OSCE PA
Organization for Security and Co-operation in Europe
PARLIAMENTARY ASSEMBLY

Strengthening Border Security and Information Sharing in the OSCE Region: A Parliamentary Oversight Exercise

OSCE PARLIAMENTARY ASSEMBLY
AD HOC COMMITTEE ON COUNTERING TERRORISM

About the OSCE Parliamentary Assembly

As the parliamentary dimension of the Organization for Security and Co-operation in Europe, whose 57 participating States span the geographical area from Vancouver to Vladivostok, the primary task of the 323-member Assembly is to facilitate inter-parliamentary dialogue to advance political-military, economic-environmental and human rights security.

Recognized as a regional arrangement under Chapter VIII of the United Nations Charter, the OSCE is a primary instrument for early warning, conflict prevention, crisis management and post-conflict rehabilitation in its area. The Parliamentary Assembly was originally established by the 1990 Paris Summit to promote greater involvement in the OSCE by national parliaments, thus bringing increased democratic legitimacy to its efforts aimed at improving the security of over 1 billion citizens.

The OSCE PA actively engages in high-level political dialogue, election observation activities and a wide range of targeted initiatives in highly sensitive security fields, including counter-terrorism.

All Rights Reserved

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the OSCE Parliamentary Assembly.

ISBN 978-87-971711-0-3
October 2019

Disclaimer

The views, opinions, findings, interpretations and conclusions expressed herein are those of the authors and contributors and do not necessarily reflect the official policy or position of the OSCE PA and its participating States. For these reasons, no claims can be made against the OSCE PA in respect of potential consequences that may arise from the information contained in this report. The designations employed and the presentation of material in this report do not imply the expression of any opinion whatsoever on the part of OSCE PA concerning the legal status of any country, territory or city, or its authorities, or concerning the delimitation of its frontiers or boundaries.

Front cover photo by: Marco Bonabello, OSCE Parliamentary Assembly
Back cover photo by: Kazu End (@kazuend) on Unsplash

Strengthening Border Security and Information Sharing in the OSCE Region: A Parliamentary Oversight Exercise

Organization for Security and Co-operation in Europe
PARLIAMENTARY ASSEMBLY
AD HOC COMMITTEE ON COUNTERING TERRORISM

Contents

FOREWORD

The present OSCE PA Initiative is a unique exercise in the area of counter-terrorism through the work of parliaments of the OSCE participating States. Building on their oversight powers, it sheds light on substantive matters concerning the adoption and implementation at the national level of obligations stemming from UN Security Council Resolution 2396 on border security and information sharing, as well as on the challenges policymakers and practitioners face in this context.

Over 20 responses were received from national parliaments, revealing several promising practices. Some are highlighted in the report and could, hopefully, inspire other countries' efforts. Many challenges were also identified by the respondents, including the need to develop efficient inter-agency operational frameworks for processing data at national level and effective schemes for exchanging information at international level. Critical challenges also relate to staff expertise, human resources development and IT capabilities. Notably, some countries called for more international support and guidance to effectively establish their Advance Passenger Information (API), Passenger Name Records (PNR) and biometric data management systems. This includes legislative, technical and operational assistance, which could be provided by the OSCE executive structures, upon request.

I am also very pleased by the highly collaborative spirit of many respondents and by their readiness to share their experience and expertise. This may be one of the most encouraging outcomes of this Initiative, as only united can we make a real difference in countering terrorism and violent extremism.

The OSCE PA stands ready to continue promoting the coordinated implementation of the global counter-terrorism framework together with OSCE executive structures, the United Nations, and other relevant inter-parliamentary and regional organizations. More specifically, through its Ad Hoc Committee on Countering Terrorism, the OSCE PA remains committed to play an important role in bridging policies and practice in line with international human rights law. This was precisely our aim when embarking on this effort: to demonstrate that parliamentarians can play an active role in protecting citizens from terrorist threats. Bearing this in mind, the report strives to identify policy recommendations for the consideration of participating States and international stakeholders.

Sincerely,

Makis Voridis,
Former Chair of the Ad Hoc Committee on Countering Terrorism (2017-2019)
Member of the Greek Delegation to the OSCE PA (2013-2019)

Photo of Makis Voridis: Janine Schmitz / photothek/Deutscher Bundestag
Photo of the Ad Hoc Committee on Countering Terrrorism: Nat Parry/OSCE PA

I. INTRODUCTION

On 28 September 2018, the OSCE Parliamentary Assembly (OSCE PA) Ad Hoc Committee on Countering Terrorism (CCT) circulated both a questionnaire and a request to inquire respective national governments to all its parliamentary delegations in the OSCE region (see Annex). The questionnaire asked national governments about the enforcement of measures provided by UNSCR 2396 (2017) on border security and information sharing, namely pertaining to Advance Passenger Information (API), Passenger Name Record (PNR) and biometrics. These data management systems are particularly crucial for law enforcement to detect and prevent the movement of terrorists across national borders.

This OSCE PA Initiative is intended to complement the longstanding work of the OSCE executive structures aimed at assisting participating States.[1] It builds upon the OSCE PA *Resolution on Preventing and Countering Terrorism and Violent Extremism and Radicalization that Lead to Terrorism* (Berlin 2018), reaffirming the need to implement UN Security Council Resolutions 2396 and 2178 and other relevant OSCE commitments. These resolutions and commitments mandate States to take far-reaching action for countering the threat posed by foreign terrorist fighters (FTFs) en route to, or relocating from, conflict zones. Moreover, the *Resolution on Preventing and Countering Terrorism* stressed the need to boost security and information sharing measures through the collection of API, PNR and biometric data, and the development of databases of known and suspected terrorists in compliance with domestic, international and human rights law.

