National Commission

Data Protection

OPINION/2022/114

I.Introduction

1. The Court of Justice of the European Union (hereinafter, CJEU), in the judgment of June 21, 2022, delivered in case 0817/19 (Ligue des droits humains v. Conseil des ministres), ruled that Directive (EU) 2016/681, of the European Parliament and of the Council of 27 April 2016, on the use of data from passenger records for the purposes of preventing, detecting, investigating and prosecuting terrorist offenses and serious crime (hereinafter , PNR Directive), provided that it is interpreted in the light of Articles 7, 8, 21 and 52, paragraph 1, of the Charter of Fundamental Rights of the European Union (hereinafter, the Charter), it is in accordance with these articles. But, it understood that the compliance of the Directive with those articles of the Charter depends on the interpretation of some of its precepts in the terms that are transcribed below:

«[...] 3) Article 6 of Directive 2016/681, read in the light of Articles 7, 8 and 52, paragraph 1, of the Charter of Fundamental Rights, must be interpreted in the sense that it precludes national legislation authorizing the processing of passenger name record data (PNR data) collected in accordance with that directive for purposes other than those expressly set out in Article 1(2) of the mentioned directive.

4) Article 12(3)(b) of Directive 2016/681 must be interpreted as precluding national legislation according to which the authority established as the Passenger Information Unit (UIP)) is also the competent national authority empowered to approve the communication of PNR data, after a period of six months following the transfer of such data to the PIU.

5) Article 12(1) of Directive 2016/681, read in conjunction with Articles 7, 8, and 52(1) of the Charter of Fundamental Rights, must be interpreted as meaning that it precludes national legislation which provides for a general retention period of five years for PNR data, applicable indifferently to all air passengers, including those for whom neither the prior assessment provided for in Article 6, paragraph 2, subparagraph a) of that directive, nor any checks carried out during the period of 6 months provided for in article 12, paragraph 2, of the said directive, nor any other circumstance, revealed the existence of susceptible objective elements to create a risk of terrorist offenses or serious criminality which have an objective link, at least indirectly, with the carriage of passengers by air.

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

f

6) Must Directive 2004/82 be interpreted as meaning that it does not apply to flights, whether scheduled or not, operated by an air carrier, originating in the territory of a Member State and which must land in the territory of one or more Member States, without stopping over the territory of a third country (intra-EU flights).

7) EU law, in particular Article 2 of Directive 2016/681, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article Article 45 of the Charter of Fundamental Rights must be interpreted as precluding:

- national legislation providing, in the absence of a real, current or foreseeable terrorist threat to which the Member State concerned must deal, a system of transfer by air carriers and travel operators, and of processing by the authorities competent authorities, PNR data of all intra-EU flights and transport by other means within the Union, from or to that Member State or transiting through it, in order to combat terrorist offenses and the organized crime. In such a situation, the application of the system established by Directive 2016/681 must be limited to the transfer and processing of PNR data for flights and/or transport relating, in particular, to certain connections or travel plans or even to certain airports, railway stations or seaports for which there are indications likely to justify such application. It is up to the Member State concerned to select the intra-EU flights and/or transport performed by other means within the Union, for which these alerts exist, and to regularly review said application in the light of changes in the conditions that justified their selection. , for the purpose of ensuring that the application of that system to those flights and/or those transports remains limited to what is strictly necessary, and

- national legislation providing for such a system for transferring and processing said data for the purpose of improving border controls and combating illegal immigration. [...]»

2. The PNR Directive was transposed into the Portuguese legal system through Law No. 21/2019, of February 25, which regulates the transfer, by air carriers, of data from passenger identification records, as well as the processing of these data.

3. The personal data processed are, pursuant to article 4 of Law No. 21/2019, those listed in Annex I of the same law, which correspond to the data in Annex I of the Directive, highlighting, «[. ..] in addition to the name of the air passenger or passengers, information necessary for the reservation, such as the expected travel dates and the

travel itinerary, information relating to tickets, groups of persons registered under the same reservation number, contact information for the passenger or passengers, information relating to payment or invoicing, information relating to luggage and general remarks on passengers .» (cf. paragraph 93 of the aforementioned judgment, hereinafter referred to as the “PNR Directive”) judgment.

4. The processing of this data has a significant impact on the rights, freedoms and guarantees of citizens, first of all, on the right to informative self-determination (also known as the right to protection of personal data), enshrined in article 35 of the Constitution of the Portuguese Republic (CRP) and Article 8 of the Charter, as it corresponds to a treatment carried out independently of the will of the data subjects, but especially in the right to privacy and family life, enshrined in Article 26 of the CRP and Article 7. ° of the Charter, in addition to Article 8 of the European Convention on Human Rights (see paragraphs 94 to 96 of the judgment "PNR Directive").

