EASTERN PARTNERSHIP
Panel on Migration and Asylum

Discussion Paper for the Expert Meeting on Information and Communication Technology Use in Migration Management

27-28 October 2016

Riga, Latvia

The Project is funded by the European Union

IOM • OIM
The Project is implemented by International Organization for Migration

www.eapmigrationpanel.org

Compiled by Yuliya Ryzhykh, Laura Scorretti, IOM Ukraine.

This publication has been produced with the assistance of the European Union based on the responses received from the European Union Member States and the Eastern Partnership countries. The contents of this publication are the sole responsibility of their authors and can in no way be taken to reflect the views of the European Union.

Table of Contents

I. Introduction

The European Union (EU) and the Eastern Partnership (EaP) region are all mobile societies. Millions of own nationals and third-country nationals cross internal and external borders every day. Beyond these regular travel flows, in 2015 alone, conflicts and crises elsewhere triggered 1.8 million irregular border crossings at the EU's external borders.

As different migration channels are increasingly used for various reasons, it becomes more and more significant for all the countries concerned to introduce, sustain and develop strategies for sound management of migratory flows, including smart border management. In addition, also security considerations, as one of the aspects of the complex phenomena of migration, must be born in mind and dealt with accordingly. In this context, information and communication technology (ICT) plays a significant role in facilitating sound migration management.

There are a number of information systems at international and EU level that provide immigration officials, border guards and police officers with relevant information on persons. Also in the EU Member States and the EaP countries there are established national information systems providing support for migration management. However, there often are persistent shortcomings in the feeding of the relevant databases and the exchange of information – gaps in the architecture of data management, a complex landscape of differently governed information systems, a fragmented architecture of data management for border control and security.

Where necessary and feasible, the information systems shall be interconnected and interoperable. Simultaneous searches of systems should be facilitated, to ensure that all relevant information is available for smart and effective use of data in order to gain the maximum effect possible. This makes even more relevant to have a cooperation and exchange of good practices, where possible.

The present expert meeting of the EaP Panel on Migration and Asylum aims at connecting experts from the EU and EaP countries involved in development and application of ICT in migration management who will share knowledge and experience on how the modern technologies shape migration management, what new possibilities they bring in for enhancing security, increasing efficiency of the migration and border control agencies, benefitting migrants and travelers, tackling irregular migration, planning national migration policies.

To facilitate and channel the discussion, the present paper was developed as a background and preparatory information basis for the meeting participants. This document provides: (i) overview of the ICT usage in the sphere of migration, including why, where and how the technology is used, challenges associated with it (e.g. interoperability of ICT systems, data protection), and benefits brought by it; (ii) national information systems of the EaP countries and EU Member States, international and EU-level information systems and solutions; and (iii) innovative ICT solutions in the sphere of migration including those related to emergency situations and the current migration crisis.

The discussion paper was prepared based on the answers received from eight EU MS[1] and six EaP countries[2] to a questionnaire (Annex I) specifically designed for this purpose. The questionnaire sent to the participating states comprised seven questions aimed at finding out more on the policies and practices concerning use of ICT in migration management in the EU MS and EaP countries. Other sources of information on the EU and individual countries' policies and practices were also used, where applicable, including regarding those countries who did not submit their inputs.

[1] The following EU MS provided input: the Czech Republic, Estonia, Hungary, Latvia, Lithuania, the Netherlands, Poland and Sweden.

[2] All the EaP countries provided input: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine.

II. Executive summary

ICT in migration management

According to a definition laid out by the UNDP “ICT is basically information-handling tools – a varied set of goods, applications and services that are used to produce, store, process, distribute and exchange information. It includes the “old” ICT of radio, television and telephone, and the “new” ICT of computers, satellite and wireless technology and the internet.” Since ICT, within this definition, is broadly available it influences all the sectors including international migration as such and migration management. In most countries informatization of migration management is indicated in the strategic documents: either those related to migration or to adjoining spheres, e.g. security, home affairs, demography, or to the governance in general, i.e. development of e-government. Implementation of ICT solutions can also be stated at political level. The advantages of ICT use in migration management are self-evident and its potential is large. ICT can be applied in virtually any area, any process in migration management. However, its further expansion can be limited by high costs, insufficient institutional and personnel capacity, strict requirements for data security and human rights safeguards and other factors. Also in the process of ICT use and development authorities are faced with constantly emerging challenges, i.e. lack of interoperability, obsolescence, partial functionality.

National and international information systems in the sphere of migration

Information systems are used at national, regional (EU) and international level. They can serve the following functions: own population registration, registration of border crossings, issuance of identity documents, issuance of visas, resident and work permits to foreigners, registration of place of stay of foreigners, registration of asylum applications, detection of wanted persons, identification of forged documents etc. Information systems can have inbuilt functions for data analysis, generation of statistical data, reporting, forecast, information exchange, provision of administrative services. Biometrics is widely used in travel documents and migration-related information systems to fight identity fraud, to prevent the wrongful or duplicate issuance of travel or ID documents.

Innovative ICT solutions in migration management, including those related to emergency situations and the current migration crisis

Innovative solutions include introduction of ground-breaking equipment, software, creation of new databases, but also original organizational approach to work with ICT, expanding functionality of the existing systems, establishing new links between them. In the EU the European Commission proposed the “Smart Borders” package which includes a new large-scale IT system for registering entries and exits of third-country nationals. Programmes for registered frequent travelers and for obtaining a pre-travel authorization are also being contemplated. INTERPOL is introducing an innovative solution which allows air-carriers to conduct advanced travel document checks in real time. Border guards and other law-enforcement authorities clearly see advantages of mobile devices for identity checks and registration of migrants. Some more traditional means – like Skype and smartphone apps – are being applied in a new context in migration management for interaction with migrants, refugees and other users. Mobile call data is used for tracking migration patterns including the population displacement for prompt decision making. Many countries introduced not only technical but also organizational changes improving the interagency cooperation in the sphere of ICT as well as monitoring and reporting by means of ICT.

III. ICT in migration management

According to a definition laid out by the UNDP "ICT is basically information-handling tools – a varied set of goods, applications and services that are used to produce, store, process, distribute and exchange information. It includes the "old" ICT of radio, television and telephone, and the "new" ICT of computers, satellite and wireless technology and the internet."[3] Since ICT, within this definition, is broadly available it influences all the sectors including international migration as such and migration management.

A. National framework for introduction and regulation of ICT in migration management

In most countries informatization of migration management is indicated in the strategic documents: either those related to migration or to adjoining spheres, e.g. security, home affairs, demography, or to development of e-government in general. The following strategic documents were adopted in the participating countries:

- migration strategy or its concept (***Armenia***, ***Georgia***, ***Moldova***, ***Ukraine***, ***the EU MS***)

  Application of modern approaches to the information and communication technologies in migration management is one of the priority areas of the 2016-2020 Migration Strategy of ***Georgia****.*

  Migration management information systems in ***Ukraine*** *are developed on the base of approved strategic documents on migration policy matters.*

  According to the ***EU's*** *European Agenda on Migration, more efficient border management also implies making better use of the opportunities offered by IT systems.*

- on informatization of the society and the government (***Azerbaijan***, ***Belarus***, ***Georgia***, ***Latvia***, ***Moldova***, ***Poland***)

  In ***Belarus****, the State Program for Development of Digital Economy and Information Society for 2016-2020 was adopted. In particular, the Program covers issues pertaining to development of the national Integrated Processing System with introduction of biometric ID documents and e-Visa Information System; improvement of information and communication infrastructure of border protection and border control information systems.*

  In general regarding the ICT, Information Society Development Guidelines for 2014 - 2020 were approved by the Cabinet of Ministers of ***Latvia*** *and they are the current National e-Government strategy. Currently there is no specific strategic document aimed to ICT in migration management.*

- in the sphere of security and justice (***the EU MS***)

[3] Information and Communication Technologies for Development, UNDP Essentials No. 5, UNDP Evaluation Office, September 2001.