Ultimately, the aim of this effort is to bring a distinct parliamentary contribution to the full implementation of the global counter-terrorism framework.

II. KEY FINDINGS

- As of 30 April 2019, 36.84% (21) of national parliaments responded to the questions addressing the international obligations on Advance Passenger Information (API), Passenger Name Record (PNR) and biometrics. Notably, the 21 respondents represent the interests and needs of over 75% of the overall population in the OSCE region. The number of national parliaments that did *not* respond to the questionnaire, but nonetheless might have posed the questions to their respective governments, is unknown with one exception.
- Out of the 21 national parliaments which responded to the OSCE PA questionnaire, 13 provided information suggesting adequate capacity to effectively manage the process of collecting, storing, analyzing and sharing API, PNR, and biometric-related data.
- The challenges faced during the implementation of API, PNR, biometric data management systems originate from the complex and novel nature of the field. These include legal, operational as well as resource and infrastructure-related matters.

1 The OSCE has been steadily increasing its efforts to promote compliance with commitments stemming from UNSC Resolutions 2178 and 2396, including by supporting the adoption of the 2014 Ministerial Declaration on the OSCE Role in Countering the Phenomenon of FTFs, and the 2016 Ministerial Decision on Enhancing the Use of API. In January 2019, the OSCE Transnational Threats Department reported that 48% of the countries in the OSCE region have set up an API system and 31% regularly collect PNR data in accordance with the UNSCR 2396.

- Noting the urgency of the UNSCR 2396 provisions, several countries' governments enacted decrees to set up the required systems/mechanisms while the parliamentary legislative process was pending or lagging.
- The need to better integrate and facilitate information exchanges across different national databases, including those managed by customs, borders and law enforcement authorities, is generally perceived as a top priority. Indeed, overcoming discrepancies and lengthy processing of data across multiple platforms is critical for a more effective use of API, PNR and biometric systems.
- Some of the most critical challenges in setting up and maintaining modern systems for API, PNR and biometrics often relate to staff expertise, human resources development and IT capabilities. IT software and hardware components present high maintenance and upgrading costs that are critical for the timely and reliable data transmission between private airlines and law enforcement authorities.
- Most respondents also raised the urgency to increase the quality and consistency of the engagement with travel companies and airlines in relation to the timely transmission of data and their completeness.
- Several promising practices were also identified during the review process, including the cross-checking of travelers information with up-to-date operational intelligence data for assessing the risk of terrorism; the centralized management of API, PNR and biometric information to facilitate the recognition of potential suspects at borders; the immediate depersonalization of PNR when not relevant to law enforcement purposes; and the development of a national crew-member program to expedite security screening of certain flight crews and attendants for national flights.
- Legislation providing independent oversight mechanisms and the opportunity for citizens to redress proves critical for complying with international human rights law in the context of API, PNR and biometric information systems. Data protection bodies, national courts, and—for certain States—the European Court of Human Rights also play a key role.
- EU Member States' efforts in this domain benefit from 2004 and 2016 Directives setting common rules for the establishment of API and PNR systems, as well as biometric data cross-checking for serious crimes based on the European Information Exchange Model (EIXM).
- The lack of harmonized approaches towards personal data protection and the right to privacy has the potential to complicate effective law enforcement co-operation.

III. POLICY RECOMMENDATIONS

To the OSCE participating States

- National parliaments are ideally positioned to pass comprehensive legislation and oversee the implementation of relevant counter-terrorism policies and measures on border security and information sharing. They should guarantee the congruence of the norms regulating API, PNR and biometrics with the national rule of law framework and relevant international standards.

- Governmental decrees enacted to regulate urgently this technical field should be increasingly replaced by comprehensive legislation adopted by national parliaments with the intent to ensure wide political participation and full democratic control over the new legislation.

- Governments in the OSCE region should set up clear operational frameworks to facilitate smooth inter-agency co-operation and coordination at the national level in alignment of the active role played by a variety of stakeholders (e.g. law enforcement, customs, borders, air carriers, etc.) in the context of API, PNR and biometrics.

- Co-operation should be further strengthened between national authorities and private companies involved in the implementation of modern API, PNR and biometrics (i.e. air carriers and travel agencies).

- Relevant information on suspected terrorists revealed through the collection of API, PNR and/or biometric data should be securely shared in a timely manner with the relevant countries through bilateral and multilateral channels (e.g. INTERPOL global databases). These channels are to be subjected to processes and procedures in compliance with international human rights law and data privacy standards.

- New inter-governmental mechanisms and agreements should be explored to enhance international co-operation on border security, especially when it comes to sharing data and relevant expertise.

- States should strive to allocate adequate financial and human resources to establish and run effective API, PNR and biometric systems.

- In pursuing the timely implementation of their obligations stemming from UNSC resolution 2396, participating States should strictly adhere to international human rights law and the rule of law by, for example, foreseeing the opportunity of redress when an infringement to privacy occurs, as well as respecting the special needs of minors. Child-specific patterns should be included when establishing API, PNR and biometric information systems with adequate staffing for child-sensitive cases.