5. As stated in the aforementioned judgment (cf. point 100), '[...] even though certain PNR data listed in Annex I to the PNR Directive [...], taken in isolation, do not seem likely to reveal precise information about the private life of the persons concerned, it remains true that, taken together, said data may reveal, inter alia, a complete travel itinerary, travel habits, existing relationships between two or more persons and information on the financial situation of air passengers, my eating habits or their state of health, and may even reveal sensitive information about these passengers" (our italics).

6. As it is well known that «[...] it is consistent case law that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever for the subsequent use of the information communicated. The same can be said of the conservation of personal data and access to said data with a view to their use by public authorities. In this regard, it matters little whether or not the information relating to privacy in question is sensitive, or whether the interested parties have or have not suffered inconvenience as a result of such interference [Opinion 1 / 15 (EU-Canada PNR Agreement), of July 26 of 2017, EU:C:2017:592, paragraphs 124

and 126 and cited case-law]' (cf. paragraph 96 of the judgment "PNR Directive")".

7. Thus, the CJEU concluded that the PNR Directive involves interference of effective gravity in the fundamental rights to the protection of personal data and respect for private and family life, insofar as it aims to establish a regime of continuous, non-targeted and systematic surveillance, which includes the automated assessment of personal data of all persons using air transport services (cf. paragraph 111 of the judgment "PNR Directive").

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

8. To that extent, because the processing of PNR personal data represents a serious interference with those fundamental rights, it is essential that this interference be proportionate, reduced to the strict minimum necessary for the intended security purpose, which is why the respective legal regulation must be clear and precise in determining the scope and application of the measures provided for therein, and must, "[...] in particular, indicate in what circumstances and under what conditions a measure that provides for the processing of such data can be adopted, thus guaranteeing that the interference is limited to what is strictly necessary' (cf. point 117 of the judgment "PNR Directive"). All the more so when, as underlined by the CJEU, personal data are subject to automated processing and are likely to reveal sensitive information about passengers.

9. Thus, in line with the recommendation approved by the European Data Protection Board, on December 13, 20221, and under the powers provided for in paragraph c) of paragraph 1 of article 57 and in paragraph b) Article 58(3) of Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27 April 2016 (General Data Protection Regulation - RGPD), in conjunction with the provisions in article 3, paragraph 2 of article 4 and paragraph a) of paragraph 1 of article 6, all of Law no. 58/2019, of August 8, as well as in paragraph c) of paragraph 1 of article 44 of Law no. 59/2019, of August 8, the National Data Protection Commission (CNPD) recommends the revision of Law no. 21/2019, of February 25, which transposes that Directive,

with the grounds and terms set out below.

II. Analysis of Law No. 21/2019

i. The revision of Article 1(1) regarding intra-EU flights

10. According to the aforementioned jurisprudence, paragraph 1 of article 1 of Law No. 21/2019 must be revised in order to ensure compliance with the Charter and with the CRP, since, when generically, permanently and systematically covering both extra-European Union (EU) and intra-EU flights, is unnecessarily and excessively restricting fundamental rights to the protection of personal data and to the preservation of private and family life, as well as the fundamental right to free movement and residence in the territory of the Member States (Articles 7, 8 and 45 of the Charter) - cf. point 173 of the judgment "PNR Directive".

11. In fact, although the PNR Directive admits that the regime provided for therein extends, if the Member State so wishes, to flights within the EU, the truth is that the conservation, communication and analysis of PNR data of all flights intra-EU must be guided by its suitability and necessity in view of the purpose of this

1 Statement 5/2022 on the implications of the CJEU judgment C-817/19 regarding the implementation of the Directive (EU) 2016/681 on the use of PNR in Member States, accessible at https://edpb.europa.eu/ svstein/files/2022-12/edpb statement 20221213 on the pnr judgment.....en.pdf

regime, that is, for the purpose of preventing, detecting, investigating and repressing terrorist offenses and serious crime (cf. no. 2 of article 1 of Law no. 21/2019).

12. Now, according to the understanding expressed in the judgment of the CJEU, the processing of personal data relating to passengers on intra-EU flights is only necessary and not excessive if it is justified by concrete circumstances that reveal or indicate, with reason, the existence of real or foreseeable terrorist threats, for a duly limited period of time, and the respective decision must be verified by a court or independent administrative entity through a binding decision (cf. paragraphs 171 and 172 of the judgment “PNR Directive”).

13. Thus, and as the CNPD had already pointed out, in its Opinions No. 61/2017, of November 21st, and No. 31/2018, of July 6th2, which were incomprehensibly ignored at this point, it is evident the unnecessary and disproportionate permanent and

systematic collection, communication and storage of personal data with the nature and extent of PNR data on all flights to or from a Member State of the Union.