> ***Hungary*** *supports to follow this issue in the framework of the "Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area" which has been agreed in the JHA Council and covers some possible actions in this area.*

Development of ICT can also be stated at political level.

> *The **Czech Republic** considers the usage of information and communication technologies essential in the field of migration management. In this regard the Czech Republic takes advantage of its membership in the EU, where the main IT systems are developed and the know-how is shared among the MSs; in case of the Czech Republic, since 1991 when the association agreement was concluded. The European Agenda on Migration and the European Agenda on Security can be considered as the most relevant strategic documents.*
>
> *The **Swedish Government** has put forward an IT-political goal: "Sweden shall be best in the world on using digitalised facilities". In order to achieve this goal three sub-targets have been established: (i) an easier everyday life for Swedish citizens; (ii) higher quality and effectivity in the operation; (iii) a more open administration supporting innovation and participation. These are the goals that guide the development of ICT solutions within the SMA.*

The countries' concrete plans for broadening use of ICT in migration management are described in the table:

Armenia	-
Azerbaijan	-
Belarus	Introduction of biometric ID documents and e-Visa Information System
Czech Republic	Development of the mobile technologies that could be used for performing registration and checks of the irregular migrants anywhere on the territory of the country, the biometric data included, in specific circumstances
Estonia	Upgrading of the existing IT-systems to provide faster and better person identification, introduction of the Passenger Name Records and the Entry-Exit System
Georgia	Establishment of the Unified Migration Analytical System (UMAS) intended for analytical and statistical purposes and not for administrative functions
Hungary	-
Latvia	Working towards digitalization of processes
Lithuania	Implementation of ICT projects in migration management: 1. "Effective Migration Management" (MIGRIS): improvement of the quality of migration services and migration management procedures by creating electronic migration files management system. 2. "Creation of Electronic Migration Services": creation of a tool for providing electronic migration services, to be integrated with MIGRIS
Moldova	Implementation of the facial recognition system (started in September 2016)
Netherlands	-
Poland	Further development of the Border Guard ICT systems; creating Advanced PI for interoperability
Sweden	Procurement of the facial recognition system equipment that will be used by the SMA ID unit and perhaps also in the case management systems (legal amendments are required)
Ukraine	Further development of ICT systems

Functioning of ICT requires solid legal basis. The table in Annex II provides information on national legal framework for use of ICT solutions in migration management in individual states.

B. Advantages and challenges

The advantages of ICT use in migration management are self-evident and its potential is large. ICT can be applied in virtually any area, any process in migration management. However, its further expansion can be limited by such factors as high costs, insufficient institutional and personnel capacity, strict requirements for data security and human rights safeguards and others. Also in the process of ICT use and development the authorities are faced with constantly emerging challenges, i.e. lack of interoperability, obsoletion, incomplete functionality etc.

Advantages

The countries provided an exhaustive list of advantages they experienced from the ICT use:

- better formulation of migration policy (***Azerbaijan***, ***Poland***);
- improved management of migration flows, including time and human resources reduction (***Armenia***, ***Azerbaijan***, ***Belarus***, ***the Czech Republic***, ***Georgia***, ***Hungary***, ***Latvia***, ***the Netherlands***, ***Poland***);
- improved data collection and its quality, statistics and reporting (***Armenia***, ***Azerbaijan***, ***Georgia***, ***the Netherlands***, ***Moldova***, ***Poland***);
- reduced risk of human errors (***Latvia***, ***Moldova***);
- facilitation of work, reduction of administrative burden (***Lithuania***, ***Moldova***, ***Sweden***);
- improved protection of migrants' rights and freedoms (***Azerbaijan***);
- better services for applicants (***Poland***, ***Sweden***, ***Ukraine***);
- improved protection of state security (***Azerbaijan***, ***the Czech Republic***);
- more effective identification of abuse (***Hungary***, ***Poland***);
- improved interagency data exchange (***Azerbaijan***, ***Hungary***, ***Latvia***, ***Moldova***, ***Sweden***, ***Ukraine***);
- substantially higher level of person identification and higher comprehensiveness of information about persons (***Belarus***, ***Estonia***, ***Hungary***, ***Poland***, ***Sweden***, ***Ukraine***).

Challenges

The European Commission's Communication "Stronger and Smarter Information Systems for Borders and Security" is analyzing the shortcomings related to information systems that impede the work of the relevant national authorities. The main shortcomings are: (a) sub-optimal functionalities of existing information systems, (b) gaps in the EU's architecture of data management, (c) a complex landscape of differently governed information systems, and (d) a fragmented architecture of data management for border control and security. Also better information exchange was highlighted as a key priority in the European Agenda on Security.

The existing information systems in the EU for border management and internal security cover a wide range of functionalities. Nevertheless, there are still shortcomings in the functionalities of existing systems. When looking at border control processes applicable to different categories of travelers, it becomes clear that there are shortcomings in some of these processes and between the respective information systems used for border controls. Likewise, the performance of existing tools for law enforcement needs to be optimized. This calls for consideration of action to improve existing information systems.

Moreover, there are gaps in the EU's architecture of data management. Issues remain for border controls of specific categories of travelers, such as third-country nationals holding a long-term visa. Also, there is an information gap prior to arrival at the borders as concerns third-country nationals who are exempt from holding a visa. Consideration should be given to whether there is a need to address these gaps by developing additional information system where necessary. Border guards and notably police officers face a complex landscape of differently governed information systems at EU level. This complexity creates practical difficulties specifically as to which databases should be checked in a given situation. Moreover, not all Member States are connected to all existing systems.

The current complexity of acceding information systems at EU level could be reduced by establishing a single search interface at national level which respects the different purposes for access.

The current EU's architecture of data management for border control and security is marked by fragmentation. This is caused by the various institutional, legal and policy contexts in which the systems have been developed. Information is stored separately in various systems that are rarely interconnected. There is inconsistency between databases and diverging access to data for relevant authorities. This can lead to blind spots notably for law enforcement authorities, as it may be very difficult to recognize connections between data fragments. It is therefore necessary and urgent to work towards integrated solutions for improved accessibility to data for border management and security, in full compliance with fundamental rights. For that, there is a need to initiate a process towards the interoperability of existing information systems.

The countries listed the following problems and challenges experienced at national level:

- lack of common standards for different information systems managed by different agencies (***the Netherlands***, ***Moldova***, ***Poland***, ***Sweden***, ***Ukraine***);
- lack of coordination of the ICT development process in different agencies (***Hungary***);
- gaps between the legislative developments and ICT (***Poland***) or vice versa, when legal or procedural norms do not keep up with the ICT developments (***Lithuania***);
- risks to (personal) data security (***Georgia***);
- ensuring high quality of data (***Latvia***).

