Warsaw, 13 June 2025
Opinion-Nr.: TERR-UKR/526/2025 [NR]

OPINION ON THE DRAFT LAW OF UKRAINE "ON THE USE OF PASSENGER INFORMATION FOR COMBATING TERRORISM, SERIOUS AND ESPECIALLY SERIOUS CRIMES"

UKRAINE

This Opinion has benefited from contributions made by **Mr. Karim Labib**, Senior Expert in Criminal Law, Anti-money Laundering and Countering the Financing of Terrorism (AML/CFT) and Terrorism; and **Ms. Nazli Yildirim Schierkolk**, Independent Expert on Security Sector Reform and Human Rights.

Based on an unofficial English translation of the Draft Law provided by the Security Service of Ukraine.

OSCE Office for Democratic Institutions and Human Rights

Ul. Miodowa 10, PL-00-251 Warsaw
Office: +48 22 520 06 00, Fax: +48 22 520 0605
www.legislationline.org

EXECUTIVE SUMMARY AND KEY RECOMMENDATIONS

The development of a Draft Law on the Use of Passenger Information for Combating Terrorism and Serious Crimes marks a significant and timely effort by Ukraine to establish a comprehensive legal framework for the processing of Advance Passenger Information (API) and Passenger Name Record (PNR) data in the context of air travel. Whilst many provisions align with international obligations, gaps remain that prevent full compliance with international personal data protection standards and the right to privacy, as derived from the international and regional human rights instruments. The Draft Law could also be improved not to unduly impact individuals' right to freedom of movement and not to directly or indirectly affect the rights of individuals in need of specific protection, such as refugees and asylum-seekers, children and victims of trafficking. In particular, some adjustments should be made, particularly concerning personal data purpose limitation, proportionality, data retention, automated processing, data transfers, and individual rights.

Refining the scope of the Draft Law to clearly limit data processing to clearly defined terrorist and serious crimes with a direct or indirect link to air travel would help ensure compliance with the principle of purpose limitation and prevent overly broad application. Similarly, reducing the retention period for PNR data to six months, with extensions up to five years allowed only where there is an objective and specific need, would better reflect the requirement of proportionality.

Incorporating robust safeguards for automated data processing, including mandatory human review, exclusion of discriminatory profiling, and clear, objective criteria, would strengthen protections against potential arbitrary application. It would also be valuable to reinforce the rights of individuals by explicitly providing access to their data, the ability to correct or delete it, and effective remedies in case of misuse.

Implementing the recommended changes will enhance compliance with international and regional human rights instruments and better balance security objectives with human rights obligations.

More specifically, and in addition to what is stated above, ODIHR makes the following recommendations to further enhance the compliance of the Draft Law with applicable regional and international human rights standards and OSCE commitments:

A. With respect to purpose limitation:

   1. to align the purpose of the PNR data collection, namely for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes only, to prevent disproportionate data collection and it being used as a mass surveillance tool, exceeding the aims laid out in international standards; [par 58]

2. to reflect in the Draft Law to delete other third-party personal data immediately and permanently by the PIU upon receipt; [par 60]

B. to ensure that data collection is limited to what is strictly required for the purpose of preventing, detecting, investigating and prosecuting terrorism and serious crimes in line with the principle of data minimization and to provide an explicit stipulation about the duty to immediately and permanently delete data that is outside of the prescribed categories in the Draft Law, including any sensitive data; [par 63]

C. to reflect in Article 18 of the Draft Law that:

- the non-automated review should exclude any discriminatory results;
- the PIU shall not transfer the results of those automated processing operations to the competent authorities when they conclude, following that review, that they do not have anything capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime in respect of the persons identified by means of those automated processing operations or when they have reason to believe that those processing operations lead to discriminatory result;
- the PIU establishes, in a clear and precise manner, objective review criteria enabling PIU agents in charge of individual review to verify, on the one hand, whether and to what extent a positive match concerns effectively an individual who may be involved in the terrorist offences or serious crime and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of the EU PNR Directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations and, in particular, the pre-determined criteria and databases used;
- Any pre-established criteria against which PNR data are compared do not lead to unlawful differentiation and ensure that discriminatory results are excluded;
- A safeguard clause concerning asylum applications is included in this provision; [pars 68-70]

D. to explicitly list the authorized bodies either in the Draft Law, or as and annex to the Draft Law or make a refence to the relevant legislation which regulate these authorized bodies and to elaborate the mechanisms of independent review prior to responding to duly reasoned request from competent authorities for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime; [pars 71-72]

E. to provide in Article 24 of the Draft Law that before entering into an API/PNR data sharing agreement, or sharing such data on an ad hoc basis, an assessment should be made of the counterpart's record on human rights and data protection, as well as of the legal safeguards and institutional controls that govern the recipient authority, to ensure that the third country meets equivalent protection standards. This agreement should also be re-assessed regularly or as warranted; [par 82]

F. to put in place effective human rights safeguards to protect passengers from being wrongfully placed under suspicion for involvement in terrorism or other serious crimes and refrain from discriminatory profiling on the basis of PNR

data in listing the tasks of the National Contact Point in Article 15. Risk criteria and profiles need to be targeted, proportionate and specific and should mandate the relevant authorities to provide necessary guidance for individual reviews to prevent discriminatory results; [par 86]

G. to clarify in Article 21 of the Draft Law that the PNR data protection officers can report to the Commissioner directly and in confidentiality, and that they can refer cases to the Commissioner and undertake other actions; [par 95] and

H. to ensure that any oversight of compliance with data regulation is carried out independently by the authorized body, which is granted the necessary resources and powers to fulfil its mandate in a manner consistent with international instruments and to ensure that this body, or the Human Rights Commissioner, be given full and unhindered access to all information processed by the PIU as well as pre-determined criteria and databases to be able to fulfil its mandate. [pars 98-99]

These and additional Recommendations, are included throughout the text of this Opinion, highlighted in bold.

As part of its mandate to assist OSCE participating States in implementing their OSCE human dimension commitments, ODIHR reviews, upon request, draft and existing laws to assess their compliance with international human rights standards and OSCE commitments and provides concrete recommendations for improvement.

TABLE OF CONTENTS

I. INTRODUCTION 6

II. SCOPE OF THE OPINION 6

III. LEGAL ANALYSIS AND RECOMMENDATIONS 7

1. Relevant International Human Rights Standards and OSCE Human Dimension Commitments 7

1.1. Standards Pertaining to Collection, Processing and Sharing of Data in the Context of Air Travels 8

1.2. Data Protection and Right to Privacy 13

1.2.1. Right to Privacy 14

1.2.1 Right to Data Protection 16

1.2.3. Potential Impact on Other Human Rights and Fundamental Freedoms 20

2. Background 21

3. Collection, Processing and Sharing API/PNR Data 21

3.1. Purpose Limitation 21

3.2. Collection and Processing of API/PNR Data 23

3.3. Automated Processing 25

3.4. Data Sharing with Authorized Bodies 27

3.5. Data Retention 29

3.6. International Co-operation 30

4. Non-Discrimination 31

5. Duty to Inform and Security of Personal Data 34

6. Independent Oversight 36

7. Appeals Mechanisms and Judicial Review 37

8. Recommendations Related to the Process of Preparing and Adopting the Draft Law 38

ANNEX: Draft Law of Ukraine "On the Usage of Passenger Information for Combating Terrorism, Serious and Especially Serious Crimes"

I. INTRODUCTION

1. On 20 September 2024, the Deputy Head of the Security Service of Ukraine sent to the OSCE Office for Democratic Institutions and Human Rights (hereinafter "ODIHR") a request for a legal review of the Draft Law of Ukraine "On the Usage of Passenger Information for Combating Terrorism, Serious and Especially Serious Crimes" (hereinafter "the Draft Law").
2. On 17 October 2024, ODIHR responded to this request, confirming the Office's readiness to prepare a legal opinion on the compliance of the Draft Law with international human rights standards and OSCE human dimension commitments. In light of the subject-matter, ODIHR invited the Border Security and Management Unit of the OSCE Secretariat to contribute to this legal review.
3. This Opinion was prepared in response to the above request. ODIHR conducted this assessment within its mandate to assist the OSCE participating States in the implementation of their OSCE human dimension commitments.[1]

II. SCOPE OF THE OPINION

4. The scope of this Opinion covers only the Draft Law submitted for review. Thus limited, the Opinion does not constitute a full and comprehensive review of the entire legal and institutional framework regulating information gathering for the purpose of combating terrorism, serious and especially serious crimes in Ukraine.
5. The Opinion raises key issues and provides indications of areas of concern. In the interest of conciseness, it focuses more on those provisions that require amendments or improvements than on the positive aspects of the Draft Law. The ensuing legal analysis is based on international and regional human rights and rule of law standards, norms and recommendations as well as relevant OSCE human dimension commitments. The Opinion also highlights, as appropriate, good practices from other OSCE participating States in this field. When referring to national legislation, ODIHR does not advocate for any specific country model; it rather focuses on providing clear information about applicable international standards while illustrating how they are implemented in practice in certain national laws. Any country example should always be approached with caution since it cannot necessarily be replicated in another country and has always to be considered in light of the broader national institutional and legal framework, as well as country context and political culture.
6. Moreover, in accordance with the *Convention on the Elimination of All Forms of Discrimination against Women*[2] (hereinafter "CEDAW") and the *2004 OSCE Action Plan for the Promotion of Gender Equality*[3] and commitments to mainstream gender into OSCE activities, programmes and projects, the Opinion integrates, as appropriate, a gender and diversity perspective.

1 In particular, ODIHR conducted this assessment within its mandate as established by the OSCE Bucharest Plan of Action for Combating Terrorism. See pars 6, 18 and 22 of the Annex to OSCE Ministerial Council Decision MC(9).DEC/1, Bucharest, 3-4 December 2001.

2 UN Convention on the Elimination of All Forms of Discrimination against Women (hereinafter "CEDAW"), adopted by General Assembly resolution 34/180 on 18 December 1979. Ukraine deposited its instrument of ratification of this Convention on 12 March 1981.

3 See OSCE Action Plan for the Promotion of Gender Equality, adopted by Decision No. 14/04, MC.DEC/14/04 (2004), par 32.

7. This Opinion is based on an unofficial English translation of the Draft Law provided by the Security Service of Ukraine, which is attached to this document as an Annex. Errors from translation may result. The Opinion is also available in Ukrainian. However, the English version remains the only official version of the Opinion.

8. In view of the above, ODIHR would like to stress that this Opinion does not prevent ODIHR from formulating additional written or oral recommendations or comments on respective subject matters in Ukraine in the future.

III. LEGAL ANALYSIS AND RECOMMENDATIONS

1. RELEVANT INTERNATIONAL HUMAN RIGHTS STANDARDS AND OSCE HUMAN DIMENSION COMMITMENTS

9. Over the last decades there has been an increase of people travelling by air. Simultaneously, innovations resulting in bigger airplanes have led to a need for more efficient and effective passenger flows at airports. In 2019, the International Civil Aviation Organisation (hereinafter "ICAO") reported 4.5 billion passengers were globally carried by air transport on scheduled services.[4] These passenger flows put increasing pressure on the international air borders. Against this background, over the last decade there has been a growing body of international and regional legally binding and soft law instruments on the collection, processing and sharing of Advance Passenger Information (API) and Passenger Name Record (PNR) data, especially in the context of countering terrorism and other serious crimes.

10. API data is a set of information concerning the travellers directly taken from their passports, combined with flight information collected at check-in and transferred to the border agencies of the country of destination. The processing of API is a border management tool aiming to enhance effectiveness and efficiency of border checks, by facilitating and speeding up traveller clearance, as well as an instrument to counter irregular immigration.[5]

11. PNR data is unverified information provided by passengers either directly or through travel agencies and collected by air carriers to enable the reservation and check-in processes. The analysis of PNR data can provide the authorities with important elements from a criminal intelligence point of view, allowing them to detect suspicious travel patterns and identify associates of criminals and terrorists, in particular those previously unknown to law enforcement.[6]

12. The collection of personal data contained in API and PNR datasets, its use, sharing and processing, which may also impact decision-making at international borders, have serious implications with respect to individuals' rights to respect for private and family life, to freedom of movement (rights of persons to leave any country and to return to their country of origin), and to seek asylum, and potentially also other fundamental rights and freedoms (particularly freedom of expression, political participation, freedoms of peaceful assembly, of association, and religion or belief), and to be free from discrimination.

4 International Civil Aviation Organisation (ICAO), The World of Air Transport in 2019.
5 COM (2022) 729 Proposal for a Regulation Of The European Parliament And Of The Council On the collection and transfer of advance passenger information (API) for enhancing and facilitating external border controls, amending Regulation (EU) 2019/817 and Regulation (EU) 2018/1726, and repealing Council Directive 2004/82/EC, (hereinafter "EU API Proposal"), page 1,
6 European Commission – Passenger Data.

13. At the outset, it must be underlined that the necessity and proportionality of non-targeted, bulk collection and processing of passenger data for the purpose of countering terrorism and other serious crime have been questioned – particularly due to the lack of serious, reliable, and verifiable evidence supporting its effectiveness, and concerns about the reliability of such systems, especially given how even small errors can have significant consequences when applied to the very large number of air travellers.[7] While it goes beyond the scope of this Opinion to assess the necessity and effectiveness of such schemes, the present legal analysis aims to provide recommendations to ensure that the API/PNR scheme contemplated in the Draft Law is compliant with international human rights standards and OSCE commitments.

1.1. Standards Pertaining to Collection, Processing and Sharing of Data in the Context of Air Travels

14. Within the UN system, in the context of countering terrorism, the United Nations Security Council (hereinafter "UNSC") adopted several resolutions, calling upon Member States and airlines to collect and process relevant passenger data. In 2014, the UNSC Resolution 2178 called upon UN Member States to require that airlines operating in their territories provide API to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee established pursuant to resolutions 1267 (1999) and 1989 (2011) (and later 2253 (2015)) ("the UNSC Committee"); in addition, UN Member States were urged to report any such departure from their territories, or such attempted entry into or transit through their territories, of such individuals to the UNSC Committee, as well as to share this information with the State of residence or nationality, as appropriate and in accordance with domestic law and international obligations.[8]

15. In 2016, the UNSC Resolution 2309 required that "*airlines operating in their territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015)"*.[9]

16. In December 2017, the UNSC unanimously adopted Resolution 2396.[10] Building upon previous Resolutions 2178 (2014) and 2309 (2016), it decides that UN Member States shall collect API and PNR data. As UNSC Resolution 2396 was adopted under Chapter VII of the UN Charter and includes language suggesting the intent to be legally binding,[11] compliance with this obligation is mandatory for all UN Member States. This Resolution establishes that states "…*shall require airlines operating in their territories to provide API to the appropriate national authorities, in accordance with domestic law and international obligations*…" and "…*to ensure API is analysed by all relevant authorities,*

7 See e.g., the European Data Protection Supervisor Opinions, especially Opinion 5/2015 on the EU PNR Directive and the Opinion on the EU-Canada draft agreement; see also Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, *Position Paper on the United Nations Countering Terrorist Travel ('CT Travel') Programme and the goTravel Software Solution* (2023). See also ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021), p. 13, and references therein.

8 UNSC Committee pursuant to resolutions 1267 (1999) 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities; see UNSC, S/RES/2178 (2014), para. 9

9 UNSC, S/RES/2178 (2016), para. 6g.

10 UNSC, S/RES/2396 (2017).

11 While the UNSC has general powers under Articles 24 and 25 of the UN Charter to adopt binding decisions, which do not need to be always taken under Chapter VII of the UN Charter, the binding effect of the provisions of a resolution of the UNSC is to be determined in each case, having regard to the terms of the resolution to be interpreted, the discussions leading to it, the Charter provisions invoked and, in general, all circumstances that might assist in determining the legal consequences of the resolution of the Security Council. See International Court of Justice (ICJ), *Advisory Opinion on the Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)*, 21 June 1971, paras. 113-114.

with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting, and investigating terrorist offenses and travel…"[12] The Resolution also decides that "…*Member States shall develop the capability to collect, process and analyse, in furtherance of ICAO standards and recommended practices, passenger name record (PNR) data and to ensure PNR data is used by and shared with all their competent national authorities, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offenses … and also urges ICAO to work with its Member States to establish a standard for the collection, use, processing and protection of PNR data."*[13]

17. Another key instrument in this area is the Convention on International Civil Aviation (also referred to as "the Chicago Convention").[14] Article 37 of the Chicago Convention mandates the International Civil Aviation Organisation (ICAO) to "*adopt and amend as may be necessary…, international standards and recommended practices and procedures dealing with….customs and immigration procedures…*".[15] In this context, ICAO developed 'International Standards and Recommended Practices', which forms the Annex 9 to the Chicago Convention. The standards and practices are regularly updated, most recently in July 2022.[16] Chapter 9 of Annex 9 is exclusively dedicated to passenger data exchange systems, outlining standards and practices in regulating API and PNR. Annex 9 stipulates robust standards and safeguards for the personal data protection aspects of regulating API/PNR, including on safeguards on legality, necessity and proportionality, standards on access to PNR and the duty to inform the data subject, safeguards against automated processing of PNR data, standards on independent oversight of PNR data, safeguards against discrimination and standards and recommended practices on processing PNR data.[17]

18. In December 2016, OSCE Ministerial Council adopted the Decision No. 6/16 on 'Enhancing the Use of Advance Passenger Information' which commits participating States to establish national API systems in accordance with the provisions contained in ICAO's Annex 9 to the Chicago Convention and aligned with the ICAO Guidelines on API, including those on privacy and data protection, in order to effectively collect passenger and/or crew data from airlines operating in their territories.[18] It is noteworthy that the OSCE Decision makes an explicit reference to privacy and data protection standards.