14. The CNPD therefore recommends that paragraph 1 of article 1 be revised, providing for, there or in another provision, the application of this legal regime to flights to and from a Member State of Union only when there are "[...] sufficiently concrete circumstances that allow considering that there is a terrorist threat that appears to be real and current or foreseeable" (cf. point 171 of the "PNR Directive" judgment) and that such circumstances are densified in the law, specifying that they are delimited according to their connection to "certain air connections or travel arrangements, or to certain airports for which there are indications capable of justifying such application" (cf. paragraph 174 of the same judgment) .

15. It is recalled that only activities that are likely to seriously destabilize the fundamental constitutional, political, economic or social structures of a country, in particular of directly threatening society, the population or the State as such may, in accordance with the CJEU jurisprudence, be classified as terrorist threats, distinguishing themselves, by their nature, their particular gravity and the specific nature of the circumstances that constitute them, from the general and permanent risk that is that of serious criminal offenses (cf. point 170 of the cited judgment).

16. In other words, it is the understanding of the CJEU that the processing of PNR personal data on intra-EU flights is only necessary and proportionate if it is demonstrably aimed at preventing and repressing terrorist threats, no longer aiming at preventing and combating crime serious.

2 Accessible, respectively, at https://www.cnpd.pt/umbraco/surface/cnpdDecision/download/113Q00 and https://www.cnpd.pt/umbraco/surface/cnDdDecision/download/121616.

Av. D. Carlos 1,134,1o

1200-651 Lisbon

I (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

3v.

r

17. In order to ensure compliance with the application of this regime to data relating to intra-EU flights, it is also important that Law No. 21/2019 establishes a time limit for this application, without prejudice to possible renewal if the circumstances justifying the extension of the regime persist, and requires that the concrete assessment that such circumstances actually exist and justify the processing of PNR data is still subject to a concrete and binding decision by a judicial (and non-judicial) body or by an independent administrative entity (cf. point 172 of the judgment " PNR Directive"). The Law must also provide for the periodic reassessment, within a reasonable period (possibly three months), of the maintenance of these circumstances, in order to renew the interest based on the need, to stop processing the data of certain intra-EU flights or to change the collection for other flights.

18. It should be recalled in this regard that, as the same Court points out, in paragraph 245 of the "PNR Directive" judgment, '[the] requirement of independence that the entity in charge of carrying out prior supervision must satisfy also requires that it have the as a third party in relation to the authority requesting access to the data, so that said entity can carry out this inspection in an objective and impartial manner, protected from any external influence. In particular, in the criminal field, the requirement of independence implies that the authority in charge of that prior inspection, on the one hand, is not involved in conducting the criminal investigation in question and, on the other hand, has a position of neutrality in relation to the parties to the criminal proceedings. .» (our underlining).

ii. The specification (taxative) of the databases object of comparison

19. It follows from the PNR Directive that PNR personal data relating to extra-EU flights may be processed for the purposes of preventing, detecting, investigating and prosecuting terrorist offenses and serious crime, involving different types of operations.

20. It is recalled that under the terms of paragraph a) of paragraph 2 of article 5 of Law no. 21/2019, it is foreseen, at first, that the PNR data collected by the carriers are systematically transferred to the Cabinet of Passenger Information (GIP), where they are subject to an automated evaluation according to pre-defined criteria, resulting from the comparison with other personal data contained in the security forces' databases, which is processed under the terms described in n. 1 to 3 of Article 6. The positive results (hits) must then be subject to a second assessment, with human intervention (not automated), before being communicated to the competent authorities provided for in article 7, pursuant to paragraphs 4 to 6 of Article 6.

21. Furthermore, under the terms of subparagraph b) of paragraph 2 of article 5 of Law no. 21/2019, the GIP is obliged to communicate PNR personal data to the competent authorities at their request. This happens during the period of six months,

but also after this period has expired - period in which the data kept are masked, not allowing the direct identification of their holders, specifying that, in the latter case, the data communicated are full PNR personal data (/.e., without masking), although only if the assumptions set forth in paragraph 3 of article 11 of the Law are fulfilled.

22. As mentioned, the principle of proportionality obliges that the interference or restriction of fundamental data here in crisis, resulting from the processing of PNR personal data, must be limited to what is strictly necessary for the pursuit of the purposes of prevention, detection, investigation and repression of terrorist offenses and serious crime. Thus, the comparison of PNR data with other personal data, carried out in an automated way, must be confined to the databases under the responsibility of the security forces, which were created for the purposes of preventing, detecting, investigating and repressing terrorist offenses and serious crime, which must be specified in the law, as recommended by the CNPD in its Opinion No. 61/2017 and reiterated in Opinion No. 31/2018.

