.

In addition to the screening device, the API-PNR system gives rise to the implementation of different techniques for targeting individuals, and therefore for analyzing data on the basis of pre-established objective criteria. These data processing methods,

which are only implemented at the request of a competent authority, make it possible to detect behavior deemed to be at risk with regard to the purposes defined in Article L. 232-7 of the CSI.

The draft decree expressly provides that the criteria are defined in cooperation with the authorities mentioned in article R. 232-15 of the CSI, that they must be targeted, proportionate, specific to the offenses and non-discriminatory, that they cannot be based on personal data which reveal, directly or indirectly, the alleged racial or ethnic origin, political, philosophical or religious opinions or trade union membership or those relating to health, sex life or the sexual orientation of people and that they are regularly updated or redefined. The commission takes note of this. against the interested parties does not result from automated processing alone. In fact, human and manual checks are carried out by the PIU when it receives a request, then by the recipient services, which decide on the action to be taken and which can, if necessary, carry out the additional checks that they deem necessary. The draft decree thus imposes, in the event of a positive agreement obtained following the assessment carried out, the individual re-examination of the situation of the person concerned by non-automated means. Finally, the committee notes that, as with the results from the screening, the results from the analysis of the data with regard to the pre-established criteria can only be kept for a maximum period of ninety-six hours, for the sole purpose of inform the competent authorities of the existence of a positive match.

More generally, Article L. 232-7 of the CSI provides that data may only be kept for a maximum period of five years. The commission recalls that data likely to reveal the identity of passengers is subject to an additional guarantee, resulting from the implementation of a masking procedure. In the context of the experimental API-PNR system, this masking procedure was implemented after the expiry of a period of two years, at the end of which the data were no longer visible either to IPU agents or by the departments that made the requests. Access to this data required making a reasoned request to the director of the UIP, who alone could lift the masking.

The committee notes that this masking process is maintained and that this guarantee is reinforced by the reduction of the period from two years to six months, to ensure the transposition of the PNR directive. On the recipients:

On the modifications relating to article R. 232-15 of the CSI:

The purpose of article 6 of the draft decree is to modify the categories of personnel who may be recipients of the data and information recorded in the processing, and this within the limits of their powers and need to know. The commission notes that, in addition to the modifications provided for by this article, the list of recipients as provided for by the experimental system is

made permanent. Firstly, the commission notes that III of article R. 232-15 is modified to take into account the aforementioned Directive 2016/681 and thus provide that certain agents may be recipients of the processing data, by means of a request to the UIP or when an intervention on the airport platforms is necessary, for the prevention, observation and collection of evidence of the search for perpetrators of offenses for the offenses mentioned in Annex II of the aforementioned directive, thus removing the reference to the provisions of article 695-23 of the CPP. Firstly, article 6 of the draft decree specifies that, with regard to the prevention and observation of acts of terrorism, the gathering of evidence of these acts and the search for their perpetrators, the services of the intelligence department of the police prefecture, and not only those attached to the sub-directorate in charge of the fight against terrorism and extremism with violent potential, can formulate requests to the UIP and receive answers. Furthermore, the aforementioned article provides that these agents may also be recipients of this data, for the sole purpose of preventing the offenses mentioned in Annex II of the aforementioned Directive 2016/681.Article 1 of the order of 27 June 2008 relating to the intelligence department of the police prefecture and amending the order of 6 June 2006 on the general employment regulations of the national police provides in particular that the intelligence department of the police prefecture contributes to the activity of the central directorate of internal intelligence for the prevention of acts of terrorism and for the surveillance of individuals, groups, organizations and phenomena of society likely, by their radical nature, their inspiration or their modes of action, to undermine national security .

In view of these elements, the commission considers that these agents are legitimate recipients of API-PNR France processing data under the conditions provided for in article R. 233-15 of the CSI and as envisaged by the draft decree .Secondly, and for the sole purpose of repressing acts of terrorism, article 6 of the draft decree provides that the agents of the national judicial customs service, individually designated and specially authorized by their head of service, may be recipients of processing data. In this respect, article 2 of the decree of 5 December 2002 establishing the service with national jurisdiction called the national judicial customs service provides that the national judicial customs service has the following missions: to carry out judicial investigations in the conditions set out in Article 28-1 of the Code of Criminal Procedure, to lead and coordinate, at the national level and in judicial matters, the fight against the perpetrators and accomplices of the offenses referred to in this same article, to collect and to exploit the information necessary for the exercise of its missions. The commission considers that the agents thus targeted, for the purposes set out, are legitimate to be recipients of the processing data, provided that they are authorized under the conditions provided for by article 28-1 of the CPP, in addition to their individual designation and special