19. At the Council of Europe level, the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*[19] and the *Convention on Access to Official Documents*[20] should also be taken into consideration with respect to the present topic.

20. As a candidate for accession to the European Union, Ukraine also needs to align its national legislation with the EU acquis and thus, the relevant EU treaty provisions, Regulations and Directives are also of relevance to this Opinion. In this respect it is noted that the Draft Law was developed as part of a comprehensive assessment of the

12 UNSC, S/RES/2396 (2017), para. 11.
13 UNSC, S/RES/2396 (2017), para. 12.
14 Ukraine submitted a notification of adherence on 10 August 1992.
15 The Convention on International Civil Aviation (Chicago Convention) was signed on 7 December 1944 by 52 States. Ukraine submitted its instrument of accession to the Chicago Convention on 10 August 1992.
16 ICAO, Annex 9 to the Convention on International Civil Aviation, International Standards and Recommended Practices, Sixteenth Edition, July 2022.
17 Chicago Convention, Annex 9, Chapter 9.
18 OSCE Ministerial Council, MC.DEC/6/16, Enhancing The Use Of Advance Passenger Information, Article 1.
19 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 28 January 1981, ratified by Ukraine on 30 September 2010 and which entered into force on 1 January 2011. Its *Protocol* (CETS No. 223) has not yet been signed nor ratified by Ukraine.
20 Council of Europe, Convention on Access to Official Documents (CETS No. 205), 18 June 2009, signed by Ukraine on 12 April 2018, ratified by Ukraine on 19 August 2020 and entered into force on 1 December 2020.

transposition of European Union legal standards into the legislation of Ukraine and with a view to carry out the implementation of the EU PNR Directive, aimed at the legislative regulation of obtaining, processing and use of such information for countering terrorism and serious crime.

21. In the European Union (EU), the collection, processing, and sharing of API/PNR data is regulated by Directives, which are binding on EU Member States as to the results to be achieved and must be transposed into the national legislation. On 27 April 2016, the European Parliament and Council adopted the Directive on the use of PNR data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crimes (hereinafter the "EU PNR Directive").[21] The Directive defines the responsibilities of EU Member States regarding the collection of PNR data, requiring them to establish specific entities responsible for the collection, storage, and processing of PNR data (the so-called passenger information units (PIUs)) and adopt a list of competent authorities entitled to request or receive PNR data. The PIUs are in charge of collecting PNR data from airlines, comparing PNR data against relevant law enforcement databases and processing them against pre-determined criteria, to identify persons potentially involved in a terrorist offence or serious crime, and, disseminating PNR data to national competent authorities, Europol, and PIUs of other EU countries, either spontaneously or in response to duly reasoned requests.[22]

22. The EU PNR Directive also provides important data protection safeguards, namely that sensitive data must not be processed and that data must be depersonalised after six months, may be re-personalised only under strict conditions, must be deleted after five years, and that a data protection officer is appointed in each PIU and independent national supervisory authorities must oversee the processing activities. The EU PNR Directive is the most comprehensive and detailed legal tool in the European region regulating the processing of PNR data.

23. The Court of Justice of the European Union (CJEU) provided a ruling on the legality of the EU PNR Directive which further underlined that the Directive must be read in the light of Articles 7 (Respect for private and family life), 8 (Protection of personal data) and 21 (Non-discrimination) as well as Article 52(1) (Legality, Necessity and Proportionality of Restrictions) of the EU Charter of Fundamental Rights and clarified the application of necessity, proportionality, and data protection standards under EU law. The recent Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of the CJEU ruling provides further useful guidance.[23] In the judgement, the CJEU affirmed that the collection and use of PNR data must be strictly limited to combatting terrorist offenses (defined under EU Directive 2017/541)[24] and to serious crime (as defined by the PNR Directive and linked to organized crime or offenses punishable by severe penalties). Vague or overbroad definitions of terrorism or serious crimes contravene the principle of purpose limitation, rendering the interference with privacy disproportionate.[25] As for the indiscriminate collection of all passengers' PNR data, it may only be justified under exceptional circumstances, such as a genuine and sufficiently serious threat to public security. Bulk collection for all

21 European Union, 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, detection, investigation and prosecution of terrorist offences and serious crime (hereinafter "EU PNR Directive").

22 European Commission, Passenger Data.

23 See European Data Protection Board (EDPB), *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025.

24 For some comments regarding the human rights compliance of the definition of "Terrorist Offence" in the EU Directive 2017/541 on Combatting Terrorism, see *ODIHR Note on the Proposed Revision of the Definition of Terrorist Offences in Article 1 of the Council of Europe Convention on the Prevention of Terrorism* (2023), especially para. 12.

25 For detailed discussion, see: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 141-175; Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Report to General Assembly 76th session, 3 August 2021, A/76/261, para. 16.

passengers without differentiation or a concrete link to public security risks exceeds proportionality requirements. In any case, bulk collection must not lead to the permanent, systematic surveillance of all travellers.[26] The CJEU further held that retention periods must be strictly necessary and proportionate to the public security objective. Key requirements in this regard include to have short retention periods for initial analysis, that data should be retained for a short, pre-defined period (6 months) before anonymization and that data access after anonymization must be tied to specific cases, with judicial or administrative approval. Beyond this period, retention is only allowed if there is an ongoing investigation or link to a specific threat and retaining non-anonymized data beyond 6 months is permissible only when strictly justified by case-specific risks.[27] The CJEU further held that automated processing of PNR data is permissible but must be limited to identifying passengers who may be involved in terrorist or serious criminal activities and to avoid using discriminatory criteria (e.g., based on "race",[28] religion, or ethnicity). In addition, automated matches must be verified by a human before enforcement action is taken and fully automated decision-making without human intervention risks violating privacy and due process rights. [29]

24. With respect to transfers of PNR data to third countries, the latter must ensure an equivalent level of data protection to that provided under EU law. Such transfers must be based on agreements or adequacy decisions under the General Data Protection Regulation's framework[30] and limit transfers to cases where the receiving state will use the data exclusively for combating terrorism or serious crime. Data-sharing agreements with countries lacking robust protections or unclear safeguards contravene EU data protection standards.[31] Before transferring PNR data, it is also fundamental that an assessment be made of the third country's record on human rights and data protection, as well as of the legal safeguards and institutional controls and oversight that govern the authority receiving such data.[32] There should also be a clear undertaking not to transfer such PNR data which is likely to be used for purposes that violate human rights, e.g., that would ultimately result in torture or other ill-treatment or would enable a country to repress free speech or human rights defenders or allow further human rights violations.[33]

---

26 For detailed discussion, see: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 158-175; D. Lowe, The European Union's Passenger Name Record Data Directive 2016/681: Is it fit for purpose? International Criminal Law Review 17 (1), 2017, p. 27.

27 For detailed discussion, see: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 214-228; 248-262; Privacy International, Response to Model Legal Provisions, 16 Nov 2021, p. 4, 6.

28 While recognizing that the term "race" is a purely social construct that has no basis as a scientific concept, for the purpose of the opinion, the term "race" or "racial" may be used in reference to international instruments using such a term to ensure that all discriminatory actions based on a person's (perceived or actual) alleged "race", ancestry, ethnicity, colour or nationality are covered - while generally preferring the use of alternative terms such "national or ethnic origin"; the use of the term 'race' in this Opinion shall not imply endorsement by ODIHR of any theory based on the existence of different 'races' (see e.g., 2022 ODIHR Practical Guide on Hate Crime Laws, revised edition, footnote 14 and Sub-Section 2.3.1 and references therein).

29 For detailed discussion, see: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, 21 Jun 2022, paras. 176-181, 202-213.

30 The European Commission has the power to determine, on the basis of Article 45 of Regulation (EU) 2016/679Regulation (EU) 2016/679 whether a country outside the EU offers an adequate level of data protection.

31 For detailed discussion, see: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 183-192; Privacy International, Response to Model Legal Provisions, 16 Nov 2021, p. 5-6.; Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Response to Call for Input by OHCHR on Privacy in Digital Age, p. 6-8.

32 See e.g., as a comparison, UN Special Rapporteur on the protection and promotion of human rights while countering terrorism, *Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism* (2010), Practice 33; see also ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), page 43.

33 See e.g., *Venice Commission, Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)011; *2015 Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)006, para. 75. See also UN Special Rapporteur on the protection and promotion of human rights while countering terrorism, *Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism* (2010), Practice 33; and ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), page 43.

25. Individuals whose PNR data are collected must have enforceable rights, including the right to access, rectify, and delete their data, and the right to an effective remedy in case of violation that must be prompt, practical rather than theoretical, accessible (without undue practical or financial barriers) and before an independent authority.[34] They also have the right to be informed of data processing practices and must have judicial or administrative remedies to challenge unlawful processing.[35] Failure to provide accessible rights and remedies for passengers undermines accountability and transparency obligations. Further, PNR data may be cross-checked against predefined watchlists. If this is the case, these watchlists should be precise, regularly updated, and based on objective criteria, not leading to profiling based on sensitive personal data or protected characteristics (e.g., "race", religion, or ethnicity); and individuals must have an effective mechanism to challenge their inclusion on such a watchlist.[36] Flawed or outdated watchlists, coupled with inadequate oversight, risk false positives and unjustified restrictions on freedom of movement.

26. It is also important to understand the context in which the PNR data processing are operated and potential implications, especially in the context of border management. PNR data reveal passengers' travel patterns and given the extensive information being collected, may also reveal sensitive data, such as ethnic origin, political opinion, religion or belief, or information concerning health or sexual life,[37] which might put people at risk of discrimination or other human rights abuses, even if the PNR Directive provides that such sensitive data may not be processed.[38] The automated processing of PNR data has the potential to reinforce discriminatory practices by associating personal traits with specific risks. Advance sharing of PNR data could also lead to restrictions on freedom of movement or may prevent people from effectively seeking asylum. PNR data enable public authorities to track persons who allegedly pose a risk to a country's security – based on the automated processing of their data. At the same time, different authorities are involved (e.g., law enforcement, border control authorities, and customs authorities) in accessing and processing the data. There is thus a greater risk of data misuse. An oversight body should have a strong mandate to exercise its responsibilities and be provided the competencies and powers to ensure compliance with human rights. The automated processing of PNR data may trigger further risk due to the lack of transparency and understanding surrounding automated systems.

27. Until 28 January 2025, the collection, processing and sharing of API data was regulated by the Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (hereinafter the "EU API Directive").[39] This Directive imposed obligations on air carriers to transmit, upon request, API data to the EU Member State of destination prior to the flight's take-off. This concerns inbound flights from a third country and aims to improve border control. On 28 January 2025, two new Regulations entered into force, namely (i) on the collection and transfer of API for

34 Article 2 (3) of the ICCPR (read together with UN Human Rights Committee, *General Comment No. 31*, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004)); and Article 13 of the ECHR (and relevant caselaw of the ECtHR: see Caselaw Guide on Article 13 of the ECHR as of February 2025, especially paras. 32-55).

35 For detailed discussion, see: D. Lowe, The European Union's Passenger Name Record Data Directive 2016/681: Is it fit for purpose? International Criminal Law Review 17 (1), 2017, p. 27; E. Brouwer, The EU Passenger Name Record (PNR) System and Human Rights: Transferring Passenger Data or Passenger Freedom?, 2009, p. 26-28.

36 For detailed discussion, see: Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, ODIHR Expert Consultation Meeting on Human Rights Challenges related to Information gathering and sharing and new Technologies in Border Management in the Counter-Terrorism and freedom of Movement, 15 June 2020, p. 3.

37 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), Article 6.

38 See EU PNR Directive 2016/681, Article 13. See also ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021), p. 13.

39 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004L0082>.

facilitating external border checks[40] (hereinafter "new EU API Regulation 2025/12 for border checks") and (ii) on the collection and transfer of advance passenger information (API) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime[41] (hereinafter "new EU API Regulation 2025/13 on terrorist offences and serious crimes") – or together referred to as "new EU API Regulations". These new regulations aim to introduce uniform requirements for the collection of API data by carriers, increase quality of API data, the collection of data by air carriers using automated means, mandatory transfer of data to Member States and increase the efficient transfer of data by air carriers to Member States, while aiming to ensure full compliance with EU data protection rules.[42] It is also clarified that the rules of the EU PNR Directive apply in respect of matters not specifically covered by new EU API Regulation 2025/13 on terrorist offences and serious crimes, especially regarding the rules on the subsequent processing of the API data received by the PIUs, exchange of information between Member States, conditions of access by the EU Agency for Law Enforcement Cooperation (Europol), transfers to third countries, retention and depersonalisation, as well as the protection of personal data.[43]

1.2. Data Protection and Right to Privacy

28. Human rights and fundamental freedoms are often curtailed for the presumed benefit of security. While human rights and security issues are sometimes conceptualised in an inverse relation to each other – i.e., in order to increase security one must reduce human rights, OSCE human dimension commitments and the UN approach underline that effective security measures and the protection of human rights are not conflicting but mutually reinforcing.[44] As such, respect for human rights and fundamental freedoms for all, democracy and the rule of law is at the core of the OSCE's comprehensive concept of security[45] and should constitute the fundamental basis of any security sector reform.[46]

29. The OSCE participating States have acknowledged[47] the importance of the "*human security*" approach which places the rights and security needs of individuals at the heart of the security functions. This approach recognizes that the primary aim of security sector institutions is to adequately and effectively provide services to all individuals in the community, regardless of their national or ethnic origin, political or other opinion, sex, gender identity or sexual orientation, religion or belief or any other status.[48] Security sector, including law enforcement and border management, is subject to the same standards of good governance as any other public sector, and is to provide security in an

40 Regulation (EU) 2025/12 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for enhancing and facilitating external border checks, amending Regulations (EU) 2018/1726 and (EU) 2019/817, and repealing Council Directive 2004/82/EC.

41 Regulation (EU) 2025/13 of the European Parliament and of the Council of 19 December 2024 on the collection and transfer of advance passenger information for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, and amending Regulation (EU) 2019/818.

42 <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1262>.

43 See new EU API Regulation 2025/13 on terrorist offences and serious crimes, Recital 5.

44 ODIHR, Background Paper on Addressing Transnational Threats and Challenges in the OSCE Region: the Human Dimension (2012). See also UN General Assembly, 15 September 2005, A/60/L.1, par 72; and UN Secretary- General, Kofi Annan, Statement to the Security Council on 18 January 2002.

45 OSCE, Istanbul Charter for European Security (1999), par 19.

46 See OSCE, Charter on Preventing and Combating Terrorism, 10th Ministerial Council Meeting, Porto 2002, pars 5-7; and OSCE Consolidated Framework for the Fight against Terrorism, adopted by Decision no. 1063 of the Permanent Council, at its 934th Plenary Meeting on 7 December 2012 (PC.DEC/1063). See also UN, Global Counter-Terrorism Strategy and Plan of Action (2006), Pillar IV; and OSCE Ministerial Statement supporting the UN Global Counter-Terrorism Strategy (MC.DOC/3/07, 30 November 2007). See also the Joint Statement of the UN High Commissioner for Human Rights, the Secretary General of the Council of Europe and ODIHR Director (29 November 2001).

47 OSCE, Strategy to Address Threats to Security and Stability in the 21st Century, Maastricht, 2003.

48 See e.g., Geneva Centre for Security Sector Governance (DCAF), ODIHR and UN Women, A Security Sector Governance Approach to Women, Peace and Security: Policy Brief (2019), page 2; and ODIHR, Background Paper on Addressing Transnational Threats and Challenges in the OSCE Region: the Human Dimension (2012), page 2.

accountable and effective way, within a framework of democratic civilian control, rule of law and respect for human rights, including gender equality.[49]

30. In the context of border management and data collection, fundamental human rights come into play. It is noteworthy that the UNSC Resolution 2396 calls for the collection, processing and analysis of API and PNR data in line with domestic law and international obligations, and with full respect for human rights and fundamental freedoms.[50] The resolution restricts the use of PNR data to the prevention, detection and investigation of terrorist offences.[51] It can thus be inferred that states, in establishing the legal framework regulating API and PNR data, are bound by their commitments under international law to respect and protect fundamental human rights.