Full respect of fundamental rights and data protection rules is an essential precondition to addressing any of the above challenges. Compliance with fundamental rights requires well-designed and correctly-used technology and information systems. Technology and information systems can help public authorities to protect the fundamental rights of citizens. Biometric technology can reduce the risk of mistaken identities, and of discrimination and of racial profiling. It can also contribute to addressing protection risks for children such as children going missing or falling victims of trafficking, provided it goes hand in hand with fundamental rights safeguards and protection measures. It can reduce the risk of people being wrongfully apprehended and arrested. It can also contribute to increasing the security of citizens residing in the Schengen area as it will help in the fight against terrorism and serious crime. The existence of large-scale information systems also implies potential privacy risks, which need to be anticipated and addressed appropriately. The collection and use of personal data in these systems has an impact on the right to the privacy and the protection of personal data. All systems need to comply with data protection principles and the requirements of necessity, proportionality, purpose limitation and quality of data. Safeguards must be in place to ensure the rights of the data subjects in relation to the protection of their private life and personal data. Data should only be retained for as long as necessary for the purpose for which they were collected. Mechanisms ensuring an accurate risk management and effective protection of data subjects' rights need to be foreseen.

Safeguards such as compartmentalizing data within one system and specific access and use rules for each category of data and user should ensure the necessary purpose limitation in integrated solutions for data management. This opens a way towards the interoperability of information systems accompanied by the necessary strict rules on access and use without affecting the existing purpose limitation.

“Data protection by design” and “Data protection by default” are now principles of EU data protection rules. When developing new instruments that rely on the use of information technology, the Commission will seek to follow this approach. This implies embedding personal data protection in the technological basis of a proposed instrument, limiting data processing to that which is necessary for a specified purpose and granting data access only to those entities that “need to know”.

While answering the questionnaire some countries emphasized the legal aspects of the personal data protection (***Georgia***, ***Latvia***, ***Lithuania***), while others (***Belarus***, ***Hungary***, ***the Netherlands***, ***Ukraine***) focused on description of technical means and organizational arrangements.

> *In **Belarus** data protection in the course of information exchange operations between the systems is ensured by relevant hardware and software means and by organizational/technical arrangements.*
>
> *Information systems used in migration management in **Georgia** collect different personal data, including biometrics, according to internationally acknowledged standards and requirements of the Georgian Law on Personal Data Protection.*
>
> *The employees of the **Lithuanian** Residents Register management bodies shall sign commitments that they will preserve the secrecy of personal data and act without prejudice to the Law on Legal Protection of Personal Data.*
>
> *The working model in the **Netherlands** is that all shared data is available to all connected parties. Decisions on what data is shared is made via a structured analysis and development process on digitization and signed off at the highest level in the organization. The joint Chief Information Security Officers of all connected parties decide upon data protection and security issues.*

The summary of advantages and challenges experienced or envisaged by the countries is provided in Annex III.

Possible topics for discussion	*How cost-effectiveness of ICT solutions is achieved? What are the sources of funding for ICT solutions in migration management in your country?*
	Did any significant failure associated with ICT use occur before (interruption of processes and provided services, lost data, leaked personal data, breach of person’s rights) and if yes, what measures were taken to mitigate the consequences and fix the problem for the future?

IV. National and international information systems used for migration management

A. National information systems

As it was noted above, ICT solutions can be applied in any area of migration management, information systems can potentially be tasked to collect, process, store and exchange any type of migration-related data. Decision makers identify where the use of ICT is most required depending on their country’s migration situation, what purpose it needs to serve. Thus, ICT can be used for own population registration, registration of border crossings, issuance of identity documents, issuance of visas, resident and work permits to foreigners, registration of place of stay of foreigners, registration of asylum applications, detection of wanted persons, identification of forged documents etc.

Information systems and databases can have inbuilt functions for data analysis, aggregation of statistical data, reporting, forecast, information exchange, provision of administrative services.

IOM's Migration Information and Data Analysis System (MIDAS)

In order to support governments to meet today's complex migration and border management challenges, IOM has developed a border management information system: the Migration Information and Data Analysis System (MIDAS)[4]. MIDAS has been designed to equip states that have no or inadequate data capture system in place with the operational means to advance their current migration management systems.

The system enables states to collect, process and store traveler's information, including bio-data and biometrics, at entry and exit border points for the purpose of traveler identification, authentication of travel documents, data collection and analysis. Compliant with international standards, MIDAS is a high-quality, affordable system, suitable for installation also in remote areas. MIDAS contributes in improving the monitoring of border movements and helps develop evidence-based migration and border management policies. MIDAS has been adopted in 19 countries in Africa and Central and South America.

The participating countries provided a good overview of the national information systems and databases with their functionality description. Annex IV contains information on the said systems grouped according to their main purpose.

Use of biometrics

Given that biometrics has a broad impact on migration management, biometric functionality is more often used by states in travel documents and migration-related information systems and databases. In addition, biometric solutions are also:

- incorporated into document issuance processes to prevent the wrongful or duplicate issuance of travel or ID documents;
- used as part of the visa application process. Some countries even have plans to include biometric identifiers in/on visas themselves;
- deployed at certain checkpoints to assist officials in matching entry and exit records;
- used to manage the provision of services to migrant populations (biometrically-enabled identification cards that allow migrants to access benefits while reducing benefit fraud).

The following biometric identifiers are used by the countries in migration management:

Biometric Country	Fingerprints	Iris	Facial image/Facial recognition system (FRS)	Other
Armenia	+	-	+/-	Signature
Azerbaijan	+	-	+/-	-
Belarus	-	-	-	-
Czech Republic	+	-	+/-	-
Estonia	+	-	+/-	-
Georgia	+	-	+/-	-
Hungary	+	-	+/-	-
Latvia	+	-	+/+	-
Lithuania	+	-	+/-	Signature
Moldova	+	-	+/+ (implementation started in September 2016)	Signature
Netherlands	+	-	-	-

[4] https://www.iom.int/sites/default/files/our_work/DMM/IBM/updated/09-IBM-Factsheet-MIDAS-EN-2016.pdf

Poland	+	-	+/-	-
Sweden	?	-	?/- (procurement of FRS equipment is ongoing)	?
Ukraine	+	-	+/-	Signature

B. EU-level information systems

As envisaged by a European Agenda on Migration[5] managing the EU external borders more efficiently also implies making better use of the opportunities offered by IT systems and technologies. The existing information systems in the EU for border management and internal security each have their own objectives, purposes, legal bases, user groups and institutional context. Together they provide a complex pattern of relevant databases. The **three main centralized large-scale information systems** developed by the EU are (i) the Schengen Information System (SIS) with a broad spectrum of alerts on persons and objects, (ii) the Visa Information System (VIS) with data on short-stay visas, and (iii) the EURODAC system with fingerprint data of asylum applicants and third-country nationals who have crossed the external borders irregularly. These three systems are complementary, and – with the exception of SIS – primarily targeted at third-country nationals. The systems also support national authorities in fighting crime and terrorism[6].

The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) was established in 2011. The Agency is responsible for the operational management of the second-generation SIS – SIS II, VIS and EURODAC. The Agency may also be made responsible for the preparation, development and operational management of other large-scale IT systems. The first such system – pending approval of the relevant legislative proposals – may be Entry-Exit System (EES), proposed as part of the European Commission's **Smart Borders package** which is expected to be implemented by 2020, again addressing third-country nationals.