authorization by their department head. Thirdly, article 6 of the draft decree aims to introduce the possibility for certain tain categories of agents to be recipients of the data recorded in the processing, and this, under the prevention of acts of terrorism. The agents of the military intelligence directorate, the agents of the defense intelligence and security directorate, and the agents assigned to the sub-directorate of operational anticipation of the general directorate of the national gendarmerie are thus targeted. Article D. 3126-16 of the Defense Code provides that the Directorate of Military Intelligence draws up and implements guidelines for intelligence of military interest. In addition, the agents assigned to the sub-directorate of operational anticipation of the general directorate of the national gendarmerie have in particular for missions, in accordance with article 17-1 of the decree of August 12, 2013 on the organization of the directorate General of the National Gendarmerie, to process internal and external information allowing the alert of the authorities, as well as the follow-up of sensitive situations in the short term, to participate in the research, the collection, the analysis and the dissemination of defence, public order and national security information necessary for the execution of the missions of the gendarmerie and to ensure the processing of operational intelligence of public order and economic security intelligence in mainland France and overseas. committee notes that as such, the mission of preventing acts of terrorism does not appear among the prerogatives entrusted to the military intelligence directorate, nor to the sub-directorate of the operational anticipation of the General Directorate of the National Gendarmerie. However, with regard to their missions and the purposes of the processing, it considers that these services may be recipients of the processing data under the conditions provided for in Article R. 232-15 of the CSI. As regards the possibility for agents of the Defense Intelligence and Security Directorate to be recipients of the processing data, Article D. 3126-6 of the Defense Code provides that this directorate has the particular mission of preventing and investigating attacks on the national defense as defined by the criminal code and the code of military justice, in particular by implementing counter-intelligence measures to oppose any threat that may take the form of terrorism, espionage, subversion, sabotage or organized crime. However, the commission considers that only agents attached to the sub-directorate of counter-interference are legitimate to be empowered, with regard to the missions of the other sub-directorates, and the prerogatives set out above, as provided for by the decree of October 22, 2013 organizing the directorate for defense protection and security. Fourthly, article 6 of the draft decree provides for allowing agents of the general directorate for external security recipients of the data recorded in the processing, for several purposes.

Article D. 3126-2 of the Defense Code provides that the General Directorate for External Security has the task, for the benefit

of the Government and in close collaboration with the other organizations concerned, of seeking and exploiting information of interest to the security of France, as well as detecting and hindering, outside the national territory, espionage activities directed against French interests in order to prevent their consequences .

The purpose of the draft decree is to make these agents the recipients under the prevention of acts of terrorism, and under the prevention, observation, collection of evidence and search for the perpetrators of the offenses mentioned in the appendix II of Directive 2016/681 referred to above.

In addition, the aforementioned project aims to allow agents of the DGSE and agents of the General Directorate for Internal Security (DGSI) to be recipients of all the data collected within the processing, for a maximum period of twenty-eight days, and for a determined destination or origin, according to the procedures provided for in VI of article R. 232-15 of the CSI and this, for the purposes of defining or updating the criteria and elements of research relating to passengers on the flights concerned, for the purposes of preventing terrorism and the sole crimes and offenses mentioned in Annex II of the aforementioned directive, and in VIII of Article R. 232-15 of the CSI. On the one hand, the commission notes that the provisions relating to the missions of the DGSE do not explicitly target the prevention of acts of terrorism. However, with regard to the general purposes of the processing as well as the missions relating to the security of France of the department concerned, it considers that these agents are legitimate to be recipients of the data of the API-PNR France processing under the conditions provided for by the article 6 of the draft decree. On the other hand, article 2 of decree no. its missions, it contributes to the prevention and repression of acts of terrorism or which undermine the security of the State, the integrity of the territory or the permanence of the institutions of the Republic. Thus, with regard to these missions, the commission considers that these agents are legitimate recipients of the processing data, under the conditions provided for by the draft decree. Fifthly, the commission notes that article 6 of the draft decree modifies the categories of agents who may be recipients of processing data for the prevention of terrorist acts and attacks on the fundamental interests of the nation in that it removes the departments in which agents are assigned within the DGSE, the DGSI and the military intelligence directorate. Although the commission considers that this modification does not call for any particular reservations on its part, it recalls that this should not lead to extending the categories of personnel authorized to access data in accordance with these provisions and within these departments, for purposes mentioned.Finally, the commission notes that some purely formal changes have been made to certain categories of recipients, which do not call for any particular comments on its part.On the introduction of articles R. 232-16, R. 232-17, R.

