GLOBAL RISK INTEL

Risk Report

AIR TRAVEL SECURITY RISKS: NEW CHALLENGES OF PERSONAL DATA PROTECTION

www.globalriskintel.com

AIR TRAVEL SECURITY RISKS

NEW CHALLENGES OF PERSONAL DATA PROTECTION

Dr. Antonis Veneris

RISK REPORT

Global Risk Intelligence

FEBRUARY 26, 2019

Washington, D.C. · London · Singapore

www.globalriskintel.com

DISCLAIMER:

THE VIEWS EXPRESSED IN THIS DOCUMENT ARE THE SOLE RESPONSIBILITY OF THE AUTHOR(S) AND DO NOT NECESSARILY REFLECT THE VIEW OF GLOBAL RISK INTELLIGENCE. THIS DOCUMENT IS ISSUED WITH THE UNDERSTANDING THAT IF ANY EXTRACT IS USED, THE AUTHOR(S) AND GLOBAL RISK INTELLIGENCE SHALL BE CREDITED, PREFERABLY WITH THE DATE OF THE PUBLICATION.

About **Global Risk Intelligence**

For over seven years Global Risk Intelligence has advised clients about risks relevant to their business and operations using exclusive formulas and methodologies to identify key issues. We offer a comprehensive portfolio of tools, insights, briefings, and expert analysis that assist with helping clients better understand their situation.

For more information on all Global Risk Intelligence products and services, visit www.globalriskintel.com.

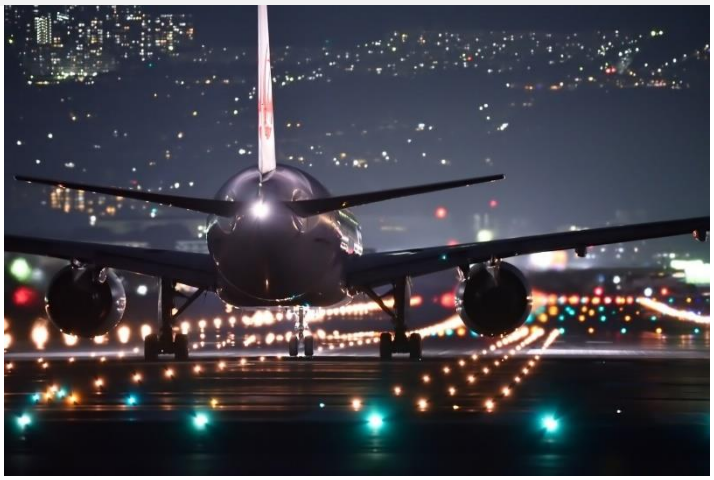
Dr. Antonis Veneris earned his doctorate in Law from Aristotle University of Thessaloniki in Greece. Previously, he earned his Master of Public Administration degree from Panteion University of Social and Political Sciences in Athens, Greece. Dr. Veneris is fluent in English in addition to his native Greek.

TAGS: AEROSPACE, AIR TRAVEL, EUROPE, EU, EUROPEAN UNION, DATA, DATA PRIVACY, LAW, LAW AND SOCIAL POLICY, POLICY, PRIVACY, RISK, SECURITY.

List of Abbreviations:

APIS	Advance Passenger Information System
CJEU	Court of Justice of the European Union
ECHR	European Court of Human Rights
EDP	European Data Protection
EU	European Union
PIU	Passenger Information Unit
PNR	Passenger Name Record
VIS	Visa Information System

Introduction



The Passenger Name Record (PNR), pursuant to the new Directive 2016/681, consists of the information that is provided by passengers when they book their flight. The PNR data is transferred by air carriers to the authorities competent for the purposes of prevention, detection, investigation or prosecution of terrorist offences or serious crime. The storage of personal data that fall within the scope of the Directive concern flying from a third country and planned to land on the territory of a Member State or flying from the territory of a Member State and planned to land in a third country, including in both cases flights with any stopovers in the territory of Member States or third countries. However, a Member State may decide to apply this Directive to intra-European Union (EU) flights as well.