Schengen Information System (SIS)

SIS is the largest and most widely used information exchange platform on immigration and law enforcement[7]. It is a centralized system used by **25 EU Member States**[8] and **four Schengen associated countries**[9], currently containing 63 million alerts. These are entered and consulted by competent authorities, such as police, border control and immigration. It contains records on third-country nationals prohibited to enter or stay in the Schengen area as well as on EU and third-country nationals who are wanted or missing (including children) and on wanted objects (firearms, vehicles, identity documents, industrial equipment, etc). The distinctive feature of SIS in comparison with other information sharing instruments is that its information is complemented by an **instruction for concrete action** to be taken by officers on the ground, such as arrest or seizure. SIS checks are mandatory for the processing of short-stay visas, for border checks for third-country nationals and, on a non-systematic basis, for EU citizens and other persons enjoying the right of free movement. Moreover, each police check on the territory should include an automatic check in SIS.

[5] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/background-information/docs/communication_on_the_european_agenda_on_migration_en.pdf

[6] Law enforcement access to VIS and EURODAC can be exercised under limited conditions due to the fact that law enforcement is an ancillary objective of those systems. Concerning VIS, Member States have to designate an authority responsible for controlling law enforcement access and the police must provide evidence that their access is necessary for criminal investigations. Concerning EURODAC, the investigative authority needs to search the national AFIS, Prüm and the VIS before being given access to EURODAC.

[7] SIS II – a more advanced version of the SIS – was launched in April 2013 with enhanced functionalities.

[8] All, except Ireland, Cyprus, Croatia.

[9] Switzerland, Liechtenstein, Norway, Iceland.

Bulgaria and ***Romania*** currently operate the SIS only for the purpose of law enforcement cooperation. They will start using the SIS for the purpose of external border control as soon as the decision for lifting the internal border checks has entered into effect.

Cyprus and ***Croatia*** are enjoying a temporary derogation from joining the Schengen area. They are currently carrying out preparatory activities to integrate into the SIS.

The ***United Kingdom*** operates the SIS within the context of law enforcement cooperation. ***Ireland*** is carrying out preparatory activities to integrate into the SIS for the purpose of law enforcement cooperation.

Hungary, ***Latvia***, ***Sweden*** mentioned use of **SIRENE** which stands for Supplementary Information Request at the National Entries. Each state operating the SIS has set up a national SIRENE Bureau, operational 24/7, that is responsible for any supplementary information exchange and coordination of activities connected to SIS alerts. In order to ensure prompt, confidential and efficient follow-up of cases, communication is accomplished through the structured exchange of standardized forms via a secure network.

Visa Information System (VIS)

The VIS is a centralized system for the exchange of data on short-stay visas between Member States. It processes data and decisions related to applications for short-stay visas to visit, or to transit through, the Schengen area. All the consulates of the Schengen States (around 2,000) and all their external border crossing points (in total some 1,800) have been connected to the system. The VIS contains data on visa applications and decisions, as well as whether issued visas are revoked, annulled or extended. It currently contains data on 20 million visa-applications and, at peak-times, it handles over 50,000 transactions per hour. Each visa applicant provides detailed biographical information, a digital photograph and ten fingerprints. As such, it is a reliable means to verify the identity of visa applicants, to assess possible cases of irregular migration and security risks, and to prevent “visa shopping”. At border-crossing points or within the territory of the Member States, the VIS is used to verify the identity of visa holders by comparing his/her fingerprints with the fingerprints stored in the VIS. This process guarantees that the person that applied for the visa is the same person as the one crossing the border. A fingerprint search in the VIS also allows the identification of a person who applied for a visa in the last five years and who may not carry identity documents.

In their answers to the questionnaire, ***Hungary*** and ***Poland*** referred to **VIS Mail** which is the platform that supports the exchange of prior consultation (Visa Code Article 22), VLTV (Visa with Limited Territorial Validity) and ex-post visa notification (Visa Code Articles 25.4 and 31) messages, between the Member States, via the VIS infrastructure.

EURODAC

EURODAC (European Dactyloscopy) contains fingerprints of asylum applicants and third-country nationals crossing irregularly the Schengen external borders. Its primary purpose currently is to determine which EU country is responsible for the processing of an asylum application, in line with the Dublin Regulation. It is available at border crossing points, but unlike SIS and VIS it is not a border management system.

Fingerprints of irregular migrants entering the EU unlawfully are taken at border crossing points. These are stored in EURODAC to verify the identity of the person in case of a future asylum application. Immigration and police authorities can also compare fingerprint data from irregular migrants found in EU Member States to check if they have applied for asylum in another Member State. Law enforcement authorities and Europol are also entitled to search EURODAC to prevent, detect or investigate a serious crime or terrorist offence.

Fingerprint registration of asylum seekers or irregular migrants in a centralized system allows the identification and monitoring of their secondary movements[10] within the EU, until an application for international protection has been submitted or a return decision has been issued (in the future, with a corresponding alert in SIS). More generally, the identification and monitoring of irregular migrants is required to ensure re-documentation by authorities in their countries of origin and thus facilitates their return.

The following data are registered in the system: the Member State of origin, the digital fingerprint, the sex and the reference number used by the Member State of origin.

DubliNet

A secure electronic network of transmission channels between the national authorities dealing with asylum applications, called DubliNet, became operational on 1 September 2003 in the EU Member States plus Norway and Iceland. It is consistent with EURODAC. The two involved Member States can exchange personal data through DubliNet that differ from EURODAC data, like name, date of birth, nationality, photo, details on family members and in some cases addresses.

DubliNet uses services offered by the IDA (interchange of data between administrations) programme to guarantee a high level of security to the protection of data pertaining to asylum seekers.

DubliNet has simplified procedures to the benefit of national administrations by identifying one single national access point the participating state.

> *While answering a question regarding authorities which are entitled to use DubliNet, the **Netherlands** indicated that DubliNet is used exclusively by 16 authorised officers of the logistic and administrative service unit (with permanent appointments) of the Dublin Unit of the Dutch Immigration and Naturalization Service (IND). 15 Officers are authorised for preparing the DubliNet forms in PDF format but they are not authorised for sending those. Only one officer of the service unit is authorised for sending and receiving data through the computer giving access to DubliNet[11].*

FADO

FADO (False and Authentic Documents Online) has been set up to facilitate exchanges of information between EU Member States. It provides for the rapid validation, storage and exchange of information on genuine and false documents by computerized means. Distinguishing between false and authentic documents is also important for citizens, organizations and businesses. Therefore, the EU has made available a Public Register of Authentic Identity and Travel Documents Online (PRADO).

The ***Czech Republic*** mentioned iFADO – Intranet False and Authentic Documents Online – which contains the most important information for document checking, derived from FADO. It is accessible for competent control authorities only.

PRADO

PRADO (Public Register of Authentic Travel and Identity Documents Online) is a multilingual site with information on authentic identity and travel documents. It includes information on the validity and on

[10] For example, refugees arriving in Greece with no intention of making an asylum application in Greece but travelling further to other Member States over land.

[11] https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/int/med_20101004_dublinet_questionnaire.pdf (as of 2010)

other legal aspects, as well as technical descriptions (including descriptions of some of the most important security features) of these documents.

PRADO is hosted in the Directorate-General Justice and Home Affairs. Document experts in all EU Member States and in Iceland, Norway and Switzerland provide and select the information to be released to the general public via PRADO. Most of the text entries in PRADO documents are standardized descriptions which are translated automatically into the 24 supported official languages of the EU. Free-text descriptions are translated by specialized linguists.