1.2.1 Right to Privacy

31. Without the effective enjoyment of the right to privacy, the full enjoyment of a broad range of other rights is endangered. The protection of personal data is intrinsically tied to the right to privacy, and is particularly relevant in the context of data processing for border management purposes, and especially in the context of counter-terrorism.

32. The right to respect for private and family life is enshrined in key international and regional instruments, including Article 17 of the International Covenant on Civil and Political Rights[52] (ICCPR), Article 8 of the European Convention on Human Rights and Fundamental Freedoms[53] (ECHR) and Article 7 of the EU Charter of Fundamental Rights.

33. As noted by the UN Special Rapporteur on the Right to Privacy, *"[i]t is necessary for States to establish a system to safeguard the right to personal data protection so that data subjects are aware of the processing to which their personal data are subjected, can exercise proper control over their data and, in the event of a violation, can opt for a remedy with a view to the reparation or restitution of the right or compensation for the damage caused, as the case may be… In the digital age, not only must States respect and refrain from violating the rights to privacy and data protection, but their obligations also include positive measures to promote the effective enjoyment of these rights*."[54] In the area of API/PNR data collection and sharing, there is an interaction of authorities with private sector actors, namely airline companies, which warrants particular care in discharging existing duties in compliance with respect for privacy rights. In this regard, it is noted that in the OSCE Ministerial Council Decision No. 6/16, OSCE participating States committed to establish API systems in accordance with data protection and privacy standards.

34. Article 7 of the EU Fundamental Charter also protects the right to privacy, which corresponds to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter "the ECHR") with the meaning and scope of this right being the same. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR. Interference with the right to respect for private life is only acceptable if it complies with the strict requirements of Article 8 (2) ECHR, meaning that such interference must be "in

49 OSCE Secretary General, Report on the OSCE Approach to Security Sector Governance and Reform (SSG/R) (2019), page 2.
50 UNSC, S/RES/2396 (2017),, paras. 11-13.
51 UNSC, S/RES/2396 (2017), paras. 11-13.
52 *UN International Covenant on Civil and Political Rights* (ICCPR), adopted by the UN General Assembly by resolution 2200A (XXI) of 16 December 1966. Ukraine deposited its instrument of ratification of the ICCPR on 12 November 1973. Article 17 states that "*no one may be subjected to arbitrary or unlawful interference with their privacy, home or correspondence, nor to unlawful attacks on their honour and reputation*".
53 Council of Europe (CoE), *Convention for the Protection of Human Rights and Fundamental Freedoms*, entered into force on 3 September 1953. Ukraine deposited its instrument of ratification of the ECHR on 11 September 1997.
54 UNGA Human Rights Council, A/HRC/55/46, Report of the Special Rapporteur on the right to privacy: Legal safeguards for personal data protection and privacy in the digital age, 18 January 2024, paras. 12-13.

accordance with the law", must pursue a "legitimate aim" (these aims are the protection of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others) and must be "necessary in a democratic society" and strictly proportionate to the aim pursued.

35. In the EU, data protection is a right in and of itself which is reflected in Article 8 of the EU Charter of Fundamental Rights and Article 16 of the Treaty of the Functioning of the European Union (hereinafter "TFEU"). The CJEU observed that the collection, processing, storing and transfer of API/PNR data – as required by Security Council resolutions 2396 (2017) and Security Council resolutions 2482 (2019)[55]– constitute *per se* a serious interference with the right to privacy.[56]

36. Interferences with the right to respect for private and family life protected inter alia by Article 17 of the ICCPR, Article 8 of the ECHR and Article 7 of the EU Charter of Fundamental Rights may, however, be justified provided they are based on law, necessary and proportionate to pursue a legitimate aim.[57] In addition, the restriction must be non-discriminatory (Articles 2 and 26 of the ICCPR, Article 14 of the ECHR and Protocol 12 to the ECHR[58] and Article 21 of the EU Charter of Fundamental Rights).

37. The requirement that the interference be based in law not only requires that the restriction should have an explicit basis in domestic law, but also refers to the quality of the law in question, which should be clear, foreseeable, and adequately accessible.[59] As such the said legislation must be sufficiently clear and precise to enable individuals to act in accordance with the law, while demarcating clearly the scope of discretion for public authorities and providing a reasonable indication as to how these provisions will be interpreted and applied.[60] Proportionality requires that the chosen measure must be appropriate, least intrusive and proportionate *stricto sensu* to achieve the pursued aim. Accordingly, the collection, processing, storing and transfer of API/PNR data must be appropriate and proportional to the purpose of combatting terrorism or serious crime offenses. The law needs to authorize the collection, processing, storing and transfer of API/PNR data by competent authorities; have a purpose limitation of API/PNR data collection, processing, storing and transfer to narrowly defined offenses of (strictly and precisely defined) terrorism[61] and serious crime offenses; ensure that the collection of personal information is limited to what is directly relevant and necessary to accomplish a specified purpose; ensure the accuracy, confidentiality and integrity of the data; regulate competencies to avoid the abuse of API/PNR data, and lastly include protections of data subject rights and ensure access to effective remedies in case of violation.[62]

---

55 UNSC, S/RES/2396 (2017),, para. 12; and UNSC, S/Res/2482 (2019), para. 15.

56 See CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 111.

57 Article 8(2) of the ECHR provides: "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others". See also CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 113.

58 Ukraine ratified the Protocol no. 12 to the ECHR on 27 March 2006 and it entered into force on 1 July 2006.

59 See e.g., UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation; see also ECtHR, *Silver and Others v. the United Kingdom*, no. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, 25 March 1983, para. 87.

60 See, for example, ECtHR, *Lebois v. Bulgaria*, no. 67482/14, 19 October 2017, paras. 66-67. See also e.g., Venice Commission, Rule of Law Checklist, CDL-AD(2016)007, para. 58. In addition, see ECtHR, *The Sunday Times v. the United Kingdom (No. 1)*, no. 6538/74, where the Court ruled that "*the law must be formulated with sufficient precision to enable the citizen to regulate his conduct," by being able to foresee what is reasonable and what type of consequences an action may cause*."

61 On the definition of "terrorism", see *ODIHR Note on the Proposed Revision of the Definition of Terrorist Offences in Article 1 of the Council of Europe Convention on the Prevention of Terrorism* (2023). For a proposed model definition of terrorism based on those criteria see UN Special Rapporteur on counter-terrorism, Report to the UN Human Rights Council ("Ten areas of best practices in countering terrorism"), UN Doc. A/ HRC/16/51, 22 December 2010, para. 28.

62 See also: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 141-119-140.

1.2.2 Right to Data Protection

38. The right to data protection is not a stand-alone right under the ICCPR. At the same time, the UN Human Rights Committee has clarified that Article 17 of the ICCPR also requires that "*every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination*."[63] Two UN resolutions adopted in 2016 and 2017 are also of relevance as these refer to the responsibility of the private sector to respect human rights. The resolutions call upon companies to inform users about the collection, use, sharing and retention of personal data and to establish transparent processing policies.[64] According to the UN Special Rapporteur on the right to privacy "*[p]rocessing of personal data must be carried out respectfully and in accordance with a series of principles and requirements, thus ensuring that it is done properly while guaranteeing privacy and the unhindered development of personality, among other rights…. To achieve this goal, data subjects must be able to exercise control over their personal information, which is why data protection and privacy laws grant them a number of rights*."[65] Some of these rights are of particular relevance in the context of API/PNR data collection and processing as will be discussed later.

39. The right to personal data protection is similarly not a stand-alone right in the ECHR, but the ECtHR has acknowledged that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, home and correspondence, as guaranteed by Article 8 of the Convention.[66] In its judgments, the ECtHR relies on the right to respect privacy with regard to the automatic processing of personal data as laid out in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)[67] and the amending Protocol[68] thereto – not yet ratified by Ukraine (also known as the modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, hereinafter referred to as "modernized Convention 108"). Modernized Convention 108 provides binding commitments in the field of data protection and is of global dimension and has a horizontal scope of application, thus applying to both public and private sector data processing.

40. The modernized Convention 108 applies to all data processing carried out by both the private and public sectors, including data processing by the judiciary and law enforcement authorities. Personal data is defined as "*any information relating to an identified or identifiable individual*". Such data cover not only information directly identifying the "data subject" (such as a name and surname) but also any element indirectly identifying a person (such as an internet protocol or "IP" address). Under Article 2 of Convention 108, "data processing" includes "*any operation or set of operations performed on personal data, such as the collection, storage, preservation,*

63 See e.g., UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, para. 10.

64 UN, General Assembly, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/ Rev.1, New York, 16 November 2016; UN, Human Rights Council, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22 March 2017.

65 UN, Report of the Special Rapporteur on the right to privacy, Legal safeguards for personal data protection and privacy in the digital age, A/HRC/55/46, paras 22-23.

66 European Court of Human Rights, Guide on case-law of the Convention – Data protection, 31 August 2024 (latest update), para 3.

67 Council of Europe, Convention for the protection of individuals with regard to the processing of personal data, 28 January 1981. Ratified by Ukraine on 6 July 2010.

68 Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Ukraine has not signed nor ratified this Protocol.

alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data". It aims to protect data subjects against abuses that may result from the processing of personal data, and regulates the transborder sharing of personal data. Under Article 6 of modernized Convention 108, personal data revealing "racial" origin, political opinions, religious or other beliefs, and information on an individual's health or sex life, or on any criminal convictions, cannot be automatically processed unless domestic law provides for appropriate safeguards *complementing those of Convention 108*, and which shall "*guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination*" (new Article 6(1) and (2) of the modernized Convention 108). Information falling within these categories, described as "sensitive", warrant a heightened degree of protection and additional safeguards[69] and the automatic processing of such sensitive data "*shall only be allowed where appropriate safeguards are enshrined in law"*..

41. To assess if a certain measure meets the condition of being "*necessary in a democratic society*", the ECtHR examines whether the measure complies with the requirements listed in Article 5 of Convention 108. Thus, it reviews whether personal data undergoing automatic processing was obtained and processed fairly and lawfully. To assess if the interference had a legitimate aim, it analyses whether the requirement that personal data undergoing automatic processing must have been collected for explicit, specified and legitimate purposes, has or has not been met. The ECtHR examines whether, in particular, the requirements to minimise the amount of data collected, to ensure that they are accurate, adequate, relevant and not excessive in relation to the purposes for which they are processed, to limit the duration of their storage, to use them for the purposes for which those data have been collected and to ensure transparency in data processing have been met.[70]

42. Another key principle is that the sharing of personal data between parties to the Convention 108 is guaranteed, though that restrictions on sharing information can be introduced where the receiving state's regulations does not provide equivalent protection to the sending state. Convention 108 also regulates the mandatory establishment of national data protection supervisory authorities, amongst others.

43. In the EU, the right to data protection is considered a fundamental right distinct from the right to privacy. Article 8 of the EU Charter of Fundamental Rights not only affirms the right to data protection but also outlines the fundamental principles tied to it. It specifies that data processing must be conducted fairly, for clear purposes, and based on either the individual's consent or a legitimate legal basis. Furthermore, individuals are entitled to

69 The Protocol (CETS: 223) amending the Convention 108 (or modernized Convention 108), though not yet signed nor ratified by Ukraine, specifies that the automatic processing of such sensitive data "*shall only be allowed where appropriate safeguards are enshrined in law, complementing those of [the] Convention*", which shall "*guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination*" (proposed new Article 6(1) and (2) of the Convention). The Explanatory Report to the Protocol 223 further provides examples of the types of additional safeguards that could be considered alone or in combination regarding the handling of such sensitive data, including the data subject's explicit consent, a law covering the intended purpose and means of the processing or indicating the exceptional cases where processing such data would be permitted, a professional secrecy obligation, measures following a risk analysis (risk assessment prior to processing should assess whether data are protected against unauthorised access, modification and removal/ destruction and should seek to embed high standards of security throughout the processing; such an assessment should be informed by considerations of necessity and proportionality, and the fundamental data protection principles across the range of risks including physical accessibility, networked access to devices and data, and the backup and archiving of data; see Convention 108, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data by and for Political Campaigns* (2021), para. 4.3.5); a particular and qualified organisational or technical security measure; see *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, 10 October 2018, para. 56.

70 European Court of Human Rights, Guide on case-law of the Convention – Data protection, 31 August 2024 (latest update), para. 108.

access their personal data and request corrections, with compliance being monitored by an independent authority.[71]

44. The General Data Protection Regulation (hereinafter "GDPR")[72] is a key data protection instrument in the EU. It provides data protection rights in all areas, except law enforcement, which is governed by the Law Enforcement Directive 2016/680 (hereinafter "LED").[73] With respect to PNR information specifically, data must be transferred or processed in accordance with the GDPR (see Article 21 (2) PNR Directive with reference to the predecessor of the GDPR, namely EU Directive 95/46/EC) unless there is a criminal justice (terrorism or serious crime) objective, in which case the LED rules apply.

45. Article 5 of the GDPR sets out the principles governing the processing of personal data. These principles include, lawfulness, fairness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; integrity and confidentiality. [74]

46. In Chapter III of the GDPR, the rights of the data subject are laid out, which include access to and transparency of information (Articles 13 and 15 GDPR). Therefore, every data subject has the right to information about any data controller's processing of his or her personal data, subject to limited exemption. Other rights of data subjects, especially relevant to API/PNR data processing, include the right of access to their own data and to obtain certain information about the processing; to have data rectified by the controller processing their data, if the data are inaccurate (Article 16 GDPR); the right to have the controller erase their data, as appropriate, if the controller is processing their data illegally (Article 17 GDPR); the right to temporarily restrict processing and have their data ported to another controller under certain conditions; the right to object to processing on grounds relating to their particular situation and the use of their data for direct marketing purposes (Article 21 GDPR). Article 25 GDPR establishes the idea of data protection "by design and by default". This requires that controllers put in place appropriate technical and organisational measures that are designed to implement data protection principles. This entails that when programming, designing and conceptualizing systems and programs, as well as when acquiring systems and services from third parties, the controller has to ensure that data protection is taken into account and that the principles of the GDPR are properly integrated into the processing activity. A Data Protection Impact Assessment (DPIA) helps identify when a certain processing operation (or a set of operations with

71 EU Fundamental Rights Agency, Council of Europe and European Data Protection Supervisor, Handbook on European Data Protection Law – 2018 edition, p. 19.

72 Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR").

73 EU 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, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, OJ L 119, 4 May 2016.

74 The lawfulness principle is detailed in Article 6 (1) which requires that any processing operation must be based on at least one of the six legal bases in the exhaustive list provided (i.e., the legal bases requirement is met when consent from the person concerned is obtained; data processing is necessary for the performance of a contract; data processing is necessary because there is a legal obligation to do so; data processing is necessary for the protection of vital interests; data processing is necessary for the performance of a task carried out in the public interest / in the exercise of official authority; or data processing is necessary for representing legitimate interests). The meaning of the principle of transparency could be derived from Recital 39 GDPR which states that, "it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed"; data subjects should be "made aware of risks, rules, safeguards, and rights in relation to the processing... and how to exercise their rights"; all information communicated should be "accessible and easy to understand" and in "clear and plain language". The principle of purpose limitation, which is also enshrined in Article 8 (2) of the EU Charter of Fundamental Rights, ensures that personal data is only used for the stated and specified purpose(s); purpose limitation should ensure that controllers do not engage in further processing of the collected data when such processing exceeds the original aim or is incompatible with the specified purpose. The data minimisation principle is essentially a proportionality principle as any interference with the fundamental right to data protection must be proportionate and any processing of personal data must be necessary. Article 5 (1) (e) of the GDPR requires the controller to limit the period of collection of personal data to what is strictly necessary for the purpose. Article 5 (1) (d) requires that personal data must be accurate and, where necessary, kept up to date, and that all reasonable steps be taken to delete or rectify inaccurate data promptly. The principle of storage limitation requires that data processing is limited by time (recital 39 of the GDPR provides that "[i]n order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review"). The principle of confidentiality and integrity is detailed in Article 32 of the GDPR.

similar characteristics) presents a high risk to the rights and freedoms of natural persons (Article 35). Data subjects also have the right to complain to the supervisory authority and have the right to an effective judicial remedy. A key right for data subjects is not to be subject to decisions based solely on automated processing, including profiling, that have legal effects or that significantly affect him or her. Other rights include, obtaining human intervention on the part of the controller and expressing their point of view and contest a decision based on automated processing. The ECtHR also recognizes some of these rights through its case-law.[75]

47. The CJEU dealt with the issue of data protection rules that are applicable to automated PNR data processing in the case of *Ligue des droits humains*.[76] As noted above the EU PNR Directive authorizes the sharing of PNR data by airline companies with state authorities (law enforcement), exclusively for the purposes of the fight against terrorism and other forms of serious crime (Article 1(2) EU PNR Directive).