23. Indeed, the constitutional requirements of precision and clarity in the delimitation of interference or restriction to fundamental data here in crisis imply that that norm delimits the databases object of comparison with PNR data, and the relevant databases for this purpose.

24. Thus, paragraph a) of paragraph 1 of article 6 of Law No. 21/2019 must be amended in order to guarantee the proportionality of the interference with fundamental rights to the protection of personal data and respect for life private and family provided for in Article 6(3)(a) of the PNR Directive, as interpreted by the CJEU, that is, limiting the databases susceptible of comparison to those indicated in the final part of that provision (cf. point 188 of the judgment “PNR Directive", where it can be read that that precept «[...] must, in the light of these fundamental rights, be interpreted in the sense that these last databases are the only databases with which the UIP can compare PNR data"),

25. In short, the CNPD recommends amending paragraph a) of paragraph 1 of article 6 of Law no. 21/2019, in order to specify that the databases being compared are only those referred to in its final part, namely: databases on people or objects sought or targeted by an alert, in accordance with the rules applicable to these databases.

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

iii. Delimitation of serious crimes that justify the analysis of PNR data

26. In addition, it must be ensured that the analysis of PNR data depends on an objective connection, direct or indirect, between air passenger transport and one or more of the crimes provided for in Annex II of Law No. 21/2019.

27. Indeed, the CJEU concludes that «[...] Article 3, points 8 and 9, of this directive, in conjunction with Annex II thereof and in light of the requirements resulting from Articles 7. , 8 and 52(1) of the Charter, requires Member States to ensure, in particular in the individual verification by non-automated means provided for in Article 6(5) of that directive, that the application of the system established by it is limited to terrorist offenses and only to serious crimes which have an objective link, at least indirectly, with the carriage of passengers by air' (cf. point 157 of the judgment "PNR Directive").

28. In these terms, the CNPD recommends specifying, possibly in paragraph 1 of article 6 and in article 7 of Law no. 21/2019, that the processing of data by the competent authorities depends on the existence of a objective connection, direct or indirect, between the carriage of passengers by air and one of the serious crimes listed in Annex

iv. Limiting the reuse of PNR personal data for other purposes

29. Article 7(2) of Law No. 21/2019 limits the processing of PNR personal data to the purposes of preventing, detecting, investigating and repressing terrorist offenses or serious crime, in accordance with the principle purpose limitation. However, in the very next number, it admits that this limitation of purposes does not affect the fact that, when other infringements or indications of other infringements are detected in the course of actions triggered as a result of said processing, such data are processed by the police, customs or judicial authorities.

30. As worded, this provision allows PNR data to be used for other purposes.

31. Now, according to the interpretation of the CJEU, «[...] the list of purposes pursued by the processing of PNR data under the PNR Directive is exhaustive, whereby national legislation authorizing the processing of collected PNR data in accordance

with that directive for purposes other than those provided for therein, namely, in particular, to improve border controls and combat illegal immigration, is contrary to Article 6 of that directive, read in the light of the Charter' (cf. point 289 of the judgment "PNR Directive").

32. And the same Court specifies, in paragraph 290, that '[...] Member States may not create a single database containing both the PNR data collected under the PNR Directive and relating to extra- flights

EU and intra-EU data as well as passenger data on other means of transport, as well as data referred to in Article 3(2) of the API Directive...'. Precisely, the API Directive (Council Directive 2004/82/EC of 29 April 2004 on carriers' obligation to communicate passenger data) is aimed at improving border controls and combating illegal immigration, as of its recitals 1, 7 and 9, as well as of its article 1, through the advance transmission, by carriers, of passenger data to the competent national authorities.

33. It is therefore clear that the other purposes likely to justify the reuse of PNR data cannot correspond to the objectives of improving border control and combating illegal immigration, under penalty of contradicting paragraph 2 of article 1, ° and Article 6 of the PNR Directive, read in the light of Articles 7 and 8 of the Charter, having to integrate the domain specifically delimited in Article 1(2) of the PNR Directive.

34. In this regard, it is useful to recall the recent jurisprudence of the CJEU on the principle of limiting the purposes of processing personal data, where this Court explains, although with regard to Directive 2016/690, that «prevention», «detection », «investigation», «repression», «execution of criminal sanctions», «safeguard against threats to public security» and «threat prevention» aim at a plurality of purposes other than the processing of personal data covered by the scope of application thereof directive - cf. judgment of December 8, 2022, VS c. Inspetktor v Inspektorata kam Visshia sadeben savet (Case C-180/21), point 43.

35. To that extent, when, within the scope of application of a Directive, the further processing of data is permitted for a purpose other than that for which such data were collected, this permission assumes that this purpose is included among those set out to delimit the domain or scope of application of the same directive (cf., mutatis mutandis, paragraph 51 of the judgment of 8

December 2022, VS v. Inspetktor v Inspektorata kam Visshia sadeben savet).