C. Other international information systems (beyond the EU)

Advance Passenger Information (API)

The main purpose of Advance Passenger Information (API) is to facilitate travel for bona fide passengers by allowing for early registration and processing of travelers, thus reducing delays at the border. API involves agreement between countries, and between airlines and governments, permitting passenger manifests to be electronically sent by the airlines ahead of flights to the immigration authorities of the country of destination for pre-checking before arrival. API is limited to a relatively small number of core data elements. API data consists of information held in a travel document, and relates to a traveler’s full name, date of birth, nationality, number and type of travel document, as well as information on the border crossing point of departure and entry as well as transportation details. This information can therefore be collected by airlines at airport check-in. Once the API has been collected, it is transmitted to the country of destination, where it is analyzed and checked against databases and alert lists. The information then becomes available to immigration and customs officials at the airport of arrival. Ultimately, this leads to enhanced security, since officials have more time to identify those travelers who may pose a threat and can consequently focus their attention on these passengers upon arrival. This also means faster processing of the majority of passengers who do not need to be singled out for closer inspection and whose data has already been captured through the API system. Upon arrival, it may suffice for them to just verify their identity.

> *In **Poland** API (arrivals direction) became a helpful tool to prevent/avoid terrorist threats and control the situation of influx of migrants up to the current migration crisis.*

Passenger Name Records (PNR)

A PNR is created when a travel booking is made for a passenger and is held in the travel agent’s or airline’s reservation system. Along with the names and ticket details of the passenger, PNR typically includes information on the date and method of ticket payment, contact details such as address, telephone number or e-mail, seating information and other special requirements. However, the exact number of details held on passengers in the PNR varies between carriers.

A number of countries have introduced – or are planning to introduce – requirements for PNR since it can make a valuable contribution towards efforts aimed at preventing terrorism and serious crime. PNR data is sent ahead of flight departure and is analyzed and checked against the relevant watch lists of the country of destination.

It is the relatively extensive information on passengers contained in the PNR which makes it attractive to authorities responsible for security. However, it is also this that has given rise to concerns about privacy and data protection. API has encountered fewer objections as the data transmitted is essentially limited to that contained in the machine-readable zone of passports, information which would be available to border and customs authorities at border control posts. PNR, however, involves additional and more personal information and is consequently more intrusive in terms of privacy.

Questions often raised include the number of data elements to be submitted, as well as the amount of time the information may be retained by authorities.

Presently some EU Member States already have a PNR system (e.g. the ***UK***), while others have either enacted legislation or are currently testing PNR data systems. Most EU countries use PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime in a non-systematic way or under general powers granted to the police or other national authorities.

The text of the EU Directive regulating the use of PNR data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, first proposed in 2011, was approved by the Council of the EU in April 2016. Once it enters into force, Member States will have two years to transpose the legislation into their national laws.

Stolen and Lost Travel Documents (SLTD)

INTERPOL's database of Stolen and Lost Travel Documents (SLTD) is a central database on passports and other travel documents that have been reported stolen (including stolen blank passports) or lost by the issuing authorities to INTERPOL. It enables INTERPOL National Central Bureaus (NCBs) and other authorized law enforcement entities – such as immigration and border control officers – to ascertain the validity of a travel document (passports, identity documents, visas) in seconds.

The SLTD database was created in 2002, following the 11 September 2001 terrorist attacks in the USA, in order to help member countries secure their borders and protect their citizens from terrorists and other dangerous criminals using fraudulent travel documents.

Starting with a few thousand records from just 10 countries, the SLTD database has grown exponentially. 174 countries contribute to the database which contains more than 68 million records. From January to September 2016 it was searched more than 1,243,000,000 times, resulting in more than 115,000 positive responses, or "hits".

In the EU: (i) travel documents reported lost or stolen to the authorities of countries participating in SIS are entered both in SLTD and SIS; (ii) travel documents of all third-country nationals and persons enjoying the right of free movement should be verified against SLTD; (iii) all border control posts have to be connected to SLTD; (iv) in-country law enforcement searches in SLTD would generate additional security benefits.

Nominal data (NOM) and Notices

INTERPOL's Nominal database (NOM) contains more than 163,000 records on fugitives, suspected criminals, persons linked to or of interest in an ongoing criminal investigation, persons and entities subject to UN Security Council Sanctions, potential threats, missing persons and dead bodies, with their criminal histories, photographs, fingerprints etc. The system of Notices is used to issue international alerts for the mentioned subjects. Notices are international requests for cooperation or alerts allowing police in member countries to share critical crime-related information.

In the case of Red Notices, the persons concerned are wanted by national jurisdictions for prosecution or to serve a sentence based on an arrest warrant or court decision. INTERPOL's role is to assist the national police forces in identifying and locating these persons with a view to their arrest and extradition or similar lawful action.

In addition, Notices are used by the United Nations, International Criminal Tribunals and the International Criminal Court to seek persons wanted for committing crimes within their jurisdiction, notably genocide, war crimes, and crimes against humanity.

Georgia, ***Moldova***, ***Poland***, ***Ukraine***, among other countries, have access to the NOM database.

Electronic Documentation and Information System on Investigation Networks (Edison)

Edison provides examples of genuine travel documents in order to help identify fakes. It contains images, descriptions and security features of genuine travel and identity documents issued by countries and international organizations.

The Edison database, also accessible through INTERPOL's secure global communications network, allows frontline border officers to access detailed examples of genuine travel documents, in order to detect fakes.

Document Information System for Civil Status (DISCS)

DISCS is a document information system for civil status documents. These include various types of certificates – of birth, marriage, death etc – that say something about the civil status of a person. DISCS can be considered as a younger cousin of Edison.

This knowledge system has been developed in the Netherlands for all government agencies that use civil status documents in their primary processes. The most important of these are municipalities, the Royal Netherlands Marechaussee (police corps with military status) working at application centres for asylum-seekers, the Dutch Social Insurance Bank, Dutch embassies abroad and the IND.

The IND was originally the only party in charge of filling the system with documents. In 2006, the Canada Border Services Agency joined the operation as partner, as did the Dutch Foreign Ministry, which will enter information of a more tactical nature, such as information on issuing parties, state emblems, countries in general and so forth. Various foreign partner organizations are also either already working with the system, or else have expressed interest in it. The use of DISCS helps to increase expertise in detecting fraud with civil status documents in the processes involving aliens.

Azerbaijan and ***Georgia*** gained access to the DISCS.

Detailed information regarding access of the countries to the EU-level and international databases is contained in Annex V.

Possible topics for discussion	*What other country's experience/ICT solution do you want to learn about or adopt?*
	Despite the progress already achieved in your country what areas in migration management are still greatly requiring ICT solutions?
	Which international information systems appeared most effective in your country? Please, illustrate with examples how access to particular international information systems improved your national authorities' work.

V. Innovative ICT solutions in migration management, including those related to emergency situations and the current migration crisis

Innovative solutions can include introduction of ground-breaking equipment, software, establishment of new systems and databases, but also original organizational approach to work with ICT, expanding functionality of the existing systems, establishing new links between them.

The following are examples of innovative ICT solutions:

EU “Smart Borders” package

The package, first proposed in 2013, focuses on implementation of more modern and efficient border management by using state-of-the-art technology. The Entry-Exit System (EES), a proposed new large-scale IT system which forms a central component of the package, would provide information on over-staying third-country nationals, thereby aiding in the fight against irregular migration while also facilitating border crossings by enabling deployment of automated technologies. Current timetables indicate a go-live of the new system in 2020 should the co-legislators provide their approvals.

A Registered Traveller Programme (RTP) was another element of the Package proposed in 2013 but withdrawn in April 2016. The RTP would have a purpose of facilitating the crossing of the external borders of the EU by frequent, pre-screened and pre-vetted third-country travelers.