232-18 and R. 232-19:

Articles 8 and 9 of the draft decree introduce the possibility, also provided for by the aforementioned Directive 2016/681, of transmitting API-PNR France processing data to the PIUs of other Member States, to the competent authorities of other Member States under the purposes of the processing, to Europol and to the competent authorities of States which are not members of the European Union. The commission notes that the terms and conditions for the transmission of data to these recipients are intended to take into account the aforementioned directive 2016/681 and do not call for any particular observations on its part. On the rights and information of persons :

The commission notes that the obligation to inform passengers about the processing of their data applies to both airlines and UIPs in accordance with Article L. 237-7 of the CSI which provides that air carriers […]] inform the persons concerned by the processing, and article 2 of decree n° 2014-1566 of December 22, 2014 establishing the UIP which provides that the UIP ensures that air carriers inform passengers of their rights .It recalls that the ministry must ensure that this information is delivered in a clear, complete and educational manner. In this respect, with regard to the guarantees implemented, the Ministry indicated that general information is available concerning the implementation of the processing, via the website pnr.gouv.fr and relating in particular to the transmission of data by the carriers, the purposes of the exploitation of these data as well as their retention period. The committee notes that the information currently accessible on this site cannot be considered complete. It thus takes note of the Ministry's commitment to enrich its content in order to guarantee the right to information of the persons concerned, in accordance with the requirements of Article 13 of the aforementioned Directive 2016/68o. Article 11 of the draft of decree provides that the various rights of the persons concerned will be exercised in a mixed manner. In this respect, the rights of access, rectification and erasure of the data mentioned in article R. 232-14 are exercised directly with the Director of the UIP or his deputy. The aforementioned article of the draft submitted to the committee also provides that the right of access may be refused and that the persons concerned may informed of a refusal of rectification, erasure of their data, or limitation of their personal data relating to the mention known or unknown, in the processing operations related to the API-PNR France system and this, in particular to purposes of protecting public safety and national security. These rights are exercised with the National Commission for Computing and Liberties. If the Commission considers that these limitations are necessary and justified with regard to the reasons mentioned above, it considers that these derogations should in no case result in through a systematic restriction of the rights of data subjects.

Finally, this same article provides that the right of opposition provided for in article 38 of the amended law of 6 January 1978 does not apply to the planned processing. In this respect, the committee recalls that, if the provisions of the directive 2016/68o of 27 April 2016 referred to above as transposed into domestic law, do not mention the possibility for data subjects to object to the processing carried out, the Member States retain, in any case, the possibility of providing for more extensive safeguards than those established in the said directive for the protection of the rights and freedoms of data subjects with regard to the processing of personal data by the competent authorities. In this context, it considers that the aforementioned Article 38, which has not been repealed by the law relating to the protection of personal data and whose application to processing covered by the aforementioned directive is not further excluded by the provisions of Articles 70 -1 and following of the Data Protection Act, is also intended to apply to processing falling within the scope of this directive. It notes in this respect that Article 38 provides for the possibility of disregarding the right of opposition when the processing meets a legal obligation or when an express provision of the regulatory act authorizing the processing excludes it. , the commission considers that the exclusion of the right to object as provided for by article 11 of the draft decree is strictly proportionate with regard to the purpose pursued by the planned processing, namely the prevention and establishment of certain offences, of the collection of evidence of these offenses as well as the search for their perpetrators. In view of the foregoing, it considers that the limitation imposed on the exercise of the right of opposition falls strictly within the framework of the provisions of national law relating to the protection of personal data and is not such as to excessively interfere with the rights and freedoms of data subjects.Finally, the draft decree provides that the UIP notifies the data subject and the commission of any breach of personal data which could lead to a risk high for the protection of this data or to affect the privacy of the data subject. On data security and traceability of actions:
The committee recalls that the security measures surrounding the implementation of the API-PNR France system have been submitted to it on several occasions. Under these conditions, the project only calls on its part for the following observations and reminders.
The API-PNR system implements authorization profiles in order to manage access to data as needed. The commission notes that the ministry has planned to implement a regular access review. A logging of data consultation, creation and modification operations has been put in place. The commission takes note that the architecture of the latter is centralized and recalls that measures aiming to reinforce the security of this mechanism are necessary, in particular by the implementation of measures to reduce the risk of alteration or voluntary modification or not of this one. It also reminds that means must be provided for the

analysis of the traces.

The committee notes that the ministry undertakes to make the necessary changes to ensure compliance with its recommendations regarding the exchange of information with the recipient services. The commission recalls that guaranteeing the confidentiality of exchanges requires the implementation of encryption and authentication measures for recipients. Under these conditions, the commission considers that the measures provided for by the data controller comply with the requirement security provided for by article 34 of the law of January 6, 1978 as amended. However, it recalls that compliance with this requirement requires the updating of security measures with regard to the regular reassessment of risks.

The president,

I. Falque-Pierrotin