36. As the CJEU also explains, in paragraph 52 of the latter judgment, "[in] particular, the personal data collected for the purposes of "prevention" and "detection" of criminal offenses or of "investigation" relating to such offenses may be further processed, where appropriate, by different competent authorities, with a view to "repression" or the "execution of criminal sanctions", when a criminal offense has been identified and therefore requires repressive action".

37. Bearing this jurisprudence in mind, it seems to us that we must conclude that paragraph 5 of article 7 of the PNR Directive must also be read in accordance with the principle of purpose limitation, i.e., interpreted in the sense that, within the scope purposes of the PNR Directive (prevention, detection, investigation and prosecution of terrorist offenses or serious crime), authorities may reuse PNR personal data for one of these

purposes in the context of an action or process other than the one that gave rise to the first use of PNR personal data.

38. To that extent, the CNPD recommends revising Article 7(3) of Law No. 21/2019, to specify that the reuse of data safeguarded therein assumes that the competence to be exercised is directly aimed at a specific purpose among those provided for in paragraph 2 of article 1 and densified by the catalog contained in Annex II of the Law.

v. PNR data retention periods

39. Article 11 of Law No. 21/2019 also needs to be revised, to ensure its compliance with EU law, consistent with the CJEU's interpretation of the PNR Directive. In fact, this article reproduces, in essence, article 12 of the PNR Directive, establishing, in its paragraph 1, a period of five years for the conservation of all PNR data, counting from the date of the respective transfer to the GIP.

40. In addition, paragraph 2 of article 11 of the Law provides for the "anonymization" of all PNR data within a period of six months, counted from the date of transfer, by masking some categories of data (listed in this provision), without prejudice to the possibility of reversing this anonymization process, whenever deemed necessary, based on reasonable grounds, for the purposes referred to in paragraph b) of paragraph 2 of article 5.0 of the Law, and upon authorization by the competent judicial

authority , provided for in paragraph 3 of the same article.

41. However, the CJEU takes the view that '[...] Article 12(1) of the PNR Directive, read in conjunction with Articles 7, 8 and 52, paragraph 1 of the Charter must be interpreted as meaning that it precludes national legislation which provides for a general retention period of PNR data of five years, applicable indifferently to all air passengers, including those for whom neither the prior assessment envisaged in Article 6(2)(a) of that directive, or any checks carried out during the period of six months provided for in Article 12(2) of that directive, or any other circumstance, revealed the existence of objective elements capable of establishing a risk in terms of terrorist offenses or serious crime which have an objective link, at least indirectly, with the carriage of passengers by air' (cf. point 263 of the judgment "PNR Directive").

42. Thus, in light of the principle of limitation of conservation, the retention of PNR personal data of all passengers for a period of six months does not deserve reservations, just as the retention of such data for a longer period does not raise reservations in relation to passengers who resulted in an automatic positive result verified and confirmed as indicating a risk for terrorist offenses or serious crime.

43. But as for the other passengers, for whom the automated assessment did not give a positive result or, if it did, such a result was invalidated through non-automated individual verification, the generalized retention of data for a period of five years (even if with risk mitigation measures, i.e., the masking of certain data) is not necessary to pursue the purposes of the PNR regime, as there are no objective elements capable of establishing a risk in terms of terrorist offenses or serious crime that present a link objective, at least indirect, with the air travel carried out by these passengers.

44. In these terms, the CNPD recommends revising article 11, in particular paragraphs 1 and 2, to differentiate the universe of passengers whose data may be kept for a period exceeding six months. It is further recommended to eliminate the reference to anonymization, since this expression should be reserved for situations where this process is irreversible and what is regulated in paragraph 2 of this article is a mere masking or pseudonymization of personal information (cf. article 4, point 5) of the GDPR).

45. Still regarding Article 11 of the Law, the CNPD reiterates the reservations it indicated in Opinion No. 31/2018 regarding the

provisions of No. 6.

46. Indeed, the hypothesis provided therein that, in cases where the positive result of the automated assessment is invalidated following an individual verification by non-automated means (false hit), data preserved can be retained in order to avoid false positive results in the future, provided that the data on which it was based are not erased under the terms of paragraph 4 of the same article, it is, if not unnecessary, at least excessive due to the risks involved in keeping them in a parallel database, which may , over time, assume considerable proportions. In this way, it could be possible to circumvent the principle of limiting the retention of personal data.

