Council of the European Union

Brussels, 14 September 2022
(OR. en)

11846/22

LIMITE

CT 160
ENFOPOL 425
COTER 207
IXIM 218
AVIATION 223
CRIMORG 117

NOTE

From:	Presidency
To:	Delegations
Subject:	Travel intelligence and the identification of persons presenting a risk from the CT and CVE point of view

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (11.11.2022)

The Presidency would like to have a discussion in the Terrorism Working Party (TWP) on (the use of) travel intelligence data, with a special focus on PNR (Passenger Name Record) data, and the potential to use such data in CT (counter-terrorism) and CVE (countering violent extremism) efforts. This document, and the following discussion at the TWP, will strictly focus on CT and CVE aspects. Travel intelligence and PNR data have been discussed in other Council working groups, mainly in the IXIM (the Working Party on JHA Information Exchange). This document should help to frame the TWP's debate related to PNR.

To that end, we invite delegations to reply to the questions at the end of this paper in consultation with their experts on the PNR.

Background:

Over the years the phenomenon of travel intelligence has been a subject of global discussions. Within the EU, data was first provided through API (Advance Passenger Information) and the PNR, and later by the EES (Entry Exit System) and ETIAS (the European Travel Information and Authorisation System). All this data, taken together with data from the Schengen Information System (SIS II) and the Visa Information System (VIS), creates a comprehensive picture of travellers in the EU.

The API Directive was adopted in 2004 and its principal purpose is to fight illegal immigration and improve border control[1]. The PNR Directive was adopted in 2016 to fight terrorist offences and serious crime[2]. The EES Regulation was adopted in 2017[3] and the ETIAS Regulation was adopted in 2018[4]. Both of these systems are still being prepared and will focus on fighting illegal migration and improving border control.

1 Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data (OJ L 261, 6.8.2004, p. 24).

2 Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p. 132).

3 Regulation (EU) 2017/2226 of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011 (OJ L 327, 9.12.2017, p. 20).

4 Regulation (EU) 2018/1240 of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 (OJ L 236, 19.9.2018, p. 1).

DELETED

PNR data can be used to prevent, detect, investigate and prosecute terrorist offences and serious crime. This was one of the primary reasons that the EU PNR Directive was approved in 2016 after more than 10 years of discussion and negotiations. PNR data may consist of up to 18 data segments – name, date of reservation, date of intended travel, address, contact information (telephone number, email address), form of payment, travel itinerary (as part of one reservation code), seat number, names of other travellers (on the same reservation), etc.[5]

DELETED

[5] See Annex I to the EU PNR Directive. The air carriers are not obliged to collect all data segments.

DELETED

International efforts and challenges:

Members of terrorist groups and other transnational organised crime groups continue to take advantage of a sometimes insufficient detection capacity across the globe. Returning and relocating FTFs could pose a serious threat to global security. Therefore, processing passenger data is essential to the identification, detection and interception of FTFs and other serious criminals, including those that are otherwise unknown to authorities, both before, during and after travel. The UN, OSCE, IOM and other international organisations encourage countries to build targeting capacities at national level[6]. **DELETED**

[6] See Resolution 2396 (2017) of the UN Security Council. The UN created the Counter-Terrorism Travel Programme to assist Member States in building their capacities to prevent, detect, investigate and prosecute terrorist offences and other serious crimes by collecting and analysing passenger data. The Dutch government donated the Travel Information Portal system (TRIP) to the UN for this purpose.

DELETED