- The protection of personal data is of paramount importance in the context of the security-related provisions of UNSCR 2178 and 2396. OSCE participating States shall pursue the harmonization of personal data protection standards in the context of API, PNR and biometric information, also to overcome potential barriers to co-operation deriving from non-aligned legislation in this field.

To the OSCE PA and OSCE Executive Structures

- Members of the OSCE PA should continue to actively leverage their exposure and competence to promote the full implementation of the counter-terrorism legal framework in compliance with international human rights law. They should also advocate for strengthening international co-operation at all levels, which is vital to deter transnational threats such as terrorism and violent extremism.
- National parliamentary delegations to the OSCE PA should consider appointing dedicated parliamentary focal points to promote engagement on counter-terrorism within national parliaments. A network of focal points would significantly strengthen the coherence of the parliamentary counter-terrorism agenda across the region, vis-à-vis the evolving nature of relevant international counter-terrorism law and policies.
- The OSCE PA should further explore and take full advantage of parliamentary power to inquire national governments to push for the full and coherent implementation of the international counter-terrorism legal framework. Parliamentarians could benefit from clearer guidance and pre-set formats intended to streamline processes through a network of dedicated focal points (see point above).
- The OSCE executive structures should strive to provide—in partnership with the OSCE PA and in close coordination with the UN Office of Counter-Terrorism (UNOCT) and the UN Security Council Counter-Terrorism Committee Executive Directorate (CTED)—continued support to its participating States to effectively respond to the challenges highlighted in this report.

Table 1. Definitions and descriptions of relevant international commitments

What are the relevant commitments that States should implement?	
Advance Passenger Information (API)	An API system is an electronic communication system by which biographic data from a passenger's passport is collected by airlines when checking in and transmitted to border control agencies before a flight's departure or arrival at the airport of destination. If checked against watch-lists and risk indicators, API data provides early warnings to law enforcement officials on FTFs and other suspicious individuals who are attempting to enter their countries. The UNSC has called on States to collect API data since 2014 (Resolutions 2178 and 2309) and the OSCE adopted a politically-binding Ministerial Council Decision in 2016. United Nations Security Council Resolution 2396 (UNSCR 2396) goes further by: (i) deciding that States shall establish API systems and require airlines operating in their territories to provide API to appropriate national authorities; and calling upon States (ii) to promptly report and share any 'hits' with the relevant States and organizations; and (iii) to ensure API data is analyzed by all relevant authorities, with full respect for human rights and fundamental freedoms.
Passenger Name Record (PNR)	PNR data is the information collected from passengers by travel management systems when booking a flight, including contact details and payment information. It is useful for analyzing suspicious patterns or hits associated with these details, as well as highlighting hidden connections between known threats and unknown associates. UNSCR 2396 declared that States shall develop the capability to collect, process and analyze PNR data for the purpose of preventing, detecting and investigating terrorist offences and related travel. The Resolution also mandates the use and sharing of this passenger information by all competent national authorities with full respect for human rights and fundamental freedoms. Lastly, it calls upon regional and international organizations like the OSCE to provide technical assistance and capacity building to States in order to implement such capabilities.
Biometrics	Biometrics are technological tools that can identify someone using human physical characteristics, such as facial and eye recognition. Because fingerprints and other biometric information can be used to validate the identity of travelers and their travel documents, UNSCR 2396 mandates that all States begin collecting biometric information to responsibly detect terrorists and other serious criminals. It also encourages them to share data with other States, INTERPOL and other relevant international bodies. The collection and exchange of biometrics should be carried out in compliance with domestic and international human rights law.

IV. BACKGROUND

Recently, States have strived to bolster border security measures in compliance with international human rights law and the rule of law to prevent the transit of terrorists. Such measures include ensuring that identity documents are not forged, employing evidence-based risk assessments, screening procedures and the collection and analysis of travel data. In December 2017, prompted by the increasingly transnational nature of terrorism and violent extremist groups, including the movements of foreign terrorist fighters (FTFs), the UN Security Council adopted Resolution 2396. The resolution builds upon previous resolutions 2170 and 2178 (2014) and provides greater focus on practical measures to intercept offenders across borders and collect evidence for identifying terrorists.[2]

Domestically, parliamentarians are the backbone in developing counter-terrorism legislation. Their participation in the field increases the effectiveness of these policies that benefit from enhanced accountability mechanisms, good governance and adherence to international law requirements. One of the most important roles played by parliaments is oversight and control of government activity: to hold authorities accountable for their actions, to ensure that governments are fulfilling their obligations, and to prevent and address any abuse of power. In the context of implementing international obligations, such as UNSC Resolutions adopted under Chapter VII of the Charter of the United Nations (i.e. threats to peace), parliaments should also contribute to these efforts by exercising their institutional powers to ensure a swift response to such obligations.

The OSCE PA Ad Hoc Committee on Countering Terrorism (CCT), established in 2017 with the objective to increase the engagement of parliamentarians in countering terrorism across the OSCE region, developed a set of specific sample questions for the national parliaments to submit to their respective executives, in accordance with relevant national procedures in September 2018. This Initiative intends to promote a more coordinated role of OSCE national parliaments in monitoring the implementation at national level of relevant provisions of UNSC Resolution 2396, thereby transferring action at national level and encouraging OSCE governments to re-double their counter-terrorism efforts and carefully consider persisting challenges and the possible need for technical support.