48. The CJEU ruled that the GDPR applies to the processing of personal data under national laws that implement the API Directive and the PNR Directive, covering both private operators and public authorities. However, it does not apply to data processing carried out by the PIUs, or public authorities competent for the purposes of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Additionally, PNR data collection and transfers from private sector entities to relevant state authorities, such as PIUs, must comply with the GDPR.[77] Any exceptions, such as those specified in Article 23(1)(f) of the GDPR (which covers transfers for the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, including safeguarding public security), must be interpreted in line with the right to privacy (Article 7) and personal data protection (Article 8) as guaranteed in the EU Charter of Fundamental Rights. Moreover, PIUs and other law enforcement bodies under the PNR Directive must handle the transferred personal data according to GDPR standards, unless the processing is linked to criminal justice objectives (such as terrorism or serious crime), in which case the LED rules take precedence. The processing of personal data by PIUs is driven by the specific requests from the competent authorities. Regarding the processing of API data, the CJEU's decision indicates that the LED does not apply. Since the primary purpose of API data collection is for border control, all operations related to the processing of this data must be governed by the GDPR. The LED only becomes relevant when API data is used for law enforcement purposes as defined in national legislation (Article 6(1) of the API Directive).

49. Under Article 47 of the EU Charter of Fundamental Rights**,** individuals have the right to an effective remedy if their data protection rights are violated. This means that individuals can challenge decisions made by data controllers and seek redress, including compensation for damages.

50. According to the UN Special Rapporteur on the Right to Privacy several data protection rights can be derived from various international and regional instruments. These rights include, the right to information, right of access, right to rectification, right to update information in digital media, right to deletion, right to be forgotten, right to restriction of processing, right to data portability, right to object, right not to be subject to a decision based on automated processing, including profiling, and right to a digital will.[78] The UN

75 European Court of Human Rights, Guide on case-law of the Convention – Data protection, 31 August 2004 (latest update), Chapter II.B.

76 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022.

77 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 83-84.

78 UN, A/HRC/55/46, Report of the Special Rapporteur on the Right to Privacy - Legal safeguards for personal data protection and privacy in the digital age, 18 January 2024.

Special Rapporteur also developed a set of guiding principles, derived from the modernized Convention 108 and General Assembly resolution 45/95,[79] in addition to the GDPR, which include the principles of legality, lawfulness and legitimacy, consent, transparency, purpose, fairness, proportionality, minimization, quality, responsibility and security.[80]

1.2.3 Potential Impact on Other Human Rights and Fundamental Freedoms

51. The gathering, processing, and sharing of personal data contained in API and PNR datasets, which may impact decision-making at international borders, could also result in other human rights violations.[81] Wrong or mismatched API or PNR data entries might impact an individual's right to freedom of movement and other rights. Article 12 of the ICCPR guarantees everyone's right to leave any country, including his/her own, and the right to enter one's own country.[82] While the entry of a non-national to the territory of a State may be subject to restrictions, any restrictions must be compliant with international human rights obligations, and take account of other rights such as non-discrimination, prohibition of cruel, inhuman or degrading treatment and respect for family life.

52. Depending on how the API/PNR data influence potential decisions taken in border management and security, it can also directly and indirectly affect the rights of individuals in specific need of protection, such as refugees and asylum-seekers, children and victims of trafficking. The principle of best interest of the child should be respected (see Article 3 of the Convention on the Rights of the Child). The use of PNR as an immigration control measure should be avoided. The right to seek and enjoy asylum is enshrined in Article 14 of the Universal Declaration of Human Rights (UDHR) and further developed in the 1951 Refugee Convention and its Protocol.[83] The international protection framework of the Convention sets out the fundamental rights of refugees and related state obligations, including the prohibition of forcible return to a country where one's life or freedom would be threatened (non-refoulement).[84] States shall not return non-nationals to a country where there is a real risk of that person being subjected to torture or other cruel, inhuman or degrading treatment or punishment,[85] risks of violations to the rights to life[86] or to the integrity or freedom of the person,[87] flagrant violation with respect to arbitrary

79 Entitled "Guidelines for the regulation of computerized personal data files

80 UN, Note by the Secretary-General, A/77/196*, Right to Privacy - Report prepared by the Special Rapporteur on the right to privacy, 20 July 2022.

81 See e.g., ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context (2021).

82 The right to leave any country may be subject to certain restrictions but only as far as the restrictions are provided by law, are necessary, proportionate and non-discriminatory; regarding the right to return to one's own country, the ICCPR also underlined that the meaning of "own country" is broader than the concept "country of nationality" and embraces also non-nationals with special ties to the country, such as long-term residents; see UN Human Rights Committee, General Comment No. 27: Article 12 (Freedom of Movement), UN Doc. CCPR/C/21/Rev.1/Add.9, 2 November 1999, para. 20. See also the OSCE commitments on freedom of movement, Vienna 1989, para. 20.

83 The Convention relating to the Status of Refugees (1951), was adopted by the United Nations Conference of Plenipotentiaries on the Status of Refugees and Stateless Persons, held at Geneva from 2 to 25 July 1951. Ukraine acceded to the Convention on 10 June 2002.

84 Article 33 of the Convention relating to the Status of Refugees. The principle of non-refoulement is also enshrined in international human rights law, which prohibits the return of anyone to any country where he or she may be exposed to risks of torture or other serious human rights violations. The absolute prohibition of torture entails an absolute prohibition of refoulement to torture under all circumstances. For an overview see OHCHR "The Principle of non-refoulement under international human rights law".

85 See the UN Convention Against Torture and Cruel, Inhuman or Degrading Treatment or Punishment (adopted on 10 December 1984, entered into force on 26 June 1987, Ukraine ratified the UN CAT on 24 February 1987), 1465 UNTS 85, Article 3; International Convention for the Protection of All Persons from Enforced Disappearance (adopted on 20 December 2006, entered into force on 23 December 2010, Ukraine acceded to the CRPD on 14 August 2015), 2716 UNTS 3, Article 16; Articles 2(1) and 7 of the ICCPR (see *CCPR, General Comment no. 20 (1992)*, para. 9, which indicates that this obligation is reflected in Article 7 of the ICCPR, whilst *General Comment no. 31 (2004)*, UN Doc. CCPR/C/21/Rev.1/Add.13, para. 12, recognizes the non-refoulement principle in Article 2 of the ICCPR). See also e.g., para. 31 of 2018 CCPR *General Comment no. 36*.

86 See e.g., UN Special Rapporteur on Counter-Terrorism and Human Rights, *Annual Report: Ten areas of best practices in countering terrorism*, UN Doc. A/HRC/16/51, 22 December 2010, para. 38 and Practice 10.5; and UN Secretary General, *Report on the protection of human rights and fundamental freedoms while countering terrorism*, A/63/337, 28 August 2008, para. 45. See also OHCHR, *Technical Note on the Principle of Non-Refoulement under International Human Rights Law* (2018), page 1; and CCPR, *General Comment no. 31* (2004), para. 12.

87 *Ibid*. para. 45 (2008 UN Secretary General's Report); and page 1 (2018 OHCHR Technical Note on Non-Refoulement).

imprisonment,[88] enforced disappearance,[89] risk of manifestly unfair trial,[90] serious forms of sexual and gender-based violence,[91] prolonged solitary confinement[92] or other serious human rights violations[93]. In addition to their *non-refoulement* obligations under international refugee and human rights law, States Parties must also take into account the provisions of the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children of 2000 to the UN Convention against Transnational Organized Crime[94] (hereinafter "the UN Palermo Protocol"), in accordance with the saving clause in Article 14 (1) for victims of trafficking in persons.

2. BACKGROUND

53. As noted above, the Draft Law was developed as part of a comprehensive assessment of the transposition of European Union legal standards into the legislation of Ukraine.

54. Article 7 of the Law of Ukraine "On Combating Terrorism" authorizes the Antiterrorist Center at the Security Service of Ukraine to coordinate at the national level the implementation of the UN Security Council resolution on countering international terrorism, cooperation with special services, law enforcement bodies of foreign states and international organizations on countering terrorism and exchange of available passenger information on international flights.

55. For the purpose of implementation of the abovementioned regulation, the Security Service of Ukraine, together with other institutions of the security and defense sector, and international partners, including the OSCE's Support Program to Ukraine, has developed the Draft Law of Ukraine "On the Usage of Passenger Information for Combating Terrorism, Serious and Especially Serious Crimes".

3. COLLECTION, PROCESSING AND SHARING API/PNR DATA

3.1. Purpose Limitation

56. Article 2 of the Draft Law states the purpose of collecting API and PNR data. API data is collected to improve border control and combat "illegal migration",[95] whereas PNR is obtained for the purpose of combating international terrorism and other "serious" and

88 See e.g., European Court of Human Rights, *Othman (Abu Qatada) v. United Kingdom*,no. 8139/09, 17 January 2012, para. 233.

89 See Article 16 of the International Convention for the Protection of All Persons from Enforced Disappearance, adopted by the UN General Assembly by Resolution A/RES/61/177 of 20 December 2006 (which entered into force on 23 December 2010, Ukraine acceded to the Convention on 14 August 2015).

90 UN Secretary General, *Report on the protection of human rights and fundamental freedoms while countering terrorism*, A/63/337, 28 August 2008, para. 45; and OHCHR, *Technical Note on the Principle of Non-Refoulement under International Human Rights Law* (2018), p. 1. See also, European Court of Human Rights, *Othman (Abu Qatada) v. United Kingdom* (Application no. 8139/09, 17 January 2012), paras. 258-262.

91 *Ibid.* page 1 (2018 OHCHR *Technical Note on Non-Refoulement*). See also e.g., UN CAT Committee, *Njamba and Balikosa v. Sweden*, Communication no. 322/2007, 3 June 2010, para. 9.5; and CEDAW Committee, *General Recommendation no. 32* (2014), para. 23.

92 UN Secretary General, *Report on the protection of human rights and fundamental freedoms while countering terrorism*, A/63/337, 28 August 2008, paras. 39 and 42; and *ibid*. page 1 (2018 OHCHR Technical Note on Non-Refoulement). See also e.g., CCPR, *General Comment no. 20* (1994), para. 6.

93 UN Human Rights Committee, *Kindler v. Canada*, Communication no. 470/1991, at para. 13.2: "*If a State party extradites a person within its jurisdiction in circumstances such that as a result there is a real risk that his or her rights under the Covenant will be violated in another jurisdiction, the State party itself may be in violation of the Covenant*"; and *ARJ v. Australia*, UN Doc. CCPR/C/60/D/692/1996, 11 August 1997, para. 6.9, referring to risk of any serious human rights violation triggering non-refoulement obligations.

94 *Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children*, (hereinafter the "Palermo Protocol") supplementing the United Nations Convention against Transnational Organized Crime. Protocol adopted by GA resolution 55/25 of 15 November 2000.

95 For the purpose of this Opinion, the term "illegal migration" is used in quotation marks to refer to the terminology used in EU Directives and Regulations, although noting that the use of the word "illegal" when referring to migrants negatively impacts the general public's perception of migrants, risks legitimizing policies that are not in line with human rights guarantees and contributing to xenophobia and discrimination (see e.g., *CoE, Expert Council on NGO Laws, Using Criminal Law to Restrict the Work of NGOs Supporting Refugees and Other Migrants in CoE Member States* (2019), para. 131 (iii)).

"especially serious" crimes. The new EU API Regulation 2025/13 aims to establish clear, harmonised and effective rules at Union level on the collection and transfer of API data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes, while making it clear that the Regulation does not permit the collection or transfer of API data on intra-EU flights for the purpose of combating "illegal immigration".[96]

57. The use of API data contemplated in the Draft Law is generally in line with international standards (border control and countering irregular migration),[97] although to align with the new EU API Regulation 2025/13, the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes would need to be added. It would then also be made clear that the collection or transfer of API data on intra-EU flights for the purpose of combating "illegal immigration is prohibited.

58. At the same time, the purpose of processing PNR data envisaged in the Draft Law is drafted more broadly than what is recommended by international standards. According to UNSC Resolutions referred above, PNR data should only be processed for countering and investigating *terrorist* offences. The Standards of Annex 9 of the Chicago Convention and the EU PNR Directive expanded this scope to also include "serious crimes", with the latter specifically listing the serious crimes for which PNR can be processed.[98] The new EU API Regulation 2025/13 cross-refers to the list of serious crimes of Annex 2 of the EU PNR Directive. The Draft Law specifically also foresees the processing of PNR data to combat the "*movement of persons involved in terrorist activities*" (Article 2). This formulation is rather problematic and vague enough to increase the risk of having PNR data being used as a general immigration control measure, which would not be compliant with international standards. **It is recommended to align the purpose of the PNR data collection, namely for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes only, to prevent disproportionate data collection and it being used as a mass surveillance tool, exceeding the aims laid out in international standards.** Though going beyond the scope of this Opinion, it is also fundamental to ensure that the respective criminal offences are clearly defined in line with international human rights standards, while strictly circumscribing each of the constitutive elements of the said serious crimes, to avoid potential for arbitrary application and overreach of the law.[99]

59. Moreover, the CJEU, in its judgment in the case of *Ligue des droits humains* ruled that EU Member States should ensure that their national implementations of the PNR Directive are effectively limited to combating terrorist offences and serious crimes "*having an objective link, even if only an indirect one, with the carriage of passengers by air*".[100] It should not be applied to combat ordinary crime.[101] To address purpose limitation, the definitions of "serious and especially serious crimes" under Article 1 of the Draft Law should be clarified and narrowly drafted to meet the specificity requirements. It is noted that Article 3 (9) of the EU PNR Directive defines "serious crimes" as those mentioned in its Annex 2 and which are subject to a custodial sentence or detention for a maximum period of at least three years. While the Draft Law uses the

96 See new EU API Regulation 2025/13 on terrorist offences and serious crimes, Recitals 4 and 32.

97 In the Netherlands, the Royal Military and Border Police, which is tasked with border checks on individuals and combatting irregular migration, does not have access to PNR data. It only has access to API data. This is in line with the EU PNR Directive which allows for the processing of PNR data only for preventing, detecting, investigating prosecuting terrorist offences and serious crimes. International Experience and Good Practices in API/PNR Andrew Priestley, Marc Beauvais, 2021 p. 26.

98 EU PNR Directive (2016/681), Annex 2 lists the serious crimes.

99 On the definition of "terrorism", see *ODIHR Note on the Proposed Revision of the Definition of Terrorist Offences in Article 1 of the Council of Europe Convention on the Prevention of Terrorism* (2023).

100 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para 157.

101 Court of Justice of the European Union, Press Release No: 105/22 https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-06/cp220105en.pdf

same list of "serious crimes" and specifies that this definition involves crimes with punishment of imprisonment for "more than five years (serious) and more than ten years (especially serious)", it does not ensure that the scope is limited to those crimes "*having an objective link, even if only an indirect one, with the carriage of passengers by air*". In order to establish an objective link, there need to be objective criteria to set up a connection between PNR data and combating serious crime and terrorist offences. While a direct link relates to "offences targeting the carriage of passengers by air as well as offences committed during or through travel by air",[102] an indirect link covers all situations where there is no direct link but where serious crime and terrorist offences may be prevented, detected, investigated or prosecuted with the help of processing PNR data of selected connections or flights, i.e., in particular, when air transport is used as a means of preparing such offences or evading criminal prosecution.[103] **It is therefore recommended to reduce the scope of the criminal offences for which the processing of PNR data** (and API data in light of the new EU API Regulation 2025/13) **may happen according to the Draft Law reflecting the direct or indirect link with the carriage of passengers by air.**

60. Finally, it is also important to address the issue of personal data of third parties that may be collected. Such data only falls within the scope of the PNR Directive insofar as it relates directly to the flight operated and the passenger concerned, i.e., those related to the payment information and billing address of a person that purchased the ticket on behalf of the passenger insofar as it directly relates to the flight, and the contact details of a parent or guardian who is dropping off or picking up a passenger who is an unaccompanied minor.[104] Otherwise, **all other third-party personal data must be deleted immediately and permanently by the PIU upon receipt. It is recommended to supplement the Draft Law in this respect**.