Application and Structure

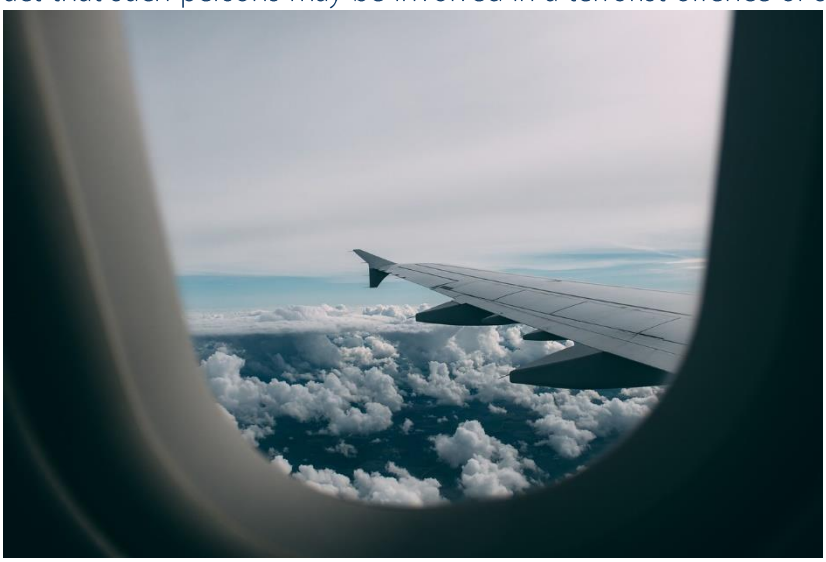
The EU has taken this measure in order to establish a common framework for the collection and exchange of personal data between member states' law enforcement authorities. In general, this Directive includes provisions concerning mainly the following:

a) The purposes for which data may be processed in the context of law enforcement obligations;
b) The transmission of data to the competent authorities, Europol, as well as to other European Union Member States and third countries;
c) The retention of personal data; and
d) Guarantees for passengers' rights based on personal data protection framework.

In order to meet these goals, every member state may establish the "Passenger Information Unit" (PIU).

Namely, based on Article 8 of the PNR Directive, air carriers transfer the PNR data to the database of the PIU of the Member State on the territory of which the flight will land or from the territory of which the flight will depart.

The PIU shall be responsible for, inter alia, collecting PNR data from air carriers, storing and processing those data and the result of the processing to the competent authorities as well as exchanging both PNR data and the result of the processing with the PIUs of other Member States and with Europol. Additionally, PIU shall process PNR data for carrying out an assessment of passengers prior to their scheduled arrival or departure in order to identify persons who require further examination by the competent authorities and, where relevant, by Europol in view of the fact that such persons may be involved in a terrorist offence or serious crime. The crimes that fall into the scope of the Directive are listed exclusively in its second Annex. However, these data may be further proceeded where other offences or indications thereof for other crimes, are detected in the context of enforcement action.



Additionally, Member States shall ensure that the PNR data provided by the air carriers to the PIU are retained in a database for a period of five years after their transfer to the PIU of the Member State on whose territory the flight is landing or departing. Upon expiry of a period of six months after the first transfer of the PNR data to PIU, all PNR data shall be depersonalised through masking out the necessary data elements which could serve to identify directly the passenger to whom the PNR data relate such as name, address, and forms of payment information.

The combat against terrorism and serious crime is a legitimate interest pursued by the EU legislator and in principle is considered to be necessary and obvious. Based on the aforementioned, the personal data contained in PNR may be proven to be valuable for public security. Nevertheless, the PNR processing system constitutes a limitation on fundamental rights and freedoms and must therefore be adequately justified and proven necessary in order to strike the right balance between

the protection of public security pursued and the limitation on privacy rights and the protection of personal data.