2 Through Resolution 2396, the UN Security Council *inter alia* requires the establishment of API systems in order to detect the air travel of FTFs and other individuals designated by the UN Counter Terrorism Committee, and to introduce PNR capabilities for preventing, detecting and investigating terrorist offenses and related travel. Watch lists of known and suspected terrorists, including FTFs, are to be developed by member States for use by their own security and intelligence agencies in compliance with domestic, international and human rights law. States shall also implement systems to collect biometric data, including but not limited to items such as fingerprints, photographs, and facial recognition in order to responsibly and properly identify terrorists.

V. OVERVIEW OF THE RESPONSES

As of 30 April 2019, 21 (or 36.84%) of the national parliaments of the OSCE participating States responded to the questions posed by the OSCE PA. Respondents are Albania, Azerbaijan, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, France, Georgia, Germany, Greece, Hungary, Italy, the Netherlands, Poland, Romania, Russian Federation, San Marino, Turkey, United Kingdom, and the United States (Figure 1). Together, the responding countries comprise about 975,120,000 citizens, constituting approximately 75.82% of the OSCE participating States' population (1,284,915,982) (Figures 2 and 3).[3]

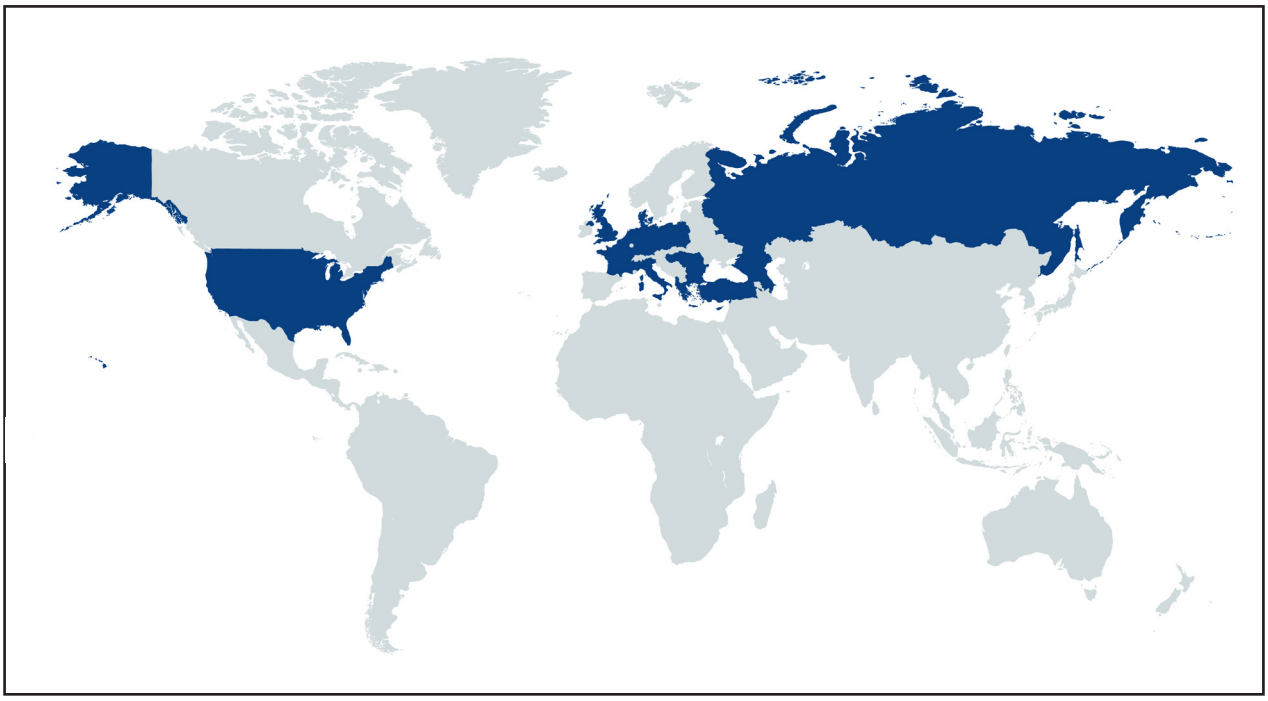


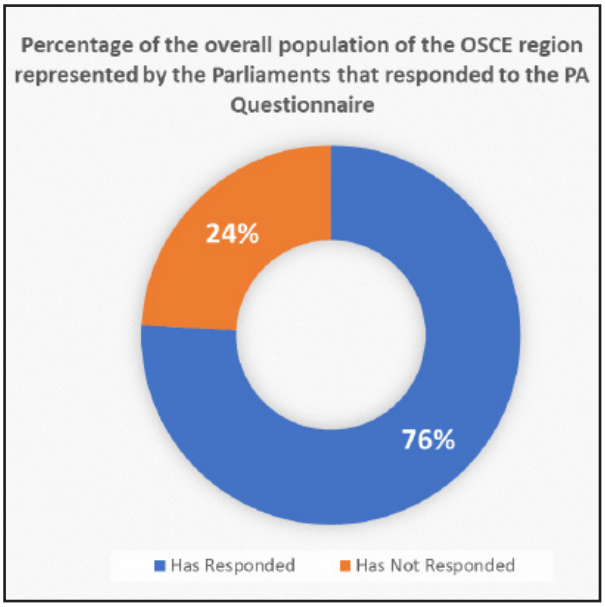
Figure 1. 21 OSCE participating States' parliaments responded to the OSCE PA CCT Questionnaire (Figure Credit: www.MapChart.net)