RECOMMENDATION A.1

It is recommended to align the purpose of the PNR data collection, namely for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crimes only, to prevent disproportionate data collection and it being used as a mass surveillance tool, exceeding the aims laid out in international standards.

RECOMMENDATION A.2

To reflect in the Draft Law to delete other third-party personal data immediately and permanently by the PIU upon receipt.

3.2. Collection and Processing of API/PNR Data

61. A passenger data single window is a facility that allows parties involved in passenger transport by air to lodge standardized passenger information, such as API/PNR, through a single data entry point to fulfil all regulatory requirements relating to the entry and/or

102 See CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 155.

103 See European Data Protection Board (EDPB), *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, para. 9.

104 See European Data Protection Board (EDPB), *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, para. 5.

exit of passengers that may be imposed by various agencies of states. The single window concept places the onus on the authorities to manage the single window and to ensure that the participating authorities or agencies are either given access to the information or actually given the information by the managing authority. It eliminates the need for the traveller or transporter to submit the same data to several different border control agencies within the same state.

62. Article 5 of the Draft Law authorizes the centralized single window system to transmit API data to the National Center and PNR data to the National Contact Point (which is the Passenger Information Unit or "PIU" as referred to in Article 4 of the EU PNR Directive). The procedure for the operation of the single window is determined by several bodies, including state border protection body, the Antiterrorist Center at the Security Service and the central body in charge of civil aviation and use of airspace, in accordance with the procedure established by law. Whilst this approach appears to align with Standards 9.1 and 9.1.1 of Annex 9 to the Chicago Convention, such phrasing is open-ended, and does not require the necessary legal safeguards to be put in place, including that any procedure set up for the single window meets cybersecurity standards respecting passengers' right to privacy. **It is recommended to strengthen this provision by requiring compliance of the single window system with cybersecurity protection standards.**

63. Articles 8 and 13 of the Draft Law concern the collection of API and PNR data respectively. The components of the PNR data largely matches the data listed in the EU PNR Directive. The only differences between the two are that the Draft Law requests the reservation identification number whereas this is not listed in the EU PNR Directive. Instead, the EU PNR Directive requests the PNR record locator. Secondly, the Draft Law requires extensive information concerning ticket payment, yet it does not include billing address which is exclusively required by the EU PNR Directive. Articles 8 and 13 include data fields (e.g. payment details) which may be excessive in view of Annex 9 to the Chicago Convention, Standard 9.22, which mandates data minimization. At the same time it is noted that the CJEU addressed the question of whether the data fields of the EU PNR Directive meet the requirements of clarity and precision and it viewed the data fields collected through the PNR Directive as of sufficiently clear and precise nature overall. It noted that certain data fields (namely information related to billing/payment, frequent flyer programs but also 'general remarks') need to be interpreted in accordance with specific considerations set out in the judgement of *Ligues des droits humains.*[105] **It is nonetheless recommended to ensure that data collection is limited to what is strictly required for the purpose of preventing, detecting, investigating and prosecuting terrorism and serious crimes in line with the principle of data minimization and to provide an explicit stipulation about the duty to immediately and permanently delete data that is outside of the prescribed categories in the Draft Law.**

64. According to Article 6 (1) of the EU PNR Directive, airlines may collect certain information for their services (such as special food requests – halal meat, kosher food – or special health requests –insulin pump, oxygen tank etc.) which is 'sensitive data' that potentially reveals ethnic/"racial" origin, religion or health status and should therefore not be processed as part of the PNR data. **Such information should be immediately and permanently deleted and it is recommended to supplement the Draft Law in this respect.**[106]

---

[105] CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras 126-140.

106 International Experience and Good Practices in API/PNR Andrew Priestley, Marc Beauvais, 2021 p.39

RECOMMENDATION B.

To ensure that data collection is limited to what is strictly required for the purpose of preventing, detecting, investigating and prosecuting terrorism and serious crimes in line with the principle of data minimization and to provide an explicit stipulation about the duty to immediately and permanently delete data that is outside of the prescribed categories in the Draft Law, including any sensitive data.

3.3. Automated Processing

65. According to Article 18 of the Draft Law, the data entered into the National PNR Processing System shall be automatically compared with the relevant data of automated information and reference systems, registers and data banks, which are managed by state bodies or operators, to which the National Contact Point has access. The latter body is the "PIU as defined by the EU PNR Directive according to which the PIU is in charge of collecting PNR data from airlines, comparing PNR data against relevant law enforcement databases and processing them against pre-determined criteria, to identify persons potentially involved in a terrorist offence or serious crime, and disseminating PNR data to national competent authorities, Europol, and PIUs of other EU countries, either spontaneously or in response to duly reasoned requests. This is in line with the definition in Article 1 of the Draft Law. Article 18 also provides that the matches obtained as a result of the preliminary automated comparison are subject to mandatory individual verification by the National Contact Point staff. [107] It further clarifies that personal data is processed in compliance with the requirements of the Law of Ukraine "On Personal Data Protection".

66. It is important that the Draft Law includes additional and sufficient safeguards with respect to the automated processing of data. The EU PNR Directive requires that "…*the competent authorities shall not take any decision that produces an adverse legal effect on a person or significantly affects a person only by reason of the automated processing of PNR data*" and that such "*decisions shall not be taken on the basis of a person's race or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation*".[108] The CJEU has also specified that the automated processing when an advance assessment of PNR data is carried out must be limited and accompanied by several safeguards. Indeed, high error rates may result from automated systems which create false positives, thereby disproportionately affecting innocent passengers.[109]

67. Article 8 of EU Regulation 2025/13 and Article 21 of the EU Charter of Fundamental Rights require that the collection and processing of passenger data by air carriers and competent authorities shall not result in discrimination against persons on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or other

107 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 152. see also: EU PNR Directive (2016/681), Article 6 (5). The EU PNR Directive for example provides that EU Member States ensure that any positive match resulting from the automated processing of PNR data is individually reviewed by non-automated means to verify whether the competent authority needs to take action under national law.

108 EU PNR Directive (2016/681), Article 7(6).

109 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 106, 123-124.

belief, political opinion, membership of a national minority, property, birth, disability, age or sexual orientation.

68. Therefore, the non-automated review should aim to exclude any discriminatory results.[110] The Draft Law should also make it clear that the PIU shall not transfer the results of those automated processing operations to the competent authorities when they conclude, following that review, that they do not have anything capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime in respect of the persons identified by means of those automated processing operations or when they have reason to believe that those processing operations lead to discriminatory results.[111] States must ensure that the PIU establishes, in a clear and precise manner, objective review criteria enabling PIU agents in charge of individual review to verify, on the one hand, whether and to what extent a positive match concerns effectively an individual who may be involved in the terrorist offences or serious crime and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of the EU PNR Directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations and, in particular, the pre-determined criteria and databases used.[112] Where applicable, PIU should give preference to the result of the individual review conducted by non-automated means by the PIU over that obtained by automated processing.[113] It is also important to provide for "…*clear and precise rules capable of providing guidance and support for the analysis carried out by the agents in charge of the individual review, for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination*."[114] Finally, states are required to ensure that **the PIUs maintain documentation relating to all processing of PNR data carried out in connection with the advance assessment, including in the context of the individual review by non-automated means, for the purpose of verifying its lawfulness and for the purpose of self-monitoring**.[115]

69. ICAO standards also have concrete safeguards against automated processing of personal data.[116] These standards require that automated processing of PNR data should be based on objective, precise, specific criteria that effectively indicate the existence of a risk without leading to unlawful differentiation and that decisions that produce significant adverse actions affecting the legal interests of individuals are not based solely on the automated processing of PNR data.

70. **It is recommended that Article 18 of the Draft Law reflect the above-mentioned safeguards explicitly and require that any pre-established criteria against which PNR data are compared do not lead to unlawful differentiation and ensure that discriminatory results are excluded**. Moreover, **it is recommended that a safeguard clause concerning asylum applications is included in this provision** in line with the Preamble of the EU PNR Directive, which states that "*[t]he result of processing PNR*

110 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 203.

111 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 204.

112 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 206.

113 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 208.

114 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 205.

115 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 202-212.

116 ICAO Annex 9, Article 9.28.

data should in no circumstances be used by Member States as a ground to circumvent their international obligations under the Convention of 28 July 1951 relating to the Status of Refugees as amended by the Protocol of 31 January 1967, nor should it be used to deny asylum seekers safe and effective legal avenues into the territory of the Union to exercise their right to international protection".[117]

RECOMMENDATION C.

To reflect in Article 18 of the Draft Law that:

- The non-automated review should exclude any discriminatory results
- The PIU shall not transfer the results of those automated processing operations to the competent authorities when they conclude, following that review, that they do not have anything capable of giving rise, to the requisite legal standard, to a reasonable suspicion of involvement in terrorist offences or serious crime in respect of the persons identified by means of those automated processing operations or when they have reason to believe that those processing operations lead to discriminatory result
- The PIU establishes, in a clear and precise manner, objective review criteria enabling PIU agents in charge of individual review to verify, on the one hand, whether and to what extent a positive match concerns effectively an individual who may be involved in the terrorist offences or serious crime and must, therefore, be subject to further examination by the competent authorities referred to Article 7 of the EU PNR Directive, as well as, on the other hand, the non-discriminatory nature of automated processing operations and, in particular, the pre-determined criteria and databases used
- Any pre-established criteria against which PNR data are compared do not lead to unlawful differentiation and ensure that discriminatory results are excluded
- A safeguard clause concerning asylum applications is included in this provision

3.4. Data Sharing with Authorized Bodies

71. Article 19 regulates the sharing of API/PNR data with the "authorised bodies" in Ukraine. The Draft Law defines these bodies quite broadly (under Article 1), without naming any specific institutions. However, according to the EU PNR Directive, states should adopt a list of the competent authorities entitled to request or receive PNR data or the result of processing those data from the PIU in order to examine that information further or to take appropriate action for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.[118] **It is therefore advised that the Draft Law explicitly lists the authorized bodies either in the Draft Law, or as and annex to the Draft Law or refers to the relevant legislation which regulate these authorized bodies.**

117 EU PNR Directive, Preamble Para 21
118 EU PNR Directive Article 7 (1).

72. With respect to duly reasoned request based on sufficient grounds from the competent authorities to provide and process PNR data in specific cases for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime – as envisaged in Article 6 (2) (b) of the EU PNR Directive, the CJEU stated that "*it is essential that disclosure of PNR data for the purposes of subsequent assessment be, as a general rule, except in the event of duly justified urgency, subject to a prior review carried out either by a court or by an independent administrative authority*".[119] To prevent the unlimited use of the data for the purpose of law enforcement, this independence is indeed essential. As underlined by the European Data Protection Board (hereinafter "EDPB"), "*leaving the prior review to an independent officer or staff of a specific section within an administrative authority, that is not independent in itself, would in principle not be in line with what the CJEU Judgment envisaged in terms of independence. The same would apply to an independent officer or staff of a specific section within the authority involved in the conduct of the criminal investigation.*"[120] **The Draft Law should further elaborate the mechanisms of independent review prior to responding to duly reasoned requests from competent authorities for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.**

73. Article 16 (5) tasks the PNR Processing System with recording of all access to PNR data. However, this clause should be further elaborated. As per the EU PNR Directive, states shall keep records of at least the collection, consultation, disclosure and erasure (of PNR data). The records of consultation and disclosure should include, in particular, the purpose, date and time of such operations and, as far as possible, the identity of the person who consulted or disclosed the PNR data and the identity of recipients of those data. The records shall be used solely for the purposes of verification, of self-monitoring, of ensuring data integrity and data security or of auditing. The PIU shall make the records available, upon request, to the 'national supervisory authority'.[121] **Accordingly the Draft Law should reflect a more detailed stipulation of the information to be collected with respect to access to PNR data in paragraph 5 of Article 16.**

74. Article 11 (4) of the Draft Law makes a reference to registration of all cases of obtaining access to API data by the National API Processing System. Whilst it is a good practice to keep logs of all processing operations relating to API data, it should elaborate further on the manner of keeping of logs. As per the new EU API Regulation 2025/13 on terrorist offences and serious crimes, the logs shall cover date, time, place of transfer of API data.[122] Logs should not contain any personal data other than information to identify the staff member of the body in charge of API processing. The logs should only be used for ensuring the security and integrity of the API data and the lawfulness of the processing, and they should be accessible to national data protection supervisory authorities.[123]

119 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 223. See also EDPB, *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, paras. 25-26.

120 EDPB, *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, para. 24.

121 EU PNR Directive, Article 13 (6).

122 See new EU API Regulation 2025/13 on terrorist offences and serious crimes, Article 17.

123 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0729 Article 13

RECOMMENDATION D

To explicitly list the authorized bodies either in the Draft Law, or as and annex to the Draft Law or make a refence to the relevant legislation which regulate these authorized bodies and to elaborate the mechanisms of independent review prior to responding to duly reasoned request from competent authorities for the purposes of preventing, detecting, investigating and prosecuting terrorist offences or serious crime.

3.5. Data Retention

75. Articles 9 and 17 of the Draft Law concern retention of API and PNR data, respectively. According to Article 9, API data should be retained as temporary files, and the National Centre for API Data Processing on International Flights ("National API Processing Centre") must delete data within 24 hours after transmission. It also provides that air carriers must delete the data within 24 hours of arrival. These are in line with the existing EU API Directive. It should be noted that the new EU API Regulations extend these timelines from 24 to 48 hours.[124]

76. Article 17 of the Draft Law mandates the retention of PNR data for five years after its collection. After six months from the moment of collection by the National Contact Point certain data must be depersonalized. Article 17 also includes a clause allowing a deviation from the standard timelines as provided in Annex 9 to the Chicago Convention recommended practices 9.32 and 9.33, when required in the course of an investigation, prosecution or court proceeding.[125] The EU PNR Directive expands the abovementioned grounds by including prevention and detection of terrorist offences or serious crimes as well, stating that "*Member States shall ensure that the PNR data are deleted permanently upon expiry of the period referred to in paragraph 1. This obligation shall be without prejudice to cases where specific PNR data have been transferred to a competent authority and are used in the context of specific cases for the purposes of preventing, detecting, investigating or prosecuting terrorist offences or serious crime, in which case the retention of such data by the competent authority shall be regulated by national law"*.[126]

77. There is no consistent policy regarding the maximum retention period for API or PNR data across the OSCE region. The Consultative Committee to Convention 108 emphasized that data retention periods should be clearly defined and limited to what is strictly necessary for the intended purpose. While the Committee acknowledged that anonymizing passenger data after a certain period can reduce some risks associated with prolonged retention, it pointed out that such anonymized data can still allow for the identification of individuals. As a result, this data remains personal data and must adhere to appropriate retention limits to prevent long-term surveillance. Additionally, the collection of health data alongside other personal information could raise further human rights concerns for international travellers by air, land, and sea.[127]

124 Article 8 of the new EU API Regulation 2025/12 and Article 6 of the new EU API Regulation 2025/13 on terrorist offences and serious crimes.
125 ICAO Annex 9 – Article 9.32
126 EU PNR Directive Article 12 (4)
127 ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 2021, p. 14.

78. While Article 12 of the PNR Directive refers to a retention period of five years, the retention of PNR data pursuant to Article 12 cannot be justified in the absence of an objective connection between that retention and the objectives pursued by the PNR Directive.[128] The CJEU has held in its caselaw that the retention period of five years "…*read in conjunction with Articles 7 and 8 as well as Article 52(1) of the Charter of Fundamental Rights, must be interpreted as precluding national legislation […], applicable indiscriminately to all air passengers, including those for whom neither the advance assessment […] nor any verification carried out during the period of six months referred to in Article 12 (2) of the said directive nor any other circumstance have revealed the existence of objective material capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air*".[129] As underlined by the European Data Protection Board, it is thus "*precluded to set a general retention period going beyond the initial period of six months*" and after the initial period of six months, "*individual PNR data sets may only be processed if for the respective data sets there is objective material capable of establishing a connection with the objectives pursued by processing under the PNR Directive, and only as long as it is necessary and proportionate*".[130]

79. Therefore, **Article 17 of the Draft Law should be amended to provide for a general retention period of six months, which may be expanded to up to five years when there exists objective material capable of establishing a risk that relates to terrorist offences or serious crime having an objective direct or indirect link with the carriage of passengers by air – while retaining the above-mentioned exceptions. Moreover, a standard clause that the PNR data should be deleted after the retention period should also be included.**

3.6. International Co-operation

80. Article 24 of the Draft Law explicitly links data sharing to international treaties ratified by Ukraine. This emanates from Standard 9.25 of Annex 9 to the Chicago Convention. As noted above, under EU law, transfers of PNR data to third countries must ensure an equivalent level of data protection to that provided under EU law, be based on agreements or adequacy decisions under the GDPR framework and states must limit transfers to cases where the receiving state will use the data exclusively for combating terrorism or serious crime. Before transferring PNR data, it is also fundamental that an assessment be made of the recipient country's record on human rights and data protection, as well as of the legal safeguards and institutional controls and oversight that govern the authority receiving such data.[131] As noted above, there should also be a clear undertaking not to transfer such PNR data which is likely to be used for purposes that violate human rights. Data-sharing agreements with countries lacking robust personal data and human rights

128 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 299. See also EDPB, *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, para. 30.