47. This conclusion is now reinforced, by virtue of the definition of the retention period of six months for all PNR data and the permission for retention for a longer period only of data relating to passengers who gave rise to an automatic positive result verified and confirmed as indicating a risk of terrorist offenses or serious crime. Indeed, this delimitation of the retention period of PNR data makes it impossible for them to be kept for more than six months in the event that the human assessment confirms that the result of the automated assessment corresponds to a false positive, with which the provisions of paragraph 6 of Article 11 becomes legally impossible or useless and must therefore be eliminated.

48. In these terms, the CNPD recommends revising article 11, in particular paragraphs 1 and 2, to differentiate the universe of passengers whose data may be kept for a period exceeding six months, and the revocation

of paragraph 6, in view of the legal impossibility or uselessness of the provisions therein. However, it is recommended to eliminate the reference to anonymization.

saw. Prior authorization for disclosure of full PNR data

49. Still in the context of article 11 of Law no. 21/2019, it is worth highlighting the provisions of no. 3. It provides, as already mentioned, that during the period in which the PNR personal data retained are masked, not allowing the direct identification of their holders, the data may be disclosed in full, "[...] if such disclosure is: a) Considered necessary, based on reasonable grounds, for the purposes referred to in paragraph b) Article 5(2); and b) where applicable, authorized by the competent

judicial authority."

50. It begins by pointing out that the real scope of the conditional wording of the second "if applicable" is not understood, since the PNR Directive requires prior authorization, which admits to being issued by «[...] i) a judicial authority, or (ii) another competent national authority, in accordance with national law, to verify that the conditions for disclosure are met, subject to the PIU's data protection officer being informed and carrying out an ex-post verification'.

51. Therefore, the conditional wording of this requirement for prior independent checking is not compatible with the PNR Directive, which imposes it on the Member States.

52. If, with such a reference, it is intended to exclude requests for access by Europol, it is clarified that nothing in the Directive legitimizes the exclusion of prior control for access and transmission of full PNR personal data, after the legal period of six months has elapsed, since Article 12(3) of the Directive does not distinguish solutions according to the nature of the applicant, nor does it make an exception to that rule for the cases provided for in Article 10 of the Directive.

53. Moreover, the eventual hypothesis that it was the GIP itself that issued the authorization is explicitly rejected by the CJEU, as it does not fulfill the quality of independence required by the Directive, when it states that «[...] it cannot be considered that the UIP has the status of a third party in relation to those same authorities and, as such, has all the qualities of independence and impartiality required to carry out the prior inspection mentioned in the previous paragraph of this judgment and verify that the conditions for disclosure of full PNR data, as provided for in Article 12(3)(b) of the same directive' (cf. paragraph 246 of the judgment "PNR Directive").

54. But the same requirement of independence, made explicit and developed by the CJEU, in point 245 of the same judgment, leads to the result that the Public Prosecutor's Office, as the competent judicial authority for directing the investigation, cannot assume this function of prior control of the disclosure of the data.

f

CNPD

'^>U XJ Ed— lirí/

National Data Protection Commission

55. In fact, the CJEU, in point 245 of the "PNR Directive" judgment, is clear in stating that "[the] requirement of independence

that the entity in charge of carrying out prior supervision must satisfy also requires that it has the status of a third party in relation to the authority requesting access to the data, so that said entity can exercise that control in an objective and impartial manner, protected from any external influence. In particular, in the criminal field, the requirement of independence implies that the authority in charge that prior inspection, on the one hand, is not involved in the conduct of the criminal investigation in question and, on the other hand, has a position of neutrality in relation to the parties to the criminal proceedings. (our italics).

56. And the provisions of paragraph 4 of article 32 of the CRP reinforce such an interpretation, by referring only to the judge the practice of instructive acts in criminal proceedings that are directly related to fundamental rights.

57. In these terms, the CNPD recommends revising paragraph b) of paragraph 3 of article 11 of Law no. 21/2019, in order to eliminate the expression "if applicable" and specifying that the prior authorization provided for therein is by the competent judicial authority, in order to comply with the requirement of prior authorization by an independent authority imposed by Article 12(3)(b) of the PNR Directive.

58. At the same time, the final part of Article 8(6) should be revised, also to provide that the authorization to issue is from the competent judicial authority.

vii. The personal data listed in Annex I

59. Finally, it is important to pay attention to the annexes to Law No. 21/2019, since, as explained above, precisely because it involves processing of personal data that represents a significant interference with the rights to respect for private life and privacy protection of personal data, the regulation of such interference must be clear and precise in determining the scope and application of the measures provided for therein, in accordance with the jurisprudence of the CJEU.

60. To that extent, the CJEU understands that imprecise concepts, used in Annex I of the PNR Directive to characterize the personal data to be collected, which do not contain any "limitation as to the nature and extent of the information that may be collected and provided" must be interpreted restrictively, considering only the type of information that is added there by way of example, as the only way to ensure certainty and predictability regarding the personal data being processed (cf. points 135 and 138 of the judgment “PNR Directive”) .