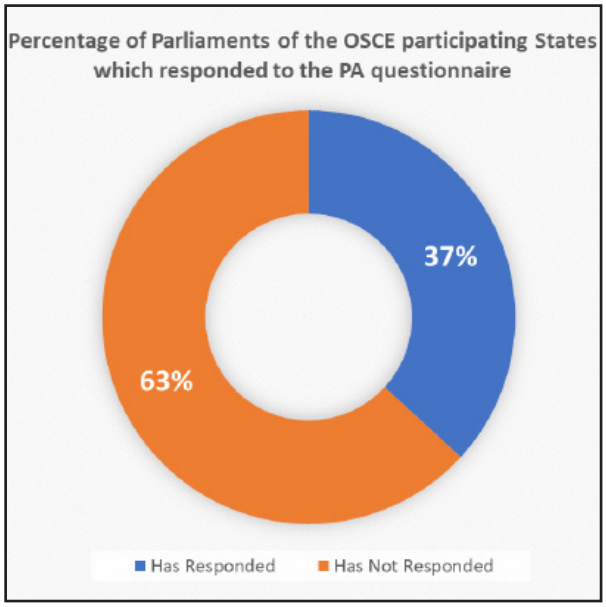
Notably, 13 national parliaments provided information suggesting sufficient capacity to effectively manage the process of collecting, storing, analyzing and sharing API/PNR/biometric information; as to the two national parliaments responding to API and PNR, only one effectively manages both, the other shared info not suggesting a sufficient capacity.

The number of national parliaments which did not respond to the OSCE PA questionnaire, but nonetheless might have posed the questions to the government is unknown, with one exception. Also, in most of the cases, it remains unclear how the questions were posed to the executive powers.[4] Some parliaments responded to the OSCE PA directly, i.e. without submitting the questions to their government. While this approach did not necessarily impact the quality of the information obtained, it did partially alter the purpose of the exercise, which was intended to prompt national parliaments to play a more prominent role in monitoring

3 Estimation based on the statistics as of 2018 elaborated by the International Monetary Fund – retrieved on 25 April 2019 from https://www.imf.org/external/datamapper/LP@WEO/OEMDC/ADVEC/WEOWORLD.

4 It should be noted that national parliaments have not been invited to report about the national procedures used to submit the proposed questions to their executive powers.





Figures 2 & 3. 36.84% (21) of the OSCE participating States—comprising approximately 75.82% of the population—responded to the OSCE PA

compliance with international standards, thereby encouraging their respective governments to follow on their obligations and assess persisting needs and challenges.[5]

Considering the urgency of UNSCR 2396 provisions, several countries have enacted the necessary legal provisions through governmental decrees, pending the parliamentary legislative process. A proper contribution of the legislative assemblies to the law-making process is nonetheless critical for the introduction of policies and practices pertaining to the API, PNR and biometric information systems. *Inter alia*, parliaments should guarantee the congruity of the norms regulating security matters with the national rule of law framework.

The policies and practices shared through this Initiative reflect the multitude of duties and actions that a variety of stakeholders should undertake at the national level in order to set effective API, PNR and biometric information systems. Legislative, data protection, central security/intelligence, customs and borders' authorities must efficiently co-operate with the private sphere – i.e. air carriers and travel agencies. Equally important, due to the transnational nature of terrorism, co-operating with foreign authorities as well as making effective use of international mechanisms and agreements were acknowledged as necessary conditions by most of the respondents.

Several countries are working on integrating and facilitating data-exchange procedures across differing national databases, such as those of customs, borders and law enforcement agencies. Overcoming discrepancies and lengthy processing of data by different national collectors is critical for the effective implementation of API, PNR and biometric systems.

Notably, some of the respondents welcomed the possibility to receive more support in establishing and running modern API, PNR and biometric data management systems. This should rely on consistent guidance to achieve clear technical and procedural standards.

5 For more information, please refer to the OSCE PA Concept Note on the *Initiative to Promote the Implementation of Relevant Commitments on Strengthening Border Security and Information Sharing in the Context of Countering Terrorism and Violent Extremism* of 28 September 2018.

One country emphasized its use of INTERPOL Face Recognition System (FIRST). Considering the impact of the FTF phenomena, FIRST is proving to be an effective tool integrating military findings with prosecutorial evidence to better inform criminal justice activities in FTF-related cases.

A good biometric information system relies on the centralized management of information provided with a modern software. The centralization of such process is designed to facilitate duties at borders for the recognition/matching with suspects' profile, thus significantly easing the workload of officers working under pressing conditions at borders' checkpoints.

As to data privacy concerns in relation to PNR, several respondents stressed the need to immediately depersonalize data when not relevant to law enforcement purposes.

The role of national supreme, or constitutional, courts and - at least for some countries - the jurisprudence of the European Court of Human Rights are critical for complying with international human rights law in the context of setting API, PNR and biometric information systems.

At the EU-level, Directives enacted in 2004 and 2016 determine common rules for the establishment of API and PNR systems as well as biometric data cross-checking for serious crimes based on the European Information Exchange Model (EIXM), set in accordance with the so-called "Prum" Decision of 2008. These norms facilitated EU Member States' efforts to establish coherent API and PNR systems as well as biometric data cross-checking vis-à-vis the requirements set by the UN Security Council in 2017. In principle, this should translate into more effective and timely co-operation at the international level.

The challenges faced during the implementation of API/PNR/biometric systems usually originate from the complex and novel nature of the field, including legal, operational as well as resource and infrastructure-related matters.

