DoT.Mig

In Brief

More connected – less protected? How the EU Interoperability Framework will affect the European Migration Space

September 2022

DIALOGUE ON TECH AND MIGRATION

A project of the Migration Strategy Group on International Cooperation and Development

BertelsmannStiftung

G|M|F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Robert Bosch Stiftung

Author

Alberto Tagliapietra, Senior Program Coordinator, Mediterranean Policy Program and Dialogue on Tech and Migration, German Marshall Fund of the United States (GMF)

The views expressed in this publication are the views of the author alone and do not necessarily reflect those of the partner institutions.

About DoT.Mig

The **DoT.Mig In Brief** paper series is part of the The Dialogue on Tech and Migration, DoT.Mig.

DoT.Mig provides a learning platform to connect the dots between digital technologies and their use and impact on migration policy, as well as connecting relevant stakeholders. The **DoT.Mig In Brief** paper series highlights debates and concepts relevant to navigate the emerging field of Tech and Migration.

DoT.Mig is a forum by the Migration Strategy Group on International Cooperation and Development (MSG). The MSG is an initiative by the German Marshall Fund of the United States, the Bertelsmann Foundation, and the Robert Bosch Stiftung.

Key Takeaways

1. To better control and monitor who crosses EU borders, the EU uses large-scale information systems composed of several databases in which people entering the union are registered depending on their entry reason. These information systems provide border guards, police officers, and migration and asylum officials with relevant information on individuals entering the union.

2. Now, the EU wants to take this system one step further, aiming to link all existing and forthcoming databases on migration and asylum. Their aim is to make them interoperable—more easily and quickly searchable—to police and border authorities.

3. While the interoperability of databases may help prevent identity fraud, fill information gaps, and improve border checks, it may also lead to a new system of massive usage and retention of third-country nationals' data.

4. Technical and legal approaches to limit the risks that interoperability constitutes for fundamental rights remain underdeveloped, and the changing scope of databases containing third-country nationals' data raises many questions.

5. Potential risks and challenges of interoperability in the migration space are: weakening of data safeguards, potential violation of purpose limitation, data quality issues, and challenge for individuals to oppose decision making based on incorrect data.

6. Using databases for objectives not envisioned when they were established, as the new tasks assigned to the main EU information systems by the interoperability regulations shows, is a worrying development.

7. Migration policy stakeholders need to better understand the shift and need to engage in discussions about the challenges of interoperability to fundamental rights and what measures could be imposed to protect them.

1. Introduction and Background

When EU member states agreed on the free movement of people and goods within the EU, they also decided that freedom of internal mobility would require strict controls at external borders—determining who can enter member states' territory and who cannot. To better control and monitor who crosses their borders, the EU set up a number of large-scale information systems composed of several databases in which people entering the union are registered depending on their entry reason (in order of creation: the Schengen Information System, Eurodac, and the Visa Information System). These information systems provide border guards, police officers, and migration and asylum officials with relevant information on individuals entering the union and have become an essential tool for external border management to pursue the internal security of the EU.

Now, the EU wants to take this system one step further, aiming to link all existing and forthcoming databases on migration and asylum. Their aim is to make them interoperable—more easily and quickly searchable—to police and border authorities. The move toward interoperability is part of a broader movement toward digitalization of border management and the establishment of a "smart" EU border. New systems and linked databases will allow digital screening and tracking of who enters and—with a new Entry-Exit System planned—leaves the EU. Along with three forthcoming databases, the EU is taking a new digital border management approach, similar to that of the United States and Canada.

In this brief, we provide more background on the issue of interoperability and its implementation. This complex reform, as designed by the EU Commission, is deemed as an infringement of (digital) rights by civil society organizations while welcomed as a step to better and more efficient monitoring of EU borders by others.

1.1. What is interoperability and why does it matter to the EU Commission?

In 2017, the European Commission presented two legislative proposals to establish an interoperability framework between EU-wide centralized information systems in the so-called Area of Freedom, Security, and Justice (AFSJ). The proposals aimed to improve security (such as tracking transborder crime), allow for more efficient identity checks, improve the detection of multiple identities, and assist to address irregular migration. The proposals were accepted in 2019, with implementation to be completed by 2022. However, this process is more likely to be completed in 2023 or beyond.