61. Thus, in Annex I of Law No. 21/2019, it is important to consider the data indicated in No. 12, which are imprecisely characterized, using the concept «general observations», followed by a statement

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

r

illustrative of the type of information contained therein. As the CJEU explains, in paragraph 136 of the aforementioned judgment, '[...] to give heading 12 an interpretation which, in application of the case-law recalled in paragraph 86 of this judgment, makes it comply with the requirements of clarity and Precisely and, more broadly, with Articles 7, 8 and 52, paragraph 1, of the Charter, it must be considered that only the collection and communication of information expressly listed under this heading is permitted , namely the name and gender of the minor air passenger, his age, the language(s) spoken, the name and contact details of the person accompanying him at the time of departure and his relationship with the minor, the name and contact details of the person who accompanies him upon arrival and his relationship with the minor, the agent present at departure and arrival».

62. At the same time, in paragraph 18 of Annex I of the Law, when referring to "[all prior information on passengers (API data) that has been collected, including [...]", such information can only be the API data expressly listed in that paragraph and in Article 3(2) of the API Directive (see paragraphs 138 and 139 of the judgment "PNR Directive").

63. In these terms, the CNPD recommends revising paragraphs 12 and 18 of Annex I of Law No. 21/2019, in order to accurately and clearly delimit the personal data subject to processing.

viii. The integration of the GPI in the PUC-CPI

64. It is also clear from the PNR Directive and the judgment of the CJEU that the PIU “is a competent authority for the purposes of preventing, detecting, investigating or repressing terrorist offenses and serious crime” (cf. paragraph 246 of the judgment). It is recalled that the Directive, in Article 4(1), determines that "[e]e Member State shall create or designate a competent authority for the purposes of preventing, detecting, investigating or prosecuting terrorist offenses and criminality serious, or creates or designates a section of such an authority, to act as its 'Passenger Information Unit'.

65. As the Portuguese State created the GIP, as a PIU, this office assumes the role of competent authority for the purposes of preventing, detecting, investigating or repressing terrorist offenses and serious crime. As such, the GIP must be responsible for the PNR database, which, according to this perspective, implies that this body must be part of an organic structure with the same nature as a competent authority for the purposes of prevention, detection, investigation or repression terrorist offenses and serious crime.

66. However, the inclusion of the GPI in the Single Point of Contact for International Police Cooperation (PUC-CPI) implies several violations of European Union Law, in particular, as will be explained below, the

processing of PNR personal data by a body that has no competence for the purposes of preventing, detecting, investigating or repressing terrorist offenses and serious crime.

67. In addition, the provisions contained in paragraph 3 of article 8 and paragraph 2 of article 13 of Law No. 21/2019, as they are written, seem to intend to legitimize the duplication of personal data PNR, which clearly contradicts the provisions of the PNR Directive and proves to be an illicit data processing, in the light of the Union data protection regime, due to manifest disproportion in relation to the attributions and competences of the PUC-CPI, allowing other entities that members of the PUC-CPI, without criminal investigation competence, may be aware of this sensitive information, going beyond the respective legal attributions.

68. It should be recalled, in this regard, that the CJEU in the judgment “PNR Directive" insists that the list of purposes of the PNR Directive is exhaustive, even stating, in paragraph 236, that «[...] insofar as [...] national legislation admits, as the purpose of processing PNR data, the monitoring of activities aimed at by intelligence and security services, thus integrating this purpose into the prevention, detection, investigation and repression of terrorist offenses and serious crime, this legislation is liable to infringe the exhaustive nature of the list of purposes pursued by the processing of PNR data under the PNR Directive [...]'.

69. As the CNPD mentioned in its Opinion No. 31/2018,

«Under the terms of paragraph 1 of article 23-A of the Internal Security Law, the PUC-CPI is the operational center responsible for coordinating international police cooperation, which ensures the forwarding of requests for national information, the

reception, forwarding and national dissemination of information from foreign police authorities, transmission of information and fulfillment of requests made.

Indeed, the PUC-CPI intends to be a common entry and exit door, at national level, within the scope of international police cooperation, managing in a more centralized way the ways for the exchange of information. The PUC-CPI works in dependence and under the coordination of the General Secretary of the Internal Security System (SG/SSI).

Therefore, PUC-CPI is not an authority nor does it have any legal attributions that allow it to maintain and manage a database for the purposes of preventing and investigating terrorist offenses or serious crime, such as the one in question here with the data PNR. [...]».

Av. D. Carlos 1,134,1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

70. Thus, the provision in no. 3 of article 8 of Law no. 21/2019 that the GIP informs the operational center of the PUC-CPI of the data transmitted to the competent national authorities, coming from other Member States. Members, has no support in the Directive, as is clear from its comparison with Article 9(3) of the PNR Directive.