EU Travel Information and Authorisation System (ETIAS)

The European Commission is currently preparing a proposal to introduce a new electronic pre-screening programme for visa-exempt visitors intending to travel to the EU – ETIAS. It is likely to propose the instigation of a US-style ESTA (Electronic System for Travel Authorisation, in use since 2009) as part of the Entry-Exit System (EES) to the Schengen Zone. The scheme would affect all 26 nations belonging to Schengen.

Under ETIAS, visa-exempt travelers would be required to apply for an authorization to travel before departing from their home country. This would be done quickly and easily online and a fee would be charged. By submitting personal and passport information to the authorities, travelers can be screened and assessed to see if they are eligible to enter the country without applying for a full visa. Anyone not holding ETIAS approval may be declined boarding of an aircraft or commercial vessel, or refused entry on arrival at the border.

Authorization differs from visa, inasmuch as visas are more detailed and time-consuming to apply for, particularly for travelers requiring a non-tourist visa, i.e. a visa for business or an extended stay in a country. Visas are issued by the embassy or consulate representing the country. They usually require the applicant to attend a personal interview at the embassy as part of their visa application.

I-Checkit

I-Checkit is an innovative solution that complements and enhances national border security systems by allowing the law enforcement community and trusted partners to conduct advanced passenger checks in real time. I-Checkit enables airlines to submit travel document information for screening against INTERPOL’s SLTD. The data screened does not include names of individuals.

A database match triggers an instant alert so the situation can be investigated. Notifications are sent to the INTERPOL General Secretariat, NCBs in the countries concerned, and other relevant national law enforcement entities. In some cases, this highly secure screening process will alert security teams within the airline company to enable them to carry out a secondary check of the document in question at the boarding gate.

In November 2015, INTERPOL’s member countries endorsed the I-Checkit Airlines solution as a key component of the Organization’s global border management strategy. This decision followed a 16-month pilot project with AirAsia which demonstrated the value of I-Checkit in mitigating the criminal risks that are behind identity fraud and gathering police intelligence, especially in countries without fully integrated border solutions.

Mobile ID devices

Mobile ID devices found several applications. They are autonomous nonstationary devices and their main advantage is that they can be used anywhere on the country’s territory, out of the migration or police office or border-crossing point (BCP), for example during police operations involving foreign national or apprehension of people between BCPs, registration of large numbers of migrants at the place of their location.

Mobile ID devices capture person's biometrics and then compare with the samples in a database stored on that device, or transmit it to a more extensive computer database located in a nearby vehicle or to a central database[12].

Such devices can also be used to verify identity of a person holding a biometric ID document by comparing his/her fingerprint with a fingerprint stored in the document chip, as well as identify validity of such document.

Where there is a need to register large numbers of people on the move at the place of their temporary location, mobile ID devices can be used to enroll migrants' data, including biometrics, into the system.

> *The* ***Czech Republic*** *particularly emphasized importance and potential of mobile solutions. On the national level, the Czech Republic supports especially the development of the mobile devices that enable checks of biometrics anywhere on the territory of the country. While preparing for possible influx of migrant the priority was given to development of the mobile technologies that could be used for performing registration and checks of the irregular migrants, including biometric data, in specific circumstances.*
>
> *The Czech system MobLus G2 for mobile screening in the databases of interest enables the authorities to check not only through local databases (specially secured), also on basis of wireless communication, including usage of fingerprints. The system allows reading RFID of chips in biometric travel documents.*
>
> ***Polish*** *border guards use mainly mobile solutions for border-check control.*
>
> *In* ***Sweden*** *both portable and stationary biometric stations are used for permits, passports and other kind of documents. They are also used to collect biometric information from asylum seekers.*

ICT solutions applied by EASO, including for emergency situations

The European Asylum Support Office (EASO) strengthens EU Member States practical cooperation on asylum, enhances the implementation of the Common European Asylum System (CEAS) and supports Member States whose asylum and reception systems are under particular pressure. For these purposes, EASO has developed different channels of information and several tools relying on diverse technologies and operates IT applications which store, organize and disseminate the information gathered:

(i) Early Warning and Preparedness System (EPS) that aims to provide internal and external stakeholders with accurate, timely information and analyses on flows of asylum seekers to and within the EU and the EU+ (EU28, Norway, Switzerland). This information supplements the official statistics regularly collected by Eurostat;

(ii) Country of Origin Information Portal based on Microsoft SharePoint, where targeted, relevant, reliable, accurate and up-to-date country of origin information is stored;

[12] https://www.nist.gov/sites/default/files/documents/itl/iad/ig/MobileID-BPRS-20090825-V100.pdf

(iii) Information and Documentation System (IDS) which acts as a knowledge base on national asylum systems of the EU states providing a detailed and up-to-date overview of the organization of national asylum systems and asylum-relevant case law.

Mobile call data

Given the popularity of mobile-cellular services, non-Internet-related mobile-network big data seems to have the widest socioeconomic coverage in the near term, and the greatest potential to produce relatively representative information globally. In 2014, the number of mobile-cellular subscriptions neared 7 billion, and the number of mobile-cellular subscriptions per 100 inhabitants reached 90 per cent. Mobile data are already being utilized for research and policy-making, not only in developed but also in developing economies. There are various examples of how mobile phone records have been used to identify socioeconomic patterns and migration patterns, describe local, national and international societal ties. Data are also being used to improve responsiveness in the event of natural disasters or disease outbreaks. Mobile call records were used to study the population displacements following Haiti's 2010 earthquake, with a view to using such methods to improve the effectiveness of humanitarian relief operations immediately after a disaster.[13]

Use of Skype, including in the context of migration crisis

Skype can be used as an alternative to telephone to contact migration authorities. In certain circumstances it is more accessible than telephone since if connected through Wi-Fi it does not incur charges and does not require a local SIM card which is convenient particularly for persons on the move and for short-term visitors. Even though Skype is not new communication software, but for migration authorities accepting it as a means of communication is a comparatively new tendency.

> *In December 2015, the State Migration Service of* ***Ukraine*** *announced that it would receive calls and messages via Skype. An increased number of inquiries related to issuance of the new national ID cards were expected at that time and Skype would help to process more such inquiries.*
>
> *In July 2014, the Asylum Service of* ***Greece****, in an effort to improve access to the procedure by minimizing queues outside its regional asylum offices, inaugurated a new system for granting appointment for registration of an asylum application through Skype. Applications were first made available in English and French and were later extended to Arabic in September 2014 and Farsi/Dari in November 2014.*

Smartphone applications for refugees

Smartphones are a great resource to help the refugees to receive information they might need but also interact with international and governmental agencies. International organizations, as part of their assistance to people on the move, distribute such items as SIM cards and solar lanterns that can also be used to charge cellphones, install solar-powered mobile charging stations in refugee camps.

The governments, volunteers and private sector were quick with developing smartphone applications (apps) that can help refugees and their supporters in different ways[14].

> *In* ***Germany*** *the government developed an app "Ankommen" ("Arrived", www.ankommenapp.de) which is aimed at helping refugees during their first weeks in the country. It provides and introduction to the German language, life in Germany*

[13] http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf

[14] For example, the website http://appsforrefugees.com contains 32 apps, including 12 working offline.

by answering practical everyday life questions, explaining the asylum process, providing advice on how to find a job or a vocational training position.