Interoperability, in its broadest sense, means the ability of information systems to exchange data and to share information. It seeks to maximize the usage of existing data without creating new databases or changing access rights to existing information systems. The reasoning behind the implementation of interoperability in the AFSJ assumes that if information is fragmented over several databases that cannot communicate, security issues may escape the attention of the

relevant security agencies. Therefore, the EU interoperability framework tries to create a system in which various large-scale IT systems in the AFSJ can communicate with each other. What makes the issue so complex is that data access and sharing for each large-scale IT system is regulated through different legal approaches—thus, interoperability requires the alignment of legal provisions.

1.2. Why is interoperability presented as a crucial development in the migration space?

The impulse to develop an interoperability framework can be traced back to the 2015 European Agenda on Migration which emphasized, among other things, the need to overcome the shortcomings and limitations of the current EU data management architecture and to make better use of the opportunities that information systems and technologies offer.

Until that point, according to the Commission, the EU was grappling with a data management system characterized by differently governed information systems and databases which failed to communicate with each other, a condition that, in their view, led to their "sub-optimal functionalities." The consequent inconsistency between them, argues the Commission, led to blind spots and a more difficult and time-consuming consultation process with law enforcement authorities. In this context, interoperability would improve the effectiveness and efficiency of border checks, help address and prevent illegal immigration, generate better working visa policies, and substantially contribute to a higher level of security.

In 2017, the European Commission announced the interoperability package, composed of two proposals: a proposal to establish a framework for interoperability between EU information systems on borders and visas (translated into Regulation 2019/817) and a proposal on interoperability in the area of police, judicial cooperation, asylum, and migration (translated into Regulation 2019/818). The two regulations were adopted on May 14, 2019.

2. How is interoperability structured?

The interoperability package envisages a system whereby authorities that already have access to one or more of the existing EU information systems (such as local, national, federal police, and border guards) can check whether information related to an individual is available in one of the current (or future) EU databases. The new system will be inextricably linked to existing large-scale EU information systems like Eurodac, the Schengen Information System, the Visa Information System, and the three new databases still under construction in the AFSJ (the Entry-Exit System, the European Travel and Authorization System, and the European Criminal Record Information System on third-country nationals).

2.1. How will interoperability change the current system?

With interoperability, the large-scale IT system in AFSJ will change from a compartmentalized "silo-based" structure to a system in which all databases are searchable from a unique portal.

Existing and forthcoming databases in the AFSJ

Existing databases

The Schengen Information System (SIS II) was established to compensate for the creation of the Schengen area of free movement. It stores fingerprints, facial images, biographic data such as name and surname, date/place of birth and sex, information on identity, and travel documents.

The European Dactyloscopy System (Eurodac) was established to assist in the determination of the state responsible for processing an application for international protection in accordance with the Dublin Regulation. Currently, it only stores fingerprints, but a proposal under discussion wants to enlarge the data stored to facial images, biographic data such as name and date/place of birth, as well as time and place of apprehension/application for international protection.

The Visa Information System (VIS) was established to store short-term visa applications and make them available across the Schengen area to facilitate the implementation of the common EU visa policy. It stores fingerprints, photos, and biographic data. A proposal approved on July 7, 2021 enlarged the data stored to include travel document copies.

Forthcoming databases

The Entry-Exit System (EES) aims to monitor border crossings and detect people whose visa has expired. Once established, it will store fingerprints, facial images, biographic data, and information on travel documents. According to eu-Lisa, it should be *implemented by the end of May 2023.*

The European Travel Information and Authorization System (ETIAS) will be established to carry out security, immigration, and health checks on visa-exempt travelers. Individuals with a passport from a visa-free country will have to obtain a travel authorization through the ETIAS system. It will store biographic data, information on travel documents, employment, and occupation. According to eu-LISA, it should be *implemented by November 2023.*

The European Criminal Records Information System on third-country nationals (ECRIS-TCN), will be used to simplify the process of finding criminal convictions against non-EU nationals in other member states. It will store fingerprints, facial images, and biographic data. Europol and Eurojust will have direct access to ECRIS-TCN. According to eu-LISA, it should be *implemented by May 2023.*

2.2. How is interoperability structured in terms of operationalization?

The interoperability package envisages the creation of four new tools to enable the separate databases to communicate with each other: the European Search Portal, the Shared Biometric Matching Service, the Common Identity Repository, and the Multiple Identity Detector.