Legal challenges

Generally, the urgent and technical nature of obligations stemming from UNSC 2396 risk to bypass the parliamentary law-making process, with executive powers enforcing provisions through decrees and the legislative branch playing a secondary role in the adoption and implementation of the new legislation.

More specifically, setting a pragmatic legal framework that facilitates the necessary co-operation among a diverse range of stakeholders at the national level (e.g. public authorities, air carriers and travel agencies) is a common challenge among many of the respondents.

Ensuring personal data protection for meeting the international human rights and fundamental freedom obligations in relation to the right to privacy is a duty often presenting challenges for the practical and procedural implementation of such norms. Only a few countries seem to have considered establishing effective mechanisms with this regard, including for redress.

A better harmonization of relevant legislation on data protection and the right to privacy would increase opportunities for effective international law enforcement co-operation across the OSCE region (i.e. US-EU co-operation on PNR exchange).

Operational challenges

Countries' law enforcement agencies are challenged by the complex and unique nature of the field. Co-operating with a diverse range of stakeholders (e.g. public authorities vs. the private sector), developing the required IT infrastructure as well as ensuring the adequacy of technical connections with air carriers and IT service providers are the main operational challenges. Equally urgent is the professional development of expert staff in charge of the management of such systems, together with those responsible of customs and border functions, and the timely analysis of collected data.

At the national level, access to relevant data might be hindered when no clear inter-agency operational framework is in place. Also, some countries stressed insufficient biometric data exchange because of limited international co-operation.

The majority of the respondents expressed concerns in relation to the quality and consistency of the engagement with travel companies and airlines, especially small ones. Their concerns centered primarily around the timely transmission of data and their completeness.

Specific child-related measures should be observed by officers who enter in contact with minors. These often imply sound knowledge of relevant national and international protocols. Specific procedures in relation to children were not shared or raised by any of the respondents. [6]

Resources and infrastructural challenges

Several respondents highlighted the lack of IT tools, expertise and human resources dedicated development. The appropriate IT infrastructures, together with reliable and safe technical connections with air carriers and service providers, are critical to initiate the subsequent analytical process.

Many responses indicated technological matters as one of the main factors preventing States to meet the requirements of UNSC Resolution 2396 and to set up and efficiently run modern systems to address API/PNR and biometric data management. Software upgrades and compatibility with hardware IT infrastructure is a common issue. IT software and hardware components present high maintenance and upgrading costs that are critical for the timely connection and data processing between airliners and law enforcement authorities.

A common matter reflected across the respondents is the challenging working conditions of customs and borders' officers who face multiple—and sometimes competing— responsibilities and priorities. Coping with large volume of passengers requires specialized training and capacities. For instance, a respondent revealed that border officers lack expertise for the timely taking and selection of anthropometric photos that can be used for comparisons. Also, investigators lack familiarity with the use of the new IT applications. This impacts on the capacity of detecting suspects, producing evidence in view of judicial proceedings and responding to "alerts" from national and foreign agencies.

6 Measures aimed at preventing terrorism must respect children rights. In accordance with the UN Convention on the Rights of the Child, any assessment of risks posed by a child in this context must be done in the best interest of the child and with the presumption that children are primarily victims of their parents' actions. The *Implementation Handbook for the Convention on the Rights of the Child* and the upcoming UN Office of Counter Terrorism / Counter Terrorism Centre handbook dedicated to the topic of children accompanying FTFs provide an useful reference with this regard.

VI. PROMISING PRACTICES

Several interesting and/or promising practices emerged from the responses received by the Secretariat, which could be considered and possibly even replicated elsewhere, such as:

- the cross-checking of travelers' information with up-to-date operational intelligence data contributing to terrorism risk assessments;
- the development of a national crewmember program to expedite security screening of certain flight crews and attendants for national flights;
- the periodical review of international agreements to foster co-operation with foreign authorities including on the fast-paced issue of border security co-operation;
- the centralized management of the biometric information database and software (i.e. Passenger Information Units) to facilitate officers' duties at borders in relation to recognition of passenger/matching with suspects' profile;
- the immediate depersonalization of PNR data when not relevant to any law enforcement purpose and its storage databases providing adequate safeguards for personal data protection.

Some concrete examples of promising practices are summarized below:

Table 2. Promising practices from respondents of the OSCE PA Questionnaire

Legal and Operational Promising Practices on API/PNR systems	
European Union	At EU-level, Directives enacted in 2004 and 2016 determine common rules for the establishment of API and PNR systems as well as biometric data cross-checking for serious crimes based on the European Information Exchange Model (EIXM), set in accordance with the so-called 'Prum' Decision of 2008. These norms facilitated EU Member States' efforts to establish coherent API and PNR systems as well as biometric data cross-checking vis-à-vis the requirements set by the UN Security Council in 2017. Moreover, the upgrade of the European Schengen Information System (SIS II) standardizes procedures and duties at EU external borders as raising alerts relevant to law enforcement and judicial counter terrorism purposes across EU countries.
Germany	In Germany, data processing of API takes place under the legal provisions contained in the Federal Police Act. Data requests are logged, and the treatment of API data is subject to ongoing audits and specialist supervision. EU 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 was implemented by the German Passenger Name Record Act (June 2017) that includes various provisions for the communication of passenger data in a national, European and international context. 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 adhered to when processing passenger data.
Belgium	The Belgium Passenger Information Unit collects, stores and processes international passenger's data centrally. It includes analysis/input from the Federal Police, the State Security, Military Intelligence, the Customs as well as a support team consisting of legal officers, experts in charge of the relations with the carriers and office managers. Data is analyzed by the operational team in real time, based on previously defined criteria, correlated with various databases of wanted persons and used for targeted searches. Carriers must send the passenger data they are already collecting in the normal course of their business to the BelPIU.