Refugees themselves have in some cases led this innovation drive. Early in 2015, a Syrian refugee who fled to Turkey, released an app featuring updates on important information for refugees, including residency regulations, registration requirements for students at universities, and job openings in host countries, particularly Turkey.

Other new products developed by the participating countries

***Estonia** mentioned its e-Residency project which offers to every world citizen a government-issued digital ID card and the opportunity to run a trusted company online.*

However, e-Residency is not strictly a migration management tool, since it does not confer citizenship, tax residency, residence or right of entry to Estonia or to the EU. The e-Resident smart ID card is not a physical identification or a travel document, and does not display a photo.

***Latvia** describes its Register of Natural Persons as one of the recent developments to facilitate the processes for third-country nationals and also for governmental authorities. This concept is still in the development stage and it is intended to register all foreigners in the Register in a centralized manner and allocate to them an individual personal ID number which will simplify further identification and provision of the electronic government services.*

Strategic and organizational changes

*In **Armenia** a document on standard response procedures in case of a massive influx of refugees to the country was developed with support of IOM Yerevan – the document provides for ICT solutions in crisis situations.*

***Belarus** can organize functioning border checkpoints at any section of the border (if deemed necessary).*

***Hungary** noted that inbuilt work-flow enables fast and efficient cooperation between the authorities involved in the crisis management.*

*In the beginning of 2000 the **Swedish** MFA, the embassies and the SMA worked together in order to develop the ICT solution "Wilma". This kind of cooperation at that time was seen as unconventional.*

Enhanced monitoring and reporting by means of ICT

*Processing of statistics has been intensified in **Azerbaijan** for analyzing the number of foreigners entering the territory of the country. Thus, now daily reports also are analyzed by processing while before analysis was conducted based on monthly, quarterly, annual reports only.*

***Belarus** ensured technical capacities to conduct comprehensive migration situation analysis by combining information from several information systems.*

The Unified Migration Analytical System (UMAS) in ***Georgia*** *intended for analytical and statistical purposes (and not for administrative functions) will become an exception from other administrative structures who mostly use relational data base solutions, as it will apply both relational data and big data opportunities. Big data solution was chosen for its unique capacities in data processing and analysis.*

In ***Poland*** *implementation of the reporting system – Data Warehouse – simplifies the generation of statistical data and their analysis in the area of migration. The solution allows for real time monitoring of aggregated data on migration helping to swiftly identify a rapid influx of migrants or other significant trends, length of decision process in various areas, numbers and types of issued decisions.*

Examples of innovative ICT solutions mentioned by the countries are listed in Annex VI. Annex VII contains examples of ICT solutions that can be applied by the countries in emergency migration situations.

Possible topics for discussion	*In your country, who usually propels the use of new ICT solutions in migration management: national authorities, academia, civil society, international partners?*
	Please describe how the staff preparedness to use new ICT solutions is ensured and how the training process is organized.
	Is open source intelligence (OSINT) used by your national authorities in the sphere of migration (for monitoring migration flows, criminal networks of migrant smugglers and traffickers, for checks on visa applicants etc)?

Annexes

Annex I. Questionnaire distributed among the participating countries

1. What is your country's approach to the use of information and communication technology in migration management: existing strategic documents, legal basis, plans for further expansion?

2. Please list the main national ICT systems used in migration management briefly indicating their main functionalities, rationale for their development, authorities involved in their management, who gets access and how data protection is ensured in the course of information exchange. What kind of biometric and identification information is used in your country's ICT systems (fingerprints, iris, FRS)?

3. To which international and EU-level ICT systems do your country's authorities have access?

4. What positive outcomes were observed after the introduction of ICT solutions in migration management?

5. Did your country's authorities encounter challenges associated with the use of ICT and if yes, how are these challenges dealt with?

6. Please describe non-conventional innovative ICT solutions used in the sphere of migration management in your country.

7. Please describe the ICT solutions applied in your country in response to unexpected and rapidly unfolding situations, if applicable (e.g. influx of migrants related to the current migration crisis, movement of IDPs, terrorist threats).

Annex II. Strategic documents and legal basis for use of ICT in migration management

	Strategic documents and legal acts
Armenia	- Concept of the State Migration Management Policy - Law "On Foreigners" - Government Decree (directly establishing the Migration Management Information System)
Azerbaijan	- Migration Code - Presidential Decree "On Entry-Exit and Registration Interagency Automated Data Search System" - Presidential Decree "On Unified Migration Information System of the State Migration Service of the Republic of Azerbaijan" - Law "On the status of Refugees and IDPs" (regulates procedures related to the information systems) - Presidential Order and Decree (programme documents for development of ICT)
Belarus	- State Program for Development of Digital Economy and Information Society for 2016-2020
Czech Republic	- European Agenda on Migration and European Agenda on Security (strategic documents) - legal basis for the IT systems is mainly part of the European law
Estonia	-
Georgia	- Migration Strategy for 2016-2020 (application of modern approaches to the ICT in migration management is one of the priority areas) - Concept of the Migration Risk Analysis System of 2015 - Governmental Decree on Creation and Administration of UMAS of 2015
Hungary	- JHA Council's "Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area"
Latvia	- Government's "Information Society Development Guidelines for 2014-2020" (National e-Government strategy) - legislative regulations for each system
Lithuania	- laws in compliance with the Law on Legal Protection of Personal Data and other legal acts - legal acts of the European Union - international treaties
Moldova	- National Strategy in the Sphere of Migration and Asylum for 2011-2020 - National Strategy for Digital Society Development (Digital Moldova 2020) - Strategic Program for Technological Modernization of Governance (e-Transformation) - Program of the Interoperability Framework - Concept of the State Population Register Automated Information System - Concept of the Automated Information Integrated System "Migration and Asylum"
Netherlands	-
Poland	- Strategic Action Priorities of the Minister of Digital Affairs in computerization of public services - National Integrated Informatisation Programme 2020 - National Development Strategy 2020 - Concept of the functioning of Border Guard 2016-2022 (plans for further development of the Border Guard ICT systems)
Sweden	- Government's IT-related political goal: "Sweden shall be best in the world on using digitalised facilities"
Ukraine	- strategic documents on migration policy matters - Government's Concept of the National System for Identification and Verification of Ukrainian Nationals, Foreigners and Stateless Persons - law and by-laws

Annex III. Advantages and challenges related to ICT use

	Advantages	Challenges (encountered or envisaged)
Armenia	- improved work with passenger flow - improved reporting - improved statistics	-
Azerbaijan	- improved control over and management of migration flows - improved data collection on FSPs entering the country and own nationals leaving the country - improved protection of migrants' rights and freedoms - improved protection of state security - better formulation of migration policy - conduction of interagency data exchange in centralized manner	-
Belarus	- reduction of time for analysis of migration flows which led to well-timed decision making - substantially higher level of identification within migration flows of persons who are of concern to the law enforcement agencies	- international treaties on protection of personal data
Czech Republic	- improved management in the migratory-and-security-policy field	- flexibility of the responsible authorities while reacting to the challenges in the field of ICT
Estonia	- better person identification and higher comprehensiveness of information about persons	-
Georgia	- quicker, more effective and secure migration management process - enhanced migration related case management - better analysis of migration data and monitoring of migration flows and stocks	- observation of personal data protection requirements - increased security risks for the technology and hence, for the data security
Hungary	- improved and accelerated person identification and registration - easier communication (e.g. through long-distance interpretation) and significant development in the field of information exchange between Member States - higher level of identification of abuse regarding the right of residence/asylum/documents - faster and much more efficient administration	- coordination of the development of interagency solutions
Latvia	- improved data exchange - more effective processes - lower consumption of time and human resources - reduced risk of human errors	- ensuring quality of biometric data - ensuring most optimal digitization processes
Lithuania	- facilitation of experts' work, reduction of administrative burden	- incompatibility of some still existing national procedural requirements (archives regulations, registration of correspondence, formal documentation etc) with the ICT solutions
Moldova	- optimisation of working procedures - improvement of data collection and data quality - improvement of statistics and reporting procedures - reduction of human error risks	- lack of common standards for different information systems managed by different agencies (solution: started implementation of the government