1. **The European Search Portal (ESP)** will allow local, national, and federal police and border guards to simultaneously search multiple EU information systems (SIS II, VIS, Eurodac, EES, ETIAS, ECRIS-TCN), Europol, and Interpol databases using both biographical and biometric data, with the results of all checks on a single computer screen. As a result of the query, the systems will provide data about the individual checked, indicating which information system the data was sourced from. The ESP will not store or process any new data and will maintain the access rights of each information system.

2. **The Shared Biometric Matching Service (BMS)** will enable the search and comparison of biometric data (fingerprints and facial images) from several systems, in particular, SIS, Eurodac, VIS, the EES, and ECRIS-TCN.

3. **The Common Identity Repository (CIR)** will create and store an individual file composed of biographical and biometric data of every third-country national recorded in Eurodac, VIS, the EES, ETIAS, and ECRIS-TCN. This is intended to enable

the effective identity checks of TCNs in the territory of a member state and to facilitate law enforcement authorities in their fight against criminal offenses. The data will still belong to the information system from which it was originally sourced, but it will no longer be stored separately. In this way, CIR will constitute a new database.

4. **The Multiple Identity Detector (MID)** will store identity confirmation files, including links created between alphanumerical data (like name, surname, address, age, etc.) contained in more than one AFSJ information system. This way, MID will enable the correct identification of individuals, the discovery of identity fraud, and the usage of multiple identities.

2.3. How will access to information be managed?

To access information stored across different systems, the interoperability package defines a two-step approach to grant law enforcement authorities access to the databases based on a "hit/no hit" process. The response to a query will only confirm whether data on the searched person exists. In the case of a "hit," authorities must place a request to access information based on the respective rules and safeguards applicable to that database. An official requesting an identity check through the ESP at the external border of the EU or within a member state territory can immediately verify if, and where, the data of the person being checked is stored in the EU's large-scale IT system (for example, in Eurodac, in the SIS II, in the VIS, etc.). **However, to view the relevant data and access the database in which it is stored, the specific rules of access and consultation applicable to each database must be followed. Obtaining immediate access to the requested information is not possible without properly documented processes and permission requests.**

2.4. How will the interoperability framework be managed?

Eu-Lisa will play a crucial role in managing interoperability. In the framework of the interoperability package, the agency will be responsible for the operational management of the system and the development of common data quality indicators so that only data fulfilling the minimum quality standards can be used and inserted into the EU IT system. Notwithstanding the centrality of eu-Lisa when it comes to management of the system and data upload and usage, regulations also place specific responsibilities on member states, creating a system of multilevel and fragmented management.

3. What are the risks of interoperability in the migration space?

Interoperability represents a crucial paradigm change in the management of EU IT systems. It may have positive repercussions on the EU system, contributing to better decision-making and the storage of better-quality data, for example, by avoiding duplication of data across various databases; yet, the challenges it poses are many. While the Commission stresses that the new approach to interoperability does not undermine the EU's strong data protection rules based on the principles of data protection "by design and by default" observers such as Picum and Statewatch argue that data usage in the interoperability framework constitutes an extension of the purposes for which the data was originally collected.

3.1. Weakening of data safeguards

While interoperability regulations have been presented as an essential tool to protect the internal security of Europe, they also have implications for human rights and data security. The European Data Protection Supervisor (EDPS) highlighted that even if interoperability represents a useful tool to address the legitimate needs of competent authorities using EU large-scale information systems, it is also fundamental that this system is implemented in compliance with the crucial requirements of necessity and proportionality. For example, the implementation of the hit/no hit system risks weakening the strict access rules that law enforcement authorities are subject to with respect to information systems like the VIS, Eurodac, EES, and ETIAS. Even if it is true that the existing rules for each database will remain in place, the result of the hit/no hit system may reveal information regarding an individual (for example, indicating that they have data stored in Eurodac). According to some observers, this could allow police authorities to make inferences from the information obtained via the ESP, and to potentially make decisions based on the specific database where an individual's data is stored.