129 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 299.

130 See EDPB, *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, para. 29.

131 See e.g., as a comparison, UN Special Rapporteur on the protection and promotion of human rights while countering terrorism, *Compilation of Good Practices on Legal and Institutional Frameworks and Measures that Ensure Respect for Human Rights by Intelligence Agencies while Countering Terrorism* (2010), Practice 33; see also ODIHR, *Guidelines on Addressing the Threats and Challenges of "Foreign Terrorist Fighters"* (2018), page 43.

protections or unclear safeguards contravene EU data protection standards[132] and international human rights obligations, more generally.

81. Where such adequate data protection standards and safeguards are lacking, this could prove to be an obstacle to information sharing between OSCE participating States. Sharing of PNR data across borders will only be lawful if the standards of privacy and data protection are safeguarded in both the sending and the receiving country. As noted in the ODIHR Policy Brief: Border Management and Human Rights, "…*sharing of data under such [in the absence of guarantees] circumstances not only undermines data protection standards but could also result in other human rights violations (e.g., undue restrictions on freedom of movement, discrimination, unlawful detention or inhuman and degrading treatment or punishment) where human rights protections are inadequate in the receiving country. This could put not only the individual traveller at risk but also their families or associates*."[133] Sharing of this data can put refugees and asylum seekers at particular risk, if as a result, they are prevented from leaving their or another country. Therefore, when developing and implementing API and PNR systems, states need to put in place effective human rights safeguards to protect individuals from being wrongfully placed under suspicion for involvement in terrorism or other crimes.

82. Before entering into agreements for sharing of API and PNR data, states must ascertain that privacy and data protection, as well as other human rights safeguards, are fully in place and respected in partner countries with which such information is sought to be shared.[134] These safeguards to ensure equivalent protection for data shared with third countries are not reflected in Article 24. It is therefore **recommended to supplement Article 24 of the Draft Law to provide that before entering into an API/PNR data sharing agreement, or sharing such data on an *ad hoc* basis, an assessment should be made of the counterpart's record on human rights and data protection, as well as of the legal safeguards and institutional controls that govern the recipient authority, to ensure that the third country meet equivalent protection standards. This agreement should also be re-assessed regularly or as warranted.**

RECOMMENDATION E.

To provide in Article 24 of the Draft Law that before entering into an API/PNR data sharing agreement, or sharing such data on an *ad hoc* basis, an assessment should be made of the counterpart's record on human rights and data protection, as well as of the legal safeguards and institutional controls that govern the recipient authority, to ensure that the third country meets equivalent protection standards. This agreement should also be re-assessed regularly or as warranted.

4. NON-DISCRIMINATION

83. PNR data contain detailed information that may reveal sensitive personal data, such as ethnicity, political opinions, religion, health, or sexual orientation, which could expose

132 For detailed discussion, see: CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 183-192; Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Response to Call for Input by OHCHR on Privacy in Digital Age, p. 6-8.

133 ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 2021, p. 15.

134 ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 2021, p. 15.

certain individuals to discrimination or human rights violations. Even when legislation prohibits the processing of sensitive data, there is still a risk that conclusions could be drawn indirectly, such as inferring someone's religious beliefs from meal preferences or political views from travel patterns. Sharing API or PNR data in advance could also lead to restrictions on the freedom of movement, particularly for political dissidents or asylum seekers.[135] Standard 9.30 of Annex 9 to the Chicago Convention provides that states shall not use PNR data revealing an individual's "racial" or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or data concerning their health, sexual life or sexual orientation, other than in exceptional and immediate circumstances to protect the vital interests of the data subject or of another natural person.

84. As noted, the EU PNR Directive obliges designated national security authorities, the PIUs, to automatically process PNR data against pre-existing databases and so-called "pre-determined criteria" criteria (Article 6 (3) (a) and (b) of the EU PNR Directive). Therefore, other than detecting the cross-border movement of known persons, PNR data is also used to identify as yet unknown threats by processing passengers' data against pre-determined criteria, which are specific risk indicators. The latter are essentially algorithms which contain "*search criteria, based on the past and ongoing criminal investigations and intelligence, which allow to filter out passengers [who correspond] to certain abstract profiles* […]".[136] These pre-determined criteria serve to "*identify persons involved in criminal or terrorist activities who are, as of yet, not known to the law enforcement authorities*."[137] These criteria are set by the PIUs and updated based on new data and patterns available in the system. The automated processing of data has many implications for the right to privacy and right to data protection as also has been acknowledged by the CJEU.[138]

85. The CJEU has highlighted the risk of discrimination in this respect. While the PNR Directive acknowledges such risks in Article 6 (4), the CJEU in the *Ligues droits humains* case emphasised that that provision covers both direct and indirect discrimination.[139] This is particularly important because pre-established criteria may rely on seemingly harmless personal information, which could nonetheless serve as indirect indicators of prohibited traits. For instance, a person's address might be used as a proxy for their religion, "race", or ethnic background. As noted above, the CJEU held that algorithms need to be targeted, proportionate, and specific ensuring they are non-discriminatory.[140] This principle has broader significance, particularly in the field of migration. The Court noted that high false-positive rates, seen in statistics from EU Member States, could compromise the system's appropriateness and proportionality.[141] Therefore, the CJEU emphasized the importance of regularly reviewing the strict necessity of the pre-determined criteria.[142] It

135 ODIHR, Policy Brief: Border Management and Human Rights - Collection, processing and sharing of personal data and the use of new technologies in the counter-terrorism and freedom of movement context, 2021, p. 15.

136 European Commission, Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {COM(2020) 305 final}, 24 July 2020 p. 11 footnote 36.

137 European Commission, Report from the Commission to the European Parliament and the Council on the review of Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime {COM(2020) 305 final}, 24 July 2020 p. 24.

138 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022. In para 103 the CJEU notes with references to previous caselaw that "Against this background, it should be borne in mind that the Court has already held that the extent of the interference which automated analyses of PNR data entail in respect of the rights enshrined in Articles 7 and 8 of the Charter essentially depends on the pre-determined models and criteria and on the databases on which that type of data processing is based (Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017, EU:C:2017:592, paragraph 172)."

139 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 197.

140 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 198.

141 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 123.

142 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 201.

also noted that EU Member States should establish clear and precise rules that provide guidance for the individual review process with a view to prevent both discriminatory outcomes and erroneous matches from being passed on to the relevant authorities, which could unjustly subject passengers to suspicion of involvement in terrorism or serious crimes. Furthermore, as underlined above, the Court also emphasized that the findings from individual human reviews should take precedence over those generated by automated systems.[143]

86. **The legal drafters should put in place effective human rights safeguards to protect passengers from being wrongfully placed under suspicion for involvement in terrorism or other serious crimes and refrain from discriminatory profiling on the basis of PNR data.** In listing the tasks of the National Contact Point, Article 15 of the Draft Law makes a reference to "*monitoring, processing and analyzing passenger check-in record […] data in order to update, update, create (cancel) risk profiles or criteria for identifying persons who may be involved in terrorist activities*". **It is important that these criteria and profiles are targeted, proportionate and specific and for the Draft Law to reflect these requirements. The Draft Law should mandate the relevant authorities to provide necessary guidance for individual reviews to prevent discriminatory results.** These criteria should be regularly reviewed and shall in no circumstances be based on a person's "race" or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, health, sexual life or sexual orientation.[144] **An explicit reference thereto should be made in Article 15 of the Draft Law. Similar considerations should apply to databases and watchlists with a view to ensure transparency in the watchlist criteria and to ensure redress is provided for wrongful inclusion.** The criteria for including individuals on such lists must be clearly defined based on a narrow and precise definition of terrorist offences and serious crimes. Also, stringent procedural safeguards must be in place to protect against arbitrariness, in particular effective remedies to challenge wrongful listing, as well as effective measures to secure delisting in practice, also when watchlists or data are shared transnationally.

87. The Draft Law also lacks an explicit provision to safeguard against indirect discrimination in data analysis. Profiling based on correlated attributes, such as travel history, nationality, or other patterns, could inadvertently result in biased outcomes disproportionately impacting certain groups. This risks undermining the principles of equality and the right to non-discrimination under Article 26 of the ICCPR, Article 14 of the ECHR and Protocol 12 to the ECHR and Article 21 of the EU Charter. **In this regard, the Draft Law should include an explicit reference to the prohibition of indirect discrimination by and through data processing.**

88. Generally, the authorities are strongly encouraged make sure that those processing API/PNR data receive adequate human rights training and are sensitized to potential human rights implications of the systems.

89. Finally, Article 16 lists the tasks of the National PNR Processing System. Paragraph 4, includes a general non-discrimination clause. Whilst this is welcome, the non-discrimination clause could also include a reference to trade union membership and health of the passenger, as it is the case in ICAO and EU PNR Directive standards.[145]

143 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 205-208.
144 Article 6 (4) of the EU PNR Directive.
145 EU PNR Directive Preamble para 15, ICAO Annex 9 Article 9.30 b)

RECOMMENDATION F.

To put in place effective human rights safeguards to protect passengers from being wrongfully placed under suspicion for involvement in terrorism or other serious crimes and refrain from discriminatory profiling on the basis of PNR data in listing the tasks of the National Contact Point in Article 15. Risk criteria and profiles need to be targeted, proportionate and specific and should mandate the relevant authorities to provide necessary guidance for individual reviews to prevent discriminatory results.

5. DUTY TO INFORM AND SECURITY OF PERSONAL DATA

90. The GDPR, EU PNR Directive, modernised Convention 108 (not yet ratified by Ukraine) and other relevant instruments all highlight the right to data protection. One of the key rights is to be informed about the processing of one's own data. Article 22 of the Draft Law entrusts air carriers with the duty to inform passengers about the processing of their data. However, it is also a state's responsibility to inform passengers on the processing of their personal data and the access to their data. The EU PNR Directive stipulates that "*Member States should ensure that passengers are provided with accurate information that is easily accessible and easy to understand about the collection of PNR data, their transfer to the PIU and their rights as data subjects"*.[146] **It is therefore recommended that the Draft Law mandates an approach whereby passengers are informed about the processing of their personal data in a clear and simple language they understand.**

91. A central provision in the Draft Law is Article 22, which concerns the protection of personal data. It provides that the record keeping of processing operations (collection, retention, review, disclosure and deletion) is ensured by the National Center (for API data) and the National Contact Point (for PNR data). The provision entrusts the National Centre and the National Contact Point with the 'security' of personal data. In case of a violation, these authorities are tasked with informing the Human Rights Commissioner and the data subject. This is in line with international and European standards, particularly Article 13 (8) of the EU PNR Directive.

92. However, as per ICAO standards, states have further obligations on personal data protection, especially with respect to the data subjects' rights. In this respect, Article 8 of the modernized CoE Convention 108 provides for clear obligations for public authorities to respond to requests concerning the existence of personal data, to communicate the data to the data subject, to rectify or erase in case of an unlawful collection/processing,[147] though there are exceptions in the interests of "*protecting state security*". These standards

146 EU PNR Directive Preamble, para. 29. For example, the **Netherlands** Government has a dedicated webpage, giving an overview in a simple, non-technical language on how passenger data is collected/used by different government agencies, as well as data protection aspects. It also provides information for passengers who wish to access this data, gives an information on how it can be appealed/ deleted (see Government of the Netherlands, Air passenger travel information https://www.government.nl/topics/aviation/air-passenger-travel-information). In **Canada,** the processing of API/PNR data is regulated by Customs Act, Privacy Act, Passenger Information Regulation along with other regulations. The main domestic authority collecting API/PNR data is the Canada Border Services Agency (CBSA). The Agency published Guidelines for the access to, use, and disclosure of API and PNR data and pre-departure air exit information, which exhibits good practices, especially with respect to data subject's access to personal data; see Government of Canada, Guidelines for the access to, use, and disclosure of advance passenger information (API), passenger name record (PNR) data and pre-departure air exit information, paras. 42-43.

147 Article 8 of the modernized CoE Convention 108 states that: "*Any person shall be enabled: a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention; d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with*".

are not only recognized by the CoE Convention, but also the international soft-law instruments such as the 1988 *UN Guidelines for the Regulation of Computerized Personal Data Files* (Principle 4) and *The Tshwane Principles* (Part III).[148] Unless already sufficiently addressed in the Law of Ukraine on the Protection of Personal Data, **the Draft Law would be substantially strengthened by explicitly reflecting such data protections rights.**

93. It is good practice that Article 21 of the Draft Law foresees the appointment of PNR data protection officers. However, this provision should be strengthened and brought in line with the above standards. Firstly, as per the EU PNR Directive, data protection officers should be provided with the means to perform their duties and tasks effectively and independently.[149] **It is recommended that a similar clause is inserted in the Draft Law to ensure effective and independent work of the data protection officers.** Secondly, the EU PNR Directive requires that states ensure "*that a data subject has the right to contact the data protection officer, as a single point of contact, on all issues relating to the processing of that data subject's PNR data*".[150] **In the absence of such a clause in the Draft Law, it is recommended to provide a means by which data subjects can reach data protection officers directly.**

94. While Article 21 of the Draft law notes that the data protection officers have access to all data processed in the PNR data collection system of the PNR PS, the CJEU specified that "while the data protection officer has access to all data processed by the PIU, that access must necessarily cover the pre-determined criteria and databases used by that unit in order to guarantee effectiveness and a high level of data protection that that officer must ensure in accordance with recital 37 of that directive".[151]

95. The last paragraph of Article 21 of the Draft Law states that the PNR data protection officers 'interact' with the Commissioner of Human Rights of the Verkhovna Rada of Ukraine. However, it is unclear what is meant by 'interact'. **It should be clarified that the PNR data protection officers can report to the Commissioner directly and in confidentiality, and that they can refer cases to the Commissioner and undertake other actions.**

RECOMMENDATION G.

To clarify in Article 21 of the Draft Law that the PNR data protection officers can report to the Commissioner directly and in confidentiality, and that they can refer cases to the Commissioner and undertake other actions.

148 See also OSCE PA Ad Hoc Committee on Countering Terrorism ' Strengthening Border Security and Information Sharing in the OSCE Region – A Parliamentary Oversight Exercise' p. 13. For example, in **Germany**, data processing of API is stipulated under the legal provisions contained in the Federal Police Act. Data requests are logged, and the processing of API data is subject to ongoing audits and specialist supervision. It also includes strict regulations for the protection of personal data (e.g., regarding the involvement of the Federal Commissioner for Data Protection and Freedom of Information, the depersonalization of passenger data along with data logging) which must be complied with when processing passenger data.

149 Article 5 (2) of the EU PNR Directive.

150 Article 5 (3) of the EU PNR Directive.

151 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 212.