	- improvement of inter-agency data exchange and data compatibility	platform MConnect to facilitate interagency information exchange)
Netherlands	- increased awareness of the 'supply chain' of data which led to process improvement, including their speed - increased data quality due to feedback from other users	- costs and benefits are not necessarily aligned between organizations - the ICT systems of different organizations are not on the same technical level, in some cases the weakest link determines the standard
Poland	- acceleration of the information flow - better accessibility of the information for the final user - development of effective and complex control of the migration influx - credible information on the migration dossier in particular cases of foreigners - significant improvement of the use of statistical data on migration, including quicker and comprehensive analysis of the data generated, simplified management and more precise identification of further development targets - identification of possible abuse of migration law much faster - more efficient, secure and accurate data processing	- maintaining, broadening and upgrading infrastructure (both hardware and software) - ensuring integration and interoperability of the systems, on the national and EU level - carrying out modifications of the ICT systems necessary to align them with legal changes
Sweden	- easier overview of a person's different migration cases - better service for the applicant including through e-services - more effective and easier communication between involved authorities - more flexible organization, using ICT-solutions cases can be managed from different places without any physical cases has to be sent between the offices	- an ICT-solution has to be suited for the working method - work in a standardized way and continuously train the staff - continuous work on the organizational development in parallel when developing ICT-solutions
Ukraine	-better service for applicants - ID data are more reliable - swift and reliable interagency data exchange	- lack of a common standard or a unified platform for interagency on-line data exchange

Annex IV. National ICT systems (by purpose)

Purpose Country	Own population registration	Biometric ID documents	Visas	Entry-exit	Residence permits	Work permits	Asylum	Administrative offences/ irregular stay
Armenia	+	+	+	+	+	-	+	+
Azerbaijan	+	+	-	+	+	+	+	+
Belarus	-	+	+	+	+	-	-	-
Czech Republic	-	+	+	-	+	-	+	+
Estonia	+	+	-	+	+	-	-	+
Georgia	+	+	+	+	+	+	+	+
Hungary	-	-	+	-	+	-	+	-
Latvia	+	+	+	+	+	+	+	+
Lithuania	+	-	+	-	+	-	-	-
Moldova	+	+	+	+	+	+	+	+
Netherlands	+	-	+	-	-	-	-	-
Poland	-	+	+	+	+	+	+	+
Sweden	-	-	+	-	+	+	+	-
Ukraine	+	+	-	+	+	-	+	-

“-“ means that the relevant information was not directly mentioned by a country and not necessarily that no such national system exists in that country

Annex V. Access to the EU-level and international databases

Database / Country	VIS/VIS Mail	SIS/SIS II/SIRENE	EURODAC	DubliNet	FADO/iFADO	Interpol's databases	Other databases
Armenia	-	-	-	-	-	-	-
Azerbaijan	-	-	-	-	-	-	DISCS
Belarus	-	-	-	-	-	-	-
Czech Republic	+	+	+	+	+	SLTD	-
Estonia	+	+	+	-		+	-
Georgia	-	-	-	-	-	SLTD NOM	DISCS
Hungary	+	+	-	+	-	-	-
Latvia	+	+	+	+	+	SLTD	-
Lithuania	+	+	+	+	+	+	Electronic Readmission Management System of Georgia
Moldova	-	-	-	-	-	NOM	-
Netherlands	+	+	+	-	-	SLTD	-
Poland	+	+	+	+	-	SLTD NOM	-
Sweden	+	+	+	+	-	-	-
Ukraine	-	-	-	-	-	+	-

"-" means that the relevant information was not directly mentioned by a country and not necessarily that the country does not have access to a particular database

Annex VI. Innovative ICT solutions for migration management

	Name	Characteristics
Armenia	-	-
Azerbaijan	Unified Migration Information System	- the key role in migration management - monitoring is carried out for revealing illegal migrants via the ways beyond the standard procedures
Belarus	-	-
Czech Republic	EU-level solutions National-level solutions	- the utilization of the biometric data - broadening of the interconnectivity and interoperability of the current IT systems - the development of the mobile devices that enable checks of biometrics anywhere on the territory of the country
Estonia	E-residency project	-
Georgia	Unified Migration Analytical System (UMAS)	- the system will apply both *relational* data and *big* data opportunities while the administrative structures in Georgia are mostly using *relational* data solution
Hungary	-	-
Latvia	Register of Natural Persons	- simplified processes for third country nationals and also for the governmental authorities (registration of all foreigners in a centralized manner and allocation to them an individual personal ID number)
Lithuania	-	-
Moldova	-	-
Netherlands	-	-
Poland	-	-
Sweden	Wilma	- it was developed in the beginning of 2000 together by the Swedish MFA, the embassies and the SMA; this kind of cooperation at that time was seen as unconventional
Ukraine	-	-

Annex VII. ICT solutions for emergency migration situations

	Name	Characteristics
Armenia	Standard operating procedures in case of influx of refugees to Armenia (under development)	Envisages application of ICT solutions in the crisis circumstances
Azerbaijan	Intensified processing of the statistics on the number of foreigners entering the territory of the country	Now daily reports also are analyzed while before analysis was conducted based on monthly, quarterly, annual reports only
Belarus	Automated System of the Border Control "Berkut-B"	- data search on persons in different databases of the law enforcement bodies - swift deployment of fully functioning border checkpoints at any section of the border - comprehensive analysis of the migration situation in border crossing points and outside BCPs
Czech Republic	Development of the mobile technologies	- performing registration and checks of the irregular migrants including their biometric data
Estonia	-	-
Georgia	Working Group on Migration Risk Analysis chaired by the MIA established in 2016	- the concept of the migration risk analysis system is developed, the methodology is under development
Hungary	- ICT applications and adapted data transfers - inbuilt work-flow	- possibility to extend the end points (practically anywhere in the world) corresponding to the systems - fast and efficient cooperation between the authorities relevant in the crisis management
Latvia	The ICT systems are developed and their functionality is being continuously improved	- rapid, effective and coordinated reaction to possible emergency situations
Lithuania	-	-
Moldova	- interagency exchange of information through ICT - Automated Information Integrated System "Migration and Asylum" (AIISMA)	- AIISMA can be adapted to the emergency migration situations if required
Netherlands	Pro-forma system was developed (to be replaced by a new system)	- keeping track of both the migrants and the staff
Poland	- mobile solutions for border-check control - access to INTERPOL data bases (SLTD, Nominal and SMV) - API (arrivals direction) and NSW (both directions – arrivals and departures) - Data Warehouse	- prevention/avoidance of terrorists threats and control the situation of influx of migrants up to the current migration crisis - simplified generation of statistical data and their analysis in the area of migration
Sweden	Increasing and upscaling of the ICT-system	- processing of the increased numbers of employees and cases
Ukraine	Development of electronic information templates for description of model situations	-