3.2. Violation of purpose limitation?

Before the approval of the two interoperability regulations in 2019, existing databases in the AFSJ were always held separately, and access and usage were limited. This way, the principle of purpose limitation (as stated in Art. 8 of the Charter of Fundamental Rights of the EU) was observed and implemented. Yet, interoperability brings a major shift to this approach. It now sees the silo structure as a flaw that must be fixed rather than as a means of safeguarding privacy and personal data by keeping databases separate. With the three new databases and search tools—CIR, the BMS, and the MID—data previously stored separately will now be jointly accessible from one central system, the ESP. Combining information from

different systems in this way allows authorities to draw an idea of who they have in front of them, while the subject remains unaware of how their data will be used (for example, the CIR will allow law enforcement authorities access to immigration data stored for non-law enforcement purposes).

3.3. The issue of data quality

Interoperability will only work if the reliability and quality of data in the databases involved are sufficiently guaranteed. The quality of stored data has been a longstanding problem of existing databases. If the stored information is not of sufficient quality, data analysis through interoperability may lead to incorrect processing, with significant repercussions for third-country nationals. For example, incorrect matching of an individual's fingerprints with someone who is already registered within Eurodac could lead to the refusal of international protection.

3.4. Are the safeguards envisaged in the two regulations enough?

Despite safeguards in the regulations and applicable data protection standards, it will be hard for individuals to oppose decision-making based on incorrect data. Interoperability risks the weakening of boundaries between law enforcement and immigration control and the intensification of surveillance of all TCNs. Finally, the consequences of wrongful decision-making based on incorrect data will be dangerous not only for the protection of fundamental rights but also for the effectiveness of interoperability as a measure per se.

Pros

- More efficient management of borders and internal security through enhanced information availability
- Better and faster decision-making when it comes to assessing the entry of an individual into the EU thanks to the linkage of all the databases and the availability of biographical and biometric information in one source (CIR)
- Improved data quality due to the implementation of new rules and standards of data upload in all the databases
- Avoidance of multi-identity registration in different EU systems due to the implementation of biometric data

Cons

- Potential breach of purpose limitation due to the usage of data collected for specific reasons for new and not previously envisoned uses
- Weakening of data protection and transparency as interoperability leads to additional processing of data without appropriately informing the person about the usage of his/her data
- Risks further pushing a linkage between migration and crime, as for example refugees' data (contained in Eurodac) will be processed side-by-side with data of crime suspects (contained in the SIS II)

4. What is next with interoperability?

Despite several critical voices from bodies like the European Data Protection Supervisor (EDPS) and the Article 29 Working Party (WP29) questioning the necessity of moving toward an interoperable system in the AFSJ from a technical point of view, the Commission, the Council, and the European Parliament decided to move forward with approving the two regulations.

The next steps concern the implementation phase of the two directives, as the system should start to work before the end of 2023. Yet, many member states question the probability of meeting this timeline. Even eu-Lisa, one of the key actors regarding interoperability, seems skeptical about the possibility of rolling out the system before the end of 2023, as reported by Statewatch.

5. Conclusion

While the interoperability of databases may help prevent identity fraud, fill information gaps, and improve border checks, it may also lead to a new system of massive usage and retention of third-country nationals' data. Technical and legal approaches to limit the risks that interoperability constitutes for fundamental rights remain underdeveloped, and the changing scope of databases containing third-country nationals' data raises many questions.

Using databases for objectives not envisioned when they were established, as the new tasks assigned to the main EU information systems by the interoperability regulations shows, is a worrying development. An example of this is Eurodac, which will begin to store biometric data and, with interoperability, detect people with multiple identities even though this task was not originally mandated. While it is true that access rights to the databases will not be weakened, there will be a relevant impact on how data of third-country nationals will be managed and, most importantly, used.

All these issues underline how the Commission warped discourse on interoperability and its choice to pursue interoperability as an objective rather than a well-thought tool to better manage EU borders risks undermining its potential and compromises the objective of building a better functioning system to manage movement within the AFSJ.