Bulgaria	The Bulgarian National Passenger Unit established a clear mechanism for cooperating with third countries, on a case-by-case basis. Four conditions are to be met simultaneously: 1) the transfer of information is necessary for the prevention, detection, investigation, or prosecution of terrorism-related offences; 2) the recipient is competent to carry out the activities referred to in item 1; 3) the recipient guarantees an adequate level of protection for the scheduled data processing; 4) the recipient agrees not to provide such data to any third country unless said data is necessary for the prevention, detection, investigation and prosecution of offences and the National Unit has given its advance consent following a reasoned request of the competent authority of the third country.
Denmark	The Danish National Police has established a PNR Unit in accordance with national legislation to: a) assess passengers prior to arrival or departure so that relevant information is made available to the national intelligence agencies and Europol; b) react to a motivated request received from a foreign law enforcement authority, Europol, or an international organization. As a part of a preliminary assessment, the PNR Unit can process the PNR-information according to predetermined criteria proportionate to the goal. The PNR-law complies with Directive (EU) 2016/661 of the European Parliament and of the Council of 27 April 2016 on the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.
Hungary	The Hungarian Passenger Information Unit, operating within the Counter-terrorism Information and Criminal Analysis Centre (TIBEK), handles PNR and API data which are consolidated and kept for a retention period of five years. Upon expiry of the retention period the data are erased. After an initial period of six months, the data are depersonalized by masking out relevant details.
Russian Federation	The Russian Federation's Integrated National Transportation Security Information System, managed by the Ministry of Transport, enables prompt detection of individuals involved in terrorist and extremist activities traveling via international or domestic routes.
Turkey	The Turkish Directorate General of Migration Management (DGMM) established the Turkey Passenger Information System in order to receive passenger and crew information effectively and solidly. Turkey Passenger Information System is integrated with infrastructures generating instant, continuous and safe data flow with the view of giving data security top priority. It operatively collects API/PNR data from air carriers.
United States of America	The United States API System (APIS) allows electronic data interchange between carriers to transmit traveler data to Customs and Borders' authorities. The APIS program is recognized by commercial carriers and the international community as the standard for passenger processing and enhanced security in the commercial air and maritime vessel environment. Air carriers are required to transmit the complete manifest for all passengers 30 minutes prior to departure, or by using the APIS Quick Query mode that allows air carriers to transmit passenger information in real time as each passenger checks in for the flight. For vessels departing from foreign ports bound for the United States, vessel carriers are required to transmit passenger and crew arrival manifest data between 24 to 96 hours prior to arrival and transmit APIS data 60 minutes prior to departure from the United States.
	United States' Customs and Border Protection (CBP) agency relies on its Automated Targeting System-Passenger (ATS-P) to perform risk assessments on inbound and outbound international travelers. For inbound flights, ATS-P serves as a tool to assist CBP in making assessments in advance of arrival as to whether an individual should be admitted to the United States. It compares elements of PNR data against terrorist and law enforcement databases to identify potential matches to terrorist identities and wanted criminals.

Legal and Operational Promising Practices on Biometrics	
Denmark	The Danish National Police shares biometric information making use of INTERPOL relevant databases that provide a clear and effective mechanism for comparing data of suspects contained in warrants issued by a foreign authority.
France	France uses INTERPOL Face Recognition System (FIRST) to effectively integrate biometric information found in conflict areas with existing national law enforcement databases in order to detect foreign terrorist fighters. FIRST is a tool integrating military findings with prosecutorial evidence to better inform the criminal justice cycle for FTF-related cases.
Italy	The Italian police authorities have begun using an advanced facial-recognition system that can identify a person by comparing a face against the archive of photographic images (mugshots) in the AFIS of the Ministry of the Interior. This software automates some of the previously manually performed tasks and enables searches to be carried out by uploading a photo into the system, whereupon the software attempts to find a match among the images in the Database. Once it has run the image comparison, the system serves up a set of possible hits and ranks them in order of probability, leaving it to the human operator to verify the results. The Interior Ministry's new system has passed muster with the Data Protection Authority (Doc. No. 9040256), which is of the opinion that it offers adequate safeguards.
The Netherlands	The Dutch Privacy Impact Assessment (PIA) is a process that ensures compliance with domestic and international human rights law. The collecting of cell material for DNA can be justified according to the relevant case-laws of the European Court of Human Rights, particularly in the context of the investigation into crimes of a certain gravity. Restrictive rules must be imposed on the retention of the obtained data in a DNA database.
The United States of America	U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), in collaboration with the Department of Defense (DOD) and CBP, manages the BITMAP program. Through BITMAP, HSI trains and equips foreign counterparts to tactically collect biometric and biographic data on special interest aliens, gang members, and other persons of interest as identified by the host country. Foreign partners share this data with HSI to populate and enhance U.S. government databases and DHS provides this information back to the host countries about these individuals. BITMAP is currently operational in 15 countries. BITMAP enrollments provide U.S. law enforcement and intelligence agencies information on foreign partners' law enforcement officers' encounters with special interest aliens, gang members, and other persons of interest who may pose a potential national security concern to the United States. HSI uses this information to identify and map illicit pathways and emerging trends among criminal organizations outside the United States; associate derogatory information with individuals; and identify known or suspected terrorists, criminals, and other persons of interest.