6. INDEPENDENT OVERSIGHT

96. According to ICAO standards, states shall designate one or more competent domestic authorities with the power to conduct independent oversight of the protection of PNR data and determine whether PNR data are being collected, used, processed, and protected with full respect of human rights and freedoms.[152] Similarly, as per the EU PNR Directive, the EU Member States shall establish a 'National Supervisory Authority' with a view to protecting fundamental rights in relation to the processing of personal data (see also Articles 51-59 of the GDPR and Article 15 Modernized Convention 108). Such a body should be structurally and operationally independent as per Articles 51 and 52 of the GDPR, deal with complaints lodged by any data subject, investigate the matter and inform the data subjects of the progress and the outcome of their complaints within a reasonable time period and verify the lawfulness of the data processing, conduct investigations, inspection and audits in accordance with national law, either on its own initiative or on the basis of a complaint. Any data subject should also be informed on the exercise of their rights.[153]

97. Article 23 of the Draft Law designates the Human Rights Commissioner of the Verkhovna Rada of Ukraine as the supervisory body. However, beyond the stipulations in the Draft Law, it is important that the Commissioner has the legal mandate, sufficient technical, human and financial resources and powers to effectively carry out the oversight of the National Centre and the National Contact Point, as laid out in the PNR Directive. **It is recommended that these aspects be incorporated in the Law governing the Human Rights Commissioner, with an appropriate reference included in the Draft Law.** Further, since Article 23 of the Draft Law refers to *parliamentary* control of the compliance of the Draft Law with data protection regulations, it raises the question of whether the Human Rights Commissioner acts as an independent supervisory body in accordance with Article 52 of the GDPR. The latter provides, amongst others, that "*each supervisory authority shall act with complete independence in performing its tasks and exercising its powers in accordance with this Regulation"* and that *"[t]he member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody*…". **It is therefore recommended to ensure that any oversight of compliance with data regulation is carried out independently by the authorized body, which is granted the necessary resources and powers to fulfil its mandate in a manner consistent with international instruments.**

98. Finally, Article 77 of the GDPR provides that every data subject shall have the right to lodge a complaint with a supervisory authority. Such a safeguard is not foreseen in the Draft Law. **It is recommended to include this complaint mechanism explicitly in the Draft Law and to reflect this mechanism in the Law governing the Human Rights Commissioner.**

99. In that regard, it is noted that the CJEU in the *Ligue des droits humains* case held that according to the EU PNR Directive, the national supervisory authority ensures the monitoring of the lawfulness of the automated processing carried out by the PIU in connection with the advance assessment. This monitoring covers, inter alia, whether those operations are not discriminatory. While the provisions concerning data protection officers state they have access to all data processed by the PIU, and that such access must necessarily cover the pre-determined criteria and databases used by that unit in order to

152 ICAO Annex 9 , Article 9.29.
153 Article 15 of the EU PNR Directive.

guarantee effectiveness and a high level of data protection that these officers must ensure, similarly, the investigations, inspections and audits that the national supervisory authority conducts pursuant to the relevant provisions of the EU PNR Directive may also concern those pre-determined criteria and those databases.[154] **Accordingly, the Human Rights Commissioner should be given full and unhindered access to all information processed by the PIU as well as pre-determined criteria and databases to be able to fulfil its mandate.**

RECOMMENDATION H.

To ensure that any oversight of compliance with data regulation is carried out independently by the authorized body, which is granted the necessary resources and powers to fulfil its mandate in a manner consistent with international instruments and to ensure that this body, or the **Human Rights Commissioner, be given full and unhindered access to all information processed by the PIU as well as pre-determined criteria and databases to be able to fulfil its mandate.**

7. APPEALS MECHANISMS AND JUDICIAL REVIEW

100. In addition to the right to file a complaint with the supervisory authority, individuals are entitled to an effective judicial remedy, allowing them to take their case regarding potential data protection breaches to court. The right to seek legal recourse is recognized in both Article 47 of the EU Charter of Fundamental Rights and Article 13 of the ECHR. Article 78 of the GDPR provides the right to an effective judicial remedy against a supervisory authority which in particular, guarantees a right of judicial review against the decisions of data protection authorities. Standard 9.26 of Annex 9 to the Chicago Convention calls on states to provide for administrative and judicial redress mechanisms to enable individuals to seek a remedy for the unlawful processing of PNR data by public authorities and provide for appropriate mechanisms, established by their legal and administrative framework, for individuals to obtain access to their PNR data and to request, if necessary, corrections, deletions, or notations.[155]

101. Article 26 of the Draft Law provides that actions or decisions of the National Center, the National Contact Point or authorized bodies may be challenged in court, though there are no references to the particular competent court(s) nor to the relevant procedure**. A cross-reference to applicable legislation and procedure could be included in this provision, unless sufficiently provided in the Ukrainian Law on the Protection of Personal Data, a reference to which could then be included in this provision.**

102. For the right to judicial redress to be effective in practice, **data subjects should be provided with comprehensive information** in a language they understand **to be able to challenge the lawfulness of the automated processing and the following individual review; similarly, comprehensive information should be provided, in the context of redress, to the court and the persons concerned, to examine the legality of the**

154 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 212.
155 ICAO Annex 9 , Standard 9.26.

decision adopted by the competent authorities, i.e., the grounds and the evidence.[156] In both situations, certain exceptions to provide information may apply.[157] **The Draft Law should be supplemented in this respect**.

8. RECOMMENDATIONS RELATED TO THE PROCESS OF PREPARING AND ADOPTING THE DRAFT LAW

103. OSCE participating States have committed to ensure that legislation will be "*adopted at the end of a public procedure, and [that] regulations will be published, that being the condition for their applicability*" (1990 Copenhagen Document, para. 5.8).[158] Moreover, key commitments specify that *"[l]egislation will be formulated and adopted as the result of an open process reflecting the will of the people, either directly or through their elected representatives"* (1991 Moscow Document, para. 18.1).[159] The ODIHR Guidelines on Democratic Lawmaking for Better Laws (2024) underline the importance of evidence-based, open, transparent, participatory and inclusive lawmaking process, offering meaningful opportunities to all interested stakeholders to provide input throughout the lawmaking process.[160]

104. It is understood that the Security Service of Ukraine has sought to consult various stakeholders, including other institutions of the security and defense sector, and international partners, to develop the Draft Law. This is generally a welcome approach that is overall in line with OSCE commitments.

105. Public consultations constitute a means of open and democratic governance as they lead to higher transparency and accountability of public institutions, and help ensure that potential controversies are identified before a law is adopted.[161] Consultations on draft legislation and policies, in order to be effective, need to be inclusive and to provide relevant stakeholders with sufficient time to prepare and submit recommendations on draft legislation; the State should also provide for an adequate and timely feedback mechanism whereby public authorities should acknowledge and respond to contributions.[162] To guarantee effective participation, consultation mechanisms should allow for input at an early stage, from the initial policymaking phase *and throughout the process*,[163] meaning not only when the draft is being prepared but also when it is discussed before Parliament, be it during public hearings or during the meetings of the parliamentary committees. Given the sensitivity and importance of such a wide-ranging reform, it is fundamental that all voices are heard, even those that may be critical of the proposed initiatives with a view to address the issues being raised and achieve broad political consensus and public support within the country about such a reform. Ultimately, this tends to improve the implementation of laws once adopted, and enhance public trust in public institutions in general.

106. The legal drafters have prepared an Explanatory Statement to the Draft Law, which lists a number of reasons justifying the contemplated reform, but does not mention the

156 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, paras. 209-211. See also EDPB, *Statement 2/2025 of the European Data Protection Board on the implementation of the PNR Directive in light of CJEU Judgment C-817/19*, adopted on 13 March 2025, para. 19.
157 CJEU, C-817/19 [GC], *Ligue des droits humains ASBL v. Conseil des ministres* (Legality of EU Passenger Name Records), 21 June 2022, para. 210.
158 Available at <http://www.osce.org/fr/odihr/elections/14304http://www.osce.org/fr/odihr/elections/14304>.
159 Available at <http://www.osce.org/fr/odihr/elections/14310http://www.osce.org/fr/odihr/elections/14310>.
160 See ODIHR Guidelines on Democratic Lawmaking for Better Laws (January 2024), in particular Principles 5, 6, 7 and 12. See also Venice Commission, Rule of Law Checklist, CDL-AD(2016)007, Part II.A.5.
161 See Recommendations on Enhancing the Participation of Associations in Public Decision-Making Processes (from the participants to the Civil Society Forum organized by ODIHR on the margins of the 2015 Supplementary Human Dimension Meeting on Freedoms of Peaceful Assembly and Association), Vienna 15-16 April 2015.
162 See ODIHR, Guidelines on Democratic Lawmaking for Better Laws (2024), Principle 7.
163 See ODIHR, Guidelines on Democratic Lawmaking for Better Laws (2024), Principle 7.

research and impact assessment on which these findings are based. In principle, laws and public decision-making should be prepared, discussed and adopted on the basis of well-founded arguments, scientific evidence and data, including information deriving from impact assessments and consultations with the public and other stakeholders.[164] Given the potential impact of the Draft Law on the exercise of human rights and fundamental freedoms, an in-depth regulatory impact assessment (see also Article 35 of the GDPR), including on human rights compliance, is essential, which should contain a proper problem analysis, using evidence-based techniques to identify the most efficient and effective regulatory option.[165] In the event that such an impact assessment has not yet been conducted, the legal drafters are encouraged to undertake such an in-depth review, to identify existing problems, and adapt proposed solutions accordingly.

107. In light of the above, **the public authorities are encouraged to ensure that the Draft Law continues to be subjected to inclusive, extensive and effective consultations, including with civil society organizations, airline companies, and offering equal opportunities for women and men to participate. According to the principles stated above, such consultations should take place in a timely manner, at all stages of the law-making process, including before Parliament. As an important element of good lawmaking, a consistent monitoring and evaluation system on the implementation of legislation should also be put in place that would efficiently evaluate the operation and effectiveness of the Draft Law, once adopted**.[166]

[END OF TEXT]

164 See ODIHR Guidelines on Democratic Lawmaking for Better Laws (January 2024), Principle 5, Evidenced-based lawmaking.

165 See e.g., ODIHR, Preliminary Assessment of the Legislative Process in the Republic of Uzbekistan (11 December 2019), Recommendations L and M; and Venice Commission, Rule of Law Checklist, CDL-AD(2016)007, Part II.A.5.

166 See ODIHR Guidelines on Democratic Lawmaking for Better Laws (January 2024), para. 23. See e.g., OECD, International Practices on Ex Post Evaluation (2010).

PROJECT

LAW OF UKRAINE
On the use of passenger information to combat terrorism, serious and especially serious crimes

This Law defines the legal and organizational framework for obtaining, processing, disseminating, storing and protecting information about passengers of international flights.

Article 1. Definition of terms

In this Law, the following terms shall have the following meanings:

"The Single Window is a unified data acquisition system that allows using its own information and communication system to receive preliminary passenger information (API) for international flights and passenger check-in record (PNR) data for international flights, as well as information about international flight carriers from air carriers

depersonalization of data by hiding its elements - hiding data elements from users that can serve to directly identify the data subject;

competent authority of a foreign state - a body for the prevention, detection and investigation of terrorist and serious crimes, or a branch of such a body that functions as a passenger information body;

international flight means the movement of a vehicle according to an established route and schedule or off-schedule with takeoff or landing on the territory of Ukraine, during which the state border of Ukraine is crossed;

The National Passenger Check-in (PNR) Data Processing System for International Flights (hereinafter referred to as the National PNR Processing System) is an information and communication system that processes international flight check-in data received in accordance with the established procedure;

The National System for Processing Advance Passenger Information (API) for International Flights (hereinafter referred to as the National API Processing System) is an information and communication system that processes advance passenger information (API) received in accordance with the established procedure;

The National Contact Point for processing international flight passenger check-in data (Passenger Information Unit, - PIU; hereinafter referred to as the National Contact Point) is a body that performs the functions of receiving international flight passenger check-in data (PNR) from air carriers, storing,

processing, distributing such data or the results of their processing to authorized bodies and exchanging PNR data and the results of processing such data with the competent authorities of foreign countries in accordance with the procedure established by this Law ;

The National Center for Processing Preliminary Information on Passengers of International Flights (hereinafter referred to as the National Center) is a body that performs the functions of receiving, processing, disseminating, storing and protecting preliminary information on passengers of international flights;

preliminary passenger information (API) - specific data on passengers and their flights collected by the air carrier and sent to the Single Window;

reservation system - an internal airline system that collects preliminary information about passengers (API) and passenger registration record (PNR) data for making a reservation;

authorized bodies - subjects of the fight against terrorism, as defined by the Law of Ukraine "On Combating Terrorism", which, within the framework of counterintelligence, operational search, intelligence cases and during the pre-trial investigation of criminal proceedings, have the right to receive information about passengers (API and PNR) and the results of processing such information upon request.

The terms "advance passenger information/passenger name record", "passenger registration record (PNR)" in this Law shall have the meanings given in the Law of Ukraine "On Combating Terrorism".

Other terms are used in this Law in the meanings given in the Air Code of Ukraine, the Laws of Ukraine "On Transport", "On Personal Data Protection" and other Laws of Ukraine

Article 2. Purpose of the Law

Advance Passenger Information (API) for international flights is obtained and used to improve border control and combat illegal migration

Passenger check-in record (PNR) data of international flights are received, processed, distributed, and stored for the purpose of combating international terrorism, including the movement of persons involved in terrorist activities, prevention, detection, and investigation of criminal offenses committed for terrorist purposes, and other serious and especially serious crimes.

Article 3. Legislation in the field of obtaining, processing, dissemination, storage and protection of passenger information (API and PNR)

The relations arising from the receipt, processing, dissemination, storage and protection of passenger information (API and PNR) for international flights are governed by the Constitution of Ukraine, applicable international treaties ratified by the Verkhovna Rada of Ukraine, this and other laws of Ukraine, as well

as regulations adopted for their implementation.

Article 4. Subjects and object of relations related to passenger information (API and PNR)

The subjects of information relations are:

National contact point

National Center

authorized bodies

competent authorities of a foreign state;

European Police Office (Europol);

International Criminal Police Organization (Interpol);

air carriers;

passengers.

The object of the relationship is the personal data of passengers of international flights.

Article 5. Functioning of the Single Window

The functions of the Single Window administrator are vested in the National Center. The owner of the information and communication system of the Single Window is the state represented by the central executive body that implements the state policy in the field of state border protection.

The procedure of the Single Window functioning, protocols and data formats, the method of transferring passenger information (API and PNR) by air carriers to the Single Window and from the Single Window to the National Center and the National Contact Point are determined jointly by the central executive body implementing the state policy in the field of state border protection, the Anti-Terrorist Center at the Security Service of Ukraine and the central executive body implementing the state policy in the field of civil aviation and airspace use.

Passenger information (API and PNR) is received from air carriers to the Single Window, where it is pre-segmented into preliminary passenger information (API) and passenger check-in record (PNR) data, and is transmitted without any changes and in full:

preliminary passenger information (API) to the National Center;

passenger registration record (PNR) data to the National Contact Point.

The information about the air carrier sent to the Single Window is provided simultaneously to the National Center and the National Contact Point.

The Single Window does not accumulate and store preliminary passenger information (API) and passenger check-in record (PNR) data. The passenger

information received from air carriers (API and PNR) is immediately deleted after it is transferred to the National Center and the National Contact Point.

The Single Window Administrator provides full access to the network equipment and software of the Single Window information and communication system to the technical specialists of the National Center and the National Contact Point in order to verify the correctness of the system settings in the process of transferring preliminary passenger information (API) and passenger registration record (PNR) data

Information on the crossing of the state border of Ukraine by the President of Ukraine, members of the Parliament of Ukraine, members of the Cabinet of Ministers of Ukraine, judges of the Constitutional Court of Ukraine and judges of the Supreme Court is received by the National Center and the National Contact Point in accordance with the procedure established by the Law of Ukraine "On Transport".

Article 6. Information about the air carrier

In order to ensure the efficient transfer of passenger information (API and PNR) for international flights, air carriers are required to provide the following information to the Single Window:

airline name, location, phone number, and email address;

international flight schedule established by the air carrier.

air carrier is obliged to transmit such information no later than ten business days before the start of international flights.

In the case of international flights not included in the schedule or international traffic program, the air carrier shall provide the information specified in part one of this Article to the Single Window immediately after the planned international flight is included in the schedule or international traffic program.

If the information specified in part one of this Article has changed, the air carrier shall immediately transmit the updated information to the Single Window.

Article 7. Procedure for the transfer of preliminary information about passengers by air carriers (API)

Air carriers are obliged to collect and provide advance passenger information (API) for international flights to the Single Window free of charge.

Preliminary passenger information (API) is provided by air carriers to the Single Window by means of electronic communication after the completion of check-in for an international flight, using common protocols and supported data formats, and in case of technical failure, by any other appropriate means that ensure an appropriate level of data security.

Article 8. Components of advance passenger information (API)

The preliminary passenger information (API) provided by the air carrier to the Single Window must contain the following information:

airline and its code;

flight number;

number of passengers;

number and type of travel document;

the country that issued the travel document;

full name of the passenger (surname, name, patronymic as indicated in the travel document);

date of birth;

gender;

type, number, country of issue and expiration date of any passenger's identity or citizenship document;

airport of arrival (or departure) in Ukraine;

the scheduled departure (or arrival) time of the flight;

the scheduled departure (or arrival) date of the flight;

airport of arrival (or departure) outside the territory of Ukraine.

Article 9. Procedure and term of storage of preliminary information about passengers (API)

The national center must store preliminary passenger information (API) in the form of temporary files.

After the passengers enter the territory of Ukraine, the National Center must delete the preliminary passenger information (API) within 24 hours after the transfer, except when such data is necessary for border control.

Air carriers are obliged to delete the preliminary passenger information (API) provided to the Single Window within 24 hours after the arrival of the aircraft.

Article 10. National center

The functions of the National Center are vested in the central executive body that implements state policy in the field of state border protection.