71. The same can be said about the provision that, in the event of an emergency, with a direct request by the competent national authorities to a passenger information unit in another Member State, a copy of the request should be sent to the PUC-CPI (no. 7 of article 8 of the Law).

72. Also the provision, in paragraph 2 of article 13 of the Law, that the PUC-CPI keep a copy of all requests submitted by the competent authorities, by the passenger information units of other MS and by Europol, as well as as with all requests and transfers of PNR data to a third country, it is not based on any rule of the Directive or any provision of EU law, corresponding to a rule that is manifestly unnecessary and excessive in the interference of fundamental rights to the preservation of privacy

and to the protection of personal data.

73. The existence of a PNR database is, it is insisted, limited to the purposes of prevention, detection, investigation and repression of terrorist offenses and serious crime, the pursuit of which is the responsibility of the entities with competence for the purpose, not being the PUC-CPI, in the exercise of auxiliary functions of single point of contact, legitimated to create and keep PNR personal data.

74. Furthermore, given the legislation that establishes the organization and functioning of the Single Point of Contact for International Police Cooperation, there is no legitimacy basis for such a prediction.

75. There is no justification for providing that the PUC-CPI keeps a vast set of personal data relating to the PNR in a database, when it is not a competent authority for the purposes of the PNR Directive, and consequently of Law No. 21/2019 , not being, therefore, qualified to keep this data.

76. In these terms, paragraphs 3 and 7 of article 8 should be revised, to remove the reference to "with knowledge of the PUC-CPI operational center" and "sending a copy of the request to PUC-CPI" , respectively, and revoked paragraph 2 of article 13, as it has no support in the Directive, contrary to its provision when it limits the creation of a PNR database under the sole responsibility of the UIP, and for embodying a measure unnecessary and excessive legislation in view of the functions of a single point of contact for data transfers.

III. Conclusion

77. On the grounds set out above, in order to ensure compliance of the legal regime relating to the registration of air passenger names with the PNR Directive, interpreted in accordance with Articles 7, 8, 45 and 52 of the Charter of Fundamental Rights of the European Union, and to ensure the proportional restriction of the rights to privacy and the protection of personal data, enshrined in articles 26 and 35 of the Constitution of the Portuguese Republic, the CNPD recommends revising the Law No. 21/2019, of February 25, highlighting the following legal provisions:

The. paragraph 1 of article 1, providing for the application of this legal regime to flights to and from a Member State of the European Union only if the processing of personal data of passengers is effective and demonstrably necessary for prevention and repression of terrorist threats and in the circumstances explained above, in points 14 to 18;

B. subparagraph aj of paragraph 1 of article 6, in order to specify that the databases object of comparison are only those

referred to in its final part, namely: databases on people or objects sought or targeted by a alert, in accordance with the rules applicable to these databases (cf. above, paragraphs 23 and 24);

w. paragraph 3 of article 7, to add that the reuse of data safeguarded therein assumes the pursuit of a specific purpose among those provided for in paragraph 2 of article 1, and densified by the catalog contained in Annex II of the Law, as explained above, in points 30 to 38;

d. article 11, in particular paragraphs 1 and 2, to differentiate the universe of passengers whose data may be kept for a period exceeding six months, and the revocation of paragraph 6, in the face of legal impossibility or the uselessness of its provisions. It is further recommended that the reference to anonymization be deleted, in the terms explained above, in points 44, 45 and 48;

It is. paragraph b) of paragraph 3 of article 11 of Law no. 21/2019, in order to eliminate the expression "if applicable" and to specify, either in that item or in paragraph 6 of article 8 of the same law, that the prior authorization is from the competent judicial authority (cf. above, points 51 to 56);

f. n.º 3 and n.º 7 of article 8, to remove the reference to «with knowledge to the operational center of PUC-CPI» and «sending a copy of the request to PUC-CPI», respectively, and revoking n. 2 of article 13, as it has no support in the Directive, contrary to its provisions when it limits the creation of a PNR database under the sole responsibility of the UIP, and for embodying a measure

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

unnecessary and excessive legislation in view of the single point of contact for data transfers (cf. above, paragraphs 66 to 75);

g. paragraphs 12 and 18 of Annex I of Law No. 21/2019, in order to accurately and clearly delimit the personal data subject to processing, in the terms explained above, in points 60 to 62;

H. provision, possibly in paragraph 1 of article 6 and in article 7, that the processing of data by the competent authorities depends on the existence of an objective connection, direct or indirect, between the air transport of passengers and one of the crimes serious problems listed in Annex II (see above, point 27).

Approved at the meeting on December 21, 2022

Fiipa Calvao (President)