VII. CONCLUSIONS

The immediacy and urgency of the new measures set primarily through UNSCR 2396 (2017) are a daunting workload for many countries with varying capacities of reaction and effective performance. The transnational nature of terrorism and the increased interdependence of national security policies—as demonstrated by the FTF phenomenon—prompted the urgent enactment of compelling international provisions by the Security Council of the United Nations. Member States are obliged to set effective border security measures and increase information-sharing aiming at robust co-operation mechanisms.

In this context, the OSCE PA Ad Hoc Committee on Countering Terrorism engaged the national parliaments of the OSCE participating States to exercise their institutional powers before their respective executive branches in order to gain insight concerning the actions countries undertook to comply with UNSCR 2396 provisions. Equally important, this effort aimed at identifying prominent legal, operational and procedural challenges hindering the smooth implementation of API, PNR and biometric systems.

This Initiative is meant to complement the work of the OSCE executive structures and support the OSCE participating States in bridging the gap between policy and practice at the national level. Against this backdrop, the political and legislative leverage of parliamentarians across the OSCE region is key to pursue the correct implementation of the counter terrorism provisions set by the United Nations.

If deemed appropriate, similar Initiatives might be replicated with the intent to coordinate OSCE participating States' parliamentary engagement in promoting timely, effective and human rights-compliant counter-terrorism polices and responses at both national and international levels.

Acknowledgments

The OSCE PA Initiative on Border Control and Information Sharing gained strong political momentum thanks to the personal engagement of George Tsereteli and Makis Voridis, President of the OSCE PA and then-Chair of the Ad Hoc Committee on Countering Terrorism respectively, and unfolded with the contribution of all members of the Ad Hoc Committee and the national parliamentary delegations to the OSCE PA, whose action was key to the success of the Initiative.

The present report was prepared by Valerio de Divitiis under the overall guidance of Roberto Montella, Secretary General of the OSCE PA, and the direct supervision of its Senior Advisor, Marco Bonabello, who significantly helped to contextualize the relevancy of this report through numerous suggestions. Valuable support was also provided by OSCE PA staff Sarah Martin, Guido Almerigogna, Stephanie Koltchanov and Nat Parry, especially in terms of editing and proofreading.

Finally, the expert advice of the OSCE Secretariat – and in particular of Simon Deignan and Adrian Carbajo from the Transnational Threats Department – proved critical to ensure the complementarity of this initiative with those of the OSCE executive structures.

List of Acronyms Used in This Report

API..... Advance Passenger Information
CT ..... Counter Terrorism
CCT ..... Ad Hoc Committee on Countering Terrorism of the OSCE PA
CVE ..... Countering Violent Extremism
FTF ..... Foreign Terrorist Fighters
OSCE..... Organization for Security and Co-operation in Europe
OSCE PA..... Organization for Security and Co-operation in Europe Parliamentary Assembly
PNR..... Passenger Name Records
PVE..... Preventing Violent Extremism
SG..... Secretary-General
UN ..... United Nations
UNGA..... United Nations General Assembly
UN CRC..... United Nations Convention on the Rights of the Child
UN CTED..... United Nations Counter-Terrorism Executive Directorate
UNOCT ..... United Nations Office of Counter Terrorism
UNSC..... United Nations Security Council

Annex
Survey Questions submitted to OSCE Parliaments 28 September 2018

Questions to be posed to OSCE governments through national Parliaments on the level of implementation of border security and information sharing provisions of UNSCR 2396

ON API

- What legislative and operational measures have you undertaken to establish an Advance Passenger Information (API) system?
- If such a system has already been put into place, how many cases were detected and promptly notified so far to relevant authorities of other countries and international organizations?
- If such a system has not yet been put into place, why is that the case and how does the Government intend to swiftly make them operational?
- How is the government ensuring that the collection, analysis and sharing of API does not violate relevant human rights and fundamental freedoms?

ON PNR

- What legislative and operational measures have you undertaken to develop your capability to collect, process and analyze Passenger Name Record (PNR) data, with full respect for human rights and fundamental freedoms for the purpose of preventing, detecting and investigating terrorist offences and related travel, and to share such data with relevant States?
- What challenges are you facing in setting such capacity?
- How is the government ensuring that the collection, analysis and sharing of PNR does not violate relevant human rights and fundamental freedoms?

ON BIOMETRICS

- What legislative and operational measures have you undertaken to develop and implement systems to collect biometric data to responsibly identify terrorists?
- What challenges are you facing in setting such capacity?
- Are you sharing this data with other States, with INTERPOL and with other relevant international bodies?
- How do you ensure that the collection and exchange of biometrics is carried out in compliance with domestic and international human rights law?

OSCE PA
Organization for Security and Co-operation in Europe
PARLIAMENTARY ASSEMBLY

www.oscepa.org
osce@oscepa.dk

OSCE PA Headquarters
Tordenskjoldsgade 1
1055 Copenhagen K
Denmark
Tel: +45 33 37 80 40
Fax: +45 33 37 80 30

Vienna Liaison Office
Neustiftgasse 3/8
1070 Vienna
Austria
Tel: +43 676 32 00 517