Further Details

Under Article 8 of the European Convention on Human Rights and Articles 7 and 8 of Charter of Fundamental Rights of the EU, which concern the rights to private life and personal data protection, public authorities may interfere with the exercise of privacy rights only in accordance with the law and where necessary in a democratic society, inter alia, in the interests of national security or public safety for the prevention of disorder or crime and subject to the principle of proportionality. The fact that the purpose of the PNR Directive is the prevention of terrorism and serious crime does not mean it clearly complies with these requirements; the necessity and proportionality of such factors have still yet to be proven. Namely, the necessity of PNR data processing does not seem to be sufficiently grounded because in the framework of the police and judicial cooperation in the EU, existing systems and other platforms including personal data are already in place, such as the Advance Passenger Information System (APIS), the Schengen Information System, and Visa Information System (VIS). Besides, various recent events in the EU demonstrate intelligence gaps unrelated to air travelers. Consequently, it could be argued that measures such as upgrading existing systems, ameliorating cooperation between Member States, and stepping up investigations into suspects, particularly those of which that are already known, might be more effective and appropriate to ensure the necessary information in comparison with the pre-profiling of millions passengers that PNR Directive pursues.

Additionally, the retention of personal data clearly constitutes an interference with the right to privacy of the persons concerned. The Court of Justice of the European Union (CJEU) held that

the determination of the period of retention must be based on objective criteria in order to ensure that it is limited to what is necessary. At the same time, the European Data Protection (EDP) Supervisor has repeatedly expressed doubts about the justification of data retention period. The PNR Directive foresees a period of 6 months of retention of the unmasked data followed by a period of 5 years of retention of the masked data. Even masked out, the data remain identifiable, and no evidence has been shown why there is a need to keep these additional 5 years.

Moreover, although the depersonalization stipulations, under special circumstances, full data are rendered invisible to a user. Although interesting examples have been reported in which retained data was used to exclude suspects from crime scenes and to verify alibis, they cannot be put forward as demonstrating the need for data retention. Moreover, the view that the PNR Directive is not in line with proportionality principle can be justified by the fact that there in no discrimination between suspects and innocent passengers. On the contrary, it could be considered proportionate to retain the data until thorough analysis has been completed, except for specific cases that led to a survey of a specific passenger.

Critical Elements

The PNR Directive lacks several elements required to meet the standards developed by the CJEU in terms of limitation of the use of personal data by the competent authorities. In this respect, the jurisprudence of the European Court of Human Rights (ECHR) confirms that the law must be sufficiently precise to indicate to citizens in what circumstances and on what terms the public authorities are empowered to file information on their private life and make use of it. In that case, based on Article 7 of Directive, the PNR data and the result of processing received by the PIU may be further processed by the competent authorities where other offences beyond this Directive are detected in the context of enforcement action. It follows that there are no objective criteria to

determine the limits of the access of the competent authorities to the data and their subsequent use in view of the extent and seriousness of the interference with the fundamental rights. Consequently, the PNR Directive does not explicitly provide that the PNR data may not be used beyond the purposes strictly identified, which contradicts the general principle of purpose limitation enshrined in Article 8 of the Charter of Fundamental Rights, as interpreted by the CJEU.

Concluding Thoughts

In sum, it must be held that the fight against serious crime, in particular against organized crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. The PNR Directive aims to preserve EU internal security and for this purpose establishes the processing of PNR Data, creating a common framework among Member States. Nevertheless, such an objective of general interest, however fundamental it may be, does not in itself justify any intervention to the right of personal data protection.

Under the PNR Directive, a huge amount of personal information on all passengers flying into and out of the EU will be collected, regardless of whether or not they are suspects. Collecting and processing PNR data for the fight against terrorism and serious crime should not enable mass tracking and surveillance of all passengers. Moreover, without any exception to the retention period of 5 years and any criteria that could be applied to shorten this period, it is not convincing that the PNR Directive meets the requirements laid down by the CJEU. The necessity for such a system, which affects millions of passengers, does not seem to be adequately justified.

Admittedly, it is not straightforward to demonstrate the proportionality of measures that intervene to the rights of privacy and personal data protection. Although, since there is no evidence to demonstrate adequately the proportionality of those measures and given that they do not provide clear and precise rules on access and retention of personal data, PNR Directive still does not meet the requirements of necessity and proportionality imposed by Articles 7, 8 and 52 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention on Human Rights.

www.globalriskintel.com