The structure and procedure of the National Center are determined by the Regulation on the National Center for Processing Preliminary Information on Passengers of International Flights, which is developed by the central executive body that implements state policy in the field of state border protection.

Tasks of the National Center:

1) processing of preliminary information about passengers (API);

2) transfer of preliminary information about passengers (API) and the results of its processing to the authorized bodies;

3) checking passenger preliminary information (API) in the relevant databases;

4) processing statistical information on preliminary passenger information (API).

The National Center performs its tasks around the clock, without days off and holidays.

The National Center is the administrator of the National API Processing System and takes measures to create, implement and maintain software, is responsible for technical and technological support, data storage and protection, takes technical and technological measures to provide, block and cancel access to the National API Processing System, as well as other measures (actions) provided for by law

Article 11. Requirements for the Functioning of the National API Processing System

The owner of the National API Processing System is the state, represented by the central executive body that implements state policy in the field of state border protection.

The structure and operation of the National API Processing System are determined by the Central Executive Body that implements the state policy in the field of state border protection

The national API processing system has:

1) prevent unauthorized access to it by unauthorized persons;

2) prevent the processing of preliminary passenger information (API) for purposes that do not comply with this Law;

3) to prevent discrimination against persons on any grounds, such as gender, race, skin color, ethnic or social origin, genetic characteristics, language, religion or belief, political or any other beliefs, membership in a national minority, property status, place of birth, disability, age or sexual orientation;

4) ensure registration of all cases of accessing or otherwise using advance passenger information (API)

Article 12. Procedure for the transfer of passenger registration data (PNR) by air carriers

Air carriers are obliged to collect and provide passenger check-in record (PNR) data of international flights to the National Contact Point free of charge.

Passenger check-in record (PNR) data is provided by air carriers to the Single Window by means of electronic communication using common protocols and supported data formats, and in case of technical failure, by any other appropriate means that ensure an appropriate level of data security.

Article 13. Components of the Passenger Record (PNR)

The following components of the Passenger Name Record (PNR) are

processed (if collected by the air carrier):

1) booking identification number (booking code);

2) date of booking or issuance of the ticket for the international flight;

3) date of the scheduled international flight;

4) surname, name, patronymic (if any) of the person;

5) address and contact information (phone number, email address, etc.);

6) information on the payment for the ticket, including the payment card number, information on cash payment, information contained in the invoice or other confirmation of payment for the ticket, as well as information set forth in the payment order, namely: bank account numbers of the sender and recipient, names and surnames or titles of the sender and recipient, amount and currency of the transfer, date and time of the transfer and its basis;

7) full description of the travel route for a specific passenger check-in record;

8) information on the availability of a loyalty program;

9) the name of the travel agency or bureau, its phone number, email address, and location;

10) data on the person's travel status, which includes:

confirmation of the booking stages;

the status of baggage and ticket processing;

information on whether the person applied for registration in person or purchased a ticket during the issuance of travel documents without prior reservation;

11) information on the separation of passenger check-in record (PNR) data, which includes data on the change of reservation made for more than one person for a new flight direction for at least one of them, or the separation of passenger check-in record (PNR) data, which includes information on the change of reservation made for more than one person for a new flight direction for all persons to whom it applies;

12) information relating to a minor:

surname, name, patronymic (if any), passport or identity document number, and contact information (country of residence (stay), telephone number, e-mail address);

Surname, name, patronymic (if any) of the accompanying person at the time of departure of the aircraft and at the time of landing, passport or identity document number, as well as contact information (country of residence (stay), telephone number, e-mail address, type of communication connecting him/her

with the minor);

13) ticket number, date of issue and information on whether a return ticket is available, as well as information on the automatically calculated fare used to determine the ticket price;

14) seat number and other information related to this seat;

15) information on joint transfer services;

16) information on the amount, type and weight of baggage;

17) the number, names and surnames of other passengers specified in the preliminary registration data of the person related to the reservation;

18) any preliminary passenger information (PI) collected, including the type, number, country of issue and expiration date of any identity document, nationality, surname, name, gender, date of birth, flight number, departure date, arrival date, departure airport, arrival airport, departure time, arrival time;

19) general information about the flight:

flight number;

airline code;

time and date of departure of the aircraft.

20) information on any changes to the passenger registration record (PNR) data.

Article 14. Time limits for the transfer of passenger check-in record (PNR) data by the air carrier

The air carrier is obliged to provide the Single Window with passenger check-in record (PNR) data that it accumulates during its operations, when booking or performing transportation.

Passenger check-in record (PNR) data is transmitted by the air carrier to the Single Window:

1) not earlier than 48 hours and not later than 24 hours before the scheduled time of the international flight;

2) immediately after the close of check-in for the relevant flight, when passengers can no longer board or disembark.

In addition to the above deadlines, in certain cases, upon request of the National Contact Point, the air carrier shall provide passenger check-in record (PNR) data through the Single Window within the timeframe specified in the request.

In case of changes to the passenger check-in record (PNR) data transmitted pursuant to part one of this Article, the air carrier shall transmit the updated data to the Single Window before flight.

Article 15. National contact point

The functions of the National Contact Point are vested in the Anti-Terrorist Center at the Security Service of Ukraine, which carries out national coordination on the receipt, processing, dissemination, storage and protection of passenger registration (PNR) data.

The structure and procedure of the National Contact Point are determined by the Regulation on the National Contact Point for Processing International Flight Passenger Check-in Data, which is being developed by the Anti-Terrorist Center at the Security Service of Ukraine

Tasks of the National Contact Point:

1) obtaining passenger check-in record (PNR) data from air carriers;

2) monitoring, processing and analyzing passenger check-in record (PNR) data in order to update, update, create (cancel) risk profiles or criteria for identifying persons who may be involved in terrorist activities, other serious and especially serious crimes, as well as other persons who pose a threat to the national security of Ukraine;

3) verification of passenger check-in record (PNR) data against information systems and databases or in accordance with defined risk profiles, including before their arrival in Ukraine;

4) processing of statistical information based on passenger registration record (PNR) data;

5) assessing the passenger registration record (PNR) data prior to their planned arrival in/through Ukraine in order to identify persons who need to be checked by the authorized bodies;

6) provision of passenger registration record (PNR) data in accordance with Article 19 of this Law;

7) exchange of passenger registration record (PNR) data or the results of their processing with the competent authorities of foreign countries, the European Police Office and the International Criminal Police Organization - Interpol;

8) taking measures to preserve the received passenger registration record (PNR) data in the manner and within the time limits specified by this Law.

The National Contact Point performs its tasks around the clock, seven days a week and on public holidays.

The national contact point has direct, including automated, access to automated information and reference systems, registers and data banks, the holders (administrators) of which are state bodies or operators, uses state, including government, means of communication and communication, special communication networks and other technical means in order to perform the tasks specified by this Law.

The owner of the National PNR Processing System, the owner of the information processed in it, is the state represented by the Anti-Terrorist Center under the Security Service of Ukraine, which is the manager of the passenger registration record (PNR) and personal data about them

Article 16. National PNR processing system

The structure and operation of the National PNR Processing System is determined by the Anti-Terrorist Center of the Security Service of Ukraine.

The national PNR processing system provides:

1) collecting, receiving, processing, and evaluating passenger check-in record (PNR) data;

2) preventing unauthorized access to it by unauthorized persons;

3) preventing the processing of passenger registration record (PNR) data for the purpose that does not comply with this Law;

4) preventing discrimination against persons on any grounds, such as gender, race, skin color, ethnic or social origin, genetic characteristics, language, religion or belief, political or any other beliefs, membership in a national minority, property status, place of birth, disability, age or sexual orientation;

5) recording of all cases of access to passenger registration data (PNR).

Article 17. The period of storage of passenger registration record (PNR) data and depersonalization of personal data

The national contact point is obliged to ensure that the Passenger Name Record (PNR) data is stored for five years after it is received.

After six months from the date of submission of the Passenger Record (PNR) data to the National Contact Point, it must be depersonalized by hiding such data elements that can serve to directly identify the passenger to whom the data relate:

1) surname, first name, patronymic (if any), including surnames, first names, patronymics (if any) of other passengers and data on the number of passengers traveling together contained in the reservation system, as well as any preliminary information about passengers (PI) received on the basis of paragraph 18 of part one of Article 13 of this Law;

2) address and contact information;

3) any forms of payment information, including the payment address, which can serve to directly identify the passenger or any other persons;

4) information about the air carrier's regular customers;

5) general information that can be used to directly identify the passenger.

The disclosure of impersonal passenger check-in data (PNR) is allowed only for the purpose specified in part two of Article 2 of this Law, in accordance

with the procedure established in the Regulation on the National Contact Point for Processing Passenger Check-in Data for International Flights in relation to Passenger Check-in Data (PNR).

After the expiration of the period of storage of passenger check-in record (PNR) data, the storage of such information may be extended only if there are grounds to believe that it is necessary to counter international terrorism, including the movement of persons involved in terrorist activities, prevention, detection, investigation of criminal offenses committed for terrorist purposes, and other serious and especially serious crimes.

Article 18. Processing of passenger registration record (PNR) data

The data entered into the National PNR Processing System shall be automatically compared with the relevant data of automated information and reference systems, registers and data banks, the holders (administrators) of which are state bodies or operators, to which the National Contact Point has access in accordance with part five of Article 15 of this Law.

The matches obtained as a result of the preliminary comparison are subject to mandatory individual verification by the National Contact Point staff.

Personal data is processed in compliance with the requirements of the Law of Ukraine "On Personal Data Protection".

Article 19. Dissemination of passenger information (API and PNR)

The National Center and the National Contact Point provide information about passengers (API and PNR) or the results of its processing to the authorized bodies for the purpose specified in Article 2 of this Law.

The procedure and terms for providing passenger information (API and PNR) to the authorized bodies are defined in the Regulations on the National Center for Processing Preliminary Information on Passengers of International Flights regarding Preliminary Information on Passengers (API) and in the Regulations on the National Contact Point for Processing Passenger Check-in Data regarding Passenger Check-in Data (PNR).

Article 20. Protection of passenger information (ARI and PNR)

The protection of information in the National API Processing System and the National PNR Processing System, as well as in the Single Window Information and Communication System, is carried out in accordance with the Constitution of Ukraine, international treaties of Ukraine, the Laws of Ukraine "On Personal Data Protection", "On Information Protection in Information and Communication Systems" and other laws of Ukraine, as well as regulations adopted for their implementation.

Article 21. Data protection officer of the passenger registration record (PNR)

The Anti-Terrorist Center of the Security Service of Ukraine appoints a

Passenger Name Record (PNR) Data Protection Officer who has access to all data processed in the Passenger Name Record (PNR) data storage system of the National PNR Processing System. The officer referred to in this article shall implement personal data protection measures during the monitoring and processing of passenger check-in data.

The use of personal data by employees of the National Contact Point should be carried out only in accordance with their official duties. These employees are obliged to prevent disclosure in any way of personal data entrusted to them or which became known in connection with the performance of their official duties, except in cases provided for by law. This obligation shall remain in force after they cease to perform activities related to personal data, except in cases provided for by law.

The Passenger Registration Record (PNR) Data Protection Officer interacts with the Ukrainian Parliament Commissioner for Personal Data Protection to prevent and eliminate violations of personal data protection legislation

Article 22. Protection of personal data

The legal basis for the protection of personal data of passengers of international flights is the Constitution of Ukraine, international treaties of Ukraine, the Law of Ukraine "On Personal Data Protection", this and other laws of Ukraine, as well as other regulatory acts adopted in accordance with them.

The processing of personal data of passengers of international flights is carried out exclusively for the purpose of achieving the goals set forth in this Law, taking into account the requirements of the legislation of Ukraine on personal data protection.

Air carriers, when making a reservation or issuing a ticket for the relevant flight, shall inform passengers about the processing of their data for the purpose specified in Article 2 of this Law, as well as about their right to personal data protection in accordance with part two of Article 12 of the Law of Ukraine "On Personal Data Protection"

The National Center and the National Contact Point should ensure that documentation of any systems and procedures for processing Advance Passenger Information (API) and Passenger Name Record (PNR) data are maintained.

The list of such documentation should include:

1) data of persons authorized to process passenger information (ARI and PNR) and access authorization levels;

2) information on requests for the transfer of preliminary passenger information (API) and passenger registration record (PNR) data received from authorized bodies and from the competent authorities of foreign countries.

The National Center and the National Contact Point shall keep records of

all personal data processing operations. These records must contain, in particular, information on the date and time, the identity of the person who accessed the advance passenger information (API) and passenger check-in record (PNR) data, and information on the requestor of such data. Such credentials must be used solely for the purposes of verification, monitoring, ensuring data security and safety, or auditing. Credentials are stored for five years.

The National Center and the National Contact Point must ensure that passengers and the Ukrainian Parliament Commissioner for Human Rights are immediately informed of any breach of personal data security that may result in a risk to the rights and freedoms of passengers.

If it is not possible to notify each passenger directly due to the excessive amount of information, the National Center and the National Contact Point are obliged to provide such notification by publishing information on the fact of a personal data security breach on their official websites. The passenger is considered to be duly notified of the fact of a breach of the security of his/her personal data from the moment such information is published on the official website of the National Center and the National Contact Point.

In case of transfer of Passenger Name Record (PNR) data in accordance with Article 24 of this Law the Passenger Name Record (PNR) Data Protection Officer must be informed each time.

Passenger information (API and PNR) is processed using the National API Processing System and the National PNR Processing System, which have their own security system that prevents the possibility of its loss, damage, distortion, and unauthorized access.

It is forbidden to process passenger information (API and PNR) that discloses information about a person's race or ethnicity, religion or ideological beliefs, membership in trade unions, genetic and biometric data, health status, sexual life or sexual orientation.

Article 23: Control over compliance with the legislation on the receipt, processing, dissemination, storage and protection of passenger information (ARI and PNR)

Parliamentary control over compliance with the legislation on personal data protection during the processing of passenger information (ARI and PNR) provided by air carriers is exercised by the Ukrainian Parliament Commissioner for Human Rights.

Article 24. International cooperation

International cooperation and the transfer of passenger information (ARI and PNR) within the framework of this Law is carried out by the National Center and the National Contact Point on the basis of international agreements ratified by the Verkhovna Rada of Ukraine, taking into account the Law of Ukraine "On Combating Terrorism".

Article 25. Liability of air carriers

The air carrier shall be liable for failure to provide, untimely provision, or provision of incomplete or inaccurate information about passengers (ARI and PNR) in accordance with the law.

Article 26: Appeal against actions and decisions

Decisions, actions or omissions of the National Center and the National Contact Point may be appealed in court.

Final and transitional provisions

1. This Law shall enter into force six months after its publication.

2. To amend the following Laws of Ukraine:

1) in Air Code of Ukraine (Vidomosti Verkhovna Rada of Ukraine (VVR), 2011, No. 48-49, p. 536):

part four of Article 70 shall be set forth in the following wording

"In order to counter international terrorism, including the movement of persons involved in terrorist activities, prevention, detection, investigation of criminal offenses committed for terrorist purposes, other serious and especially serious crimes, as well as to improve border control and combat illegal migration, air carriers are obliged to provide the Single Window with advance passenger information (API) of international flights and passenger check-in data (PNR) of international flights free of charge in accordance with the procedure established by the Law of Ukraine "On the Use of Passenger Information for Countering Terrorism, Serious and Particularly Serious Crimes"."

2) In the Law of Ukraine "On Combating Terrorism" (Vidomosti Verkhovna Rada of Ukraine, 2003, No. 25, p. 180, as amended):

part one of Article 7 shall be supplemented with new paragraph ten as follows:

"performing the function of the National Contact Point for processing international flight passenger registration data (Passenger Information Unit, PIU) in accordance with the Law of Ukraine "On the Use of Passenger Information for Countering Terrorism, Serious and Particularly Serious Crimes";";

In this regard, the tenth paragraph of part one of this Article shall be considered the eleventh paragraph accordingly;

3) in the Law of Ukraine "On the State Program of Civil Aviation Security" (Bulletin of the Verkhovna Rada of Ukraine (VRU), 2017, No. 16, p. 199):

the third paragraph of clause 58 of the State Program of Civil Security shall be set forth in the following wording:

"When operating international flights from/to Ukraine or transit flights

through Ukrainian airports, the air carrier is obliged to provide the Single Window with preliminary information on passengers (API) and passenger check-in record (PNR) data."

paragraph six of clause 58 of the State Program of Civil Security shall be deleted.

3. The Cabinet of Ministers of Ukraine within six months from the date of entry into force of this Law:

bring their regulatory acts into compliance with this Law;

ensure that acts of ministries and other central executive authorities are brought into compliance with this Law.

Chairman of the Verkhovna Rada of Ukraine