18 SEPTEMBER 2018
#EUSECURITY
#JHA

JACQUES DELORS INSTITUTE
BERLIN
Centre for European Affairs at the Hertie School of Governance

WHAT'S WRONG WITH EU INFORMATION SYSTEMS AND HOW TO FIX IT

A CRITICAL LOOK AT EUROPEAN DATA INTEGRATION

Executive summary

■ **FRANCA KÖNIG**
Research Associate,
Jacques Delors Institute
Berlin

The EU data management architecture comprises a highly complex network of different information systems and actors. Over recent years, it has become increasingly obvious that this architecture suffers from significant gaps and shortcomings, creating real-world consequences and practical security implications.

The EU has woken up to the challenge of making its information systems more interconnected since at least the recent terror attacks here. The Commission's legislative proposal on establishing a framework for interoperability in the EU foresees the streamlining of existing central databases, the creation of a few more of these and the introduction of improved, centralised procedures for information access and exchange, including for law enforcement.

This paper seeks to provide a clear and accessible overview of this urgent topic and explain why and how interoperability matters. It tackles head-on the often-neglected technicalities and complexity of the EU network of information systems by breaking these down into three blocks. First, it provides an overview of the current system and takes a critical look at its weaknesses. Second, it discusses the on-going reform initiative and how it intends to remedy these shortcomings in practice. Third, the paper evaluates remaining challenges in the way of the envisaged framework and makes concrete recommendations on how to address them.

While the interoperability framework contains many promising tools and components that could significantly improve police work in the EU, implementing it remains a matter for concern. Besides the question of political will, five types of implementation challenges stand out in particular. They relate to the legal, technical, and operational dimensions of the legislative proposal as well as to data protection and safety.

Unless member states and the EU jointly address these challenges and draw up appropriate measures, the interoperability framework could fail to sustainably enhance the European information landscape and achieve the security and data protection benefits it targets.

Heads of state or government will meet on 20 September at an informal session of the European Council on internal security that will undoubtedly also touch upon the interoperability of EU information systems and data-sharing. Against this backdrop, the paper makes six main policy recommendations:

1. Member states and the EU **should ensure that legal frameworks are properly adapted** via clear definitions of controllership, data protection regimes and access criteria, thus establishing legal clarity on which rules and principles apply within an interconnected architecture.

2. Both **should facilitate the full and coherent transposition and application of the various interoperability components** into national and EU systems, including the complete roll-out of technical extensions.

3. **Sufficient technical, financial and human resources must be made available** to guarantee the proper and complete implementation of these components at the national and EU level.

4. Practical training of end-users, harmonisation of procedures across member states, and legal safeguards are required to **ensure data input and quality as well as data safety and protection**.

5. Member states and the EU should **guarantee and maintain appropriate investment and training in cyber security and risk resilience** at the levels of technology, infrastructure, process design and functional operation.

6. **Monitoring and review mechanisms** are crucial to adapting the interoperability framework and its components on a regular basis in response to gaps and changes in the criminal and cyber landscape as they emerge.

TABLE OF CONTENTS

INTRODUCTION

The terror attacks mounted in Brussels, Paris and Berlin in recent years have cruelly exposed persistent flaws in European security cooperation. The attackers were either European citizens from differing backgrounds or had entered the EU as part of the migrant and refugee crisis. Although they had been officially clocked as terrorist suspects, they were able to freely cross several member states – often as a result of multiple residential registrations and the conscious adoption of aliases. In the case of the 2016 Berlin Christmas market attack, even cooperation among German state authorities failed dramatically, thus enabling the perpetrator, Anis Amri, to strike.

In their wake, policymakers and practitioners at the highest levels have underlined the urgency of improving exchanges of intelligence between security authorities across Europe.[1] In particular, they have criticised how stored information relevant to cross-border law enforcement has been confined to national systems and compartmentalised in silos even within single databases, thereby putting obstacles in the way of European policing and the security of EU citizens at risk. Consequently, following an initiative by the European Commission in spring 2016, the Council adopted a roadmap to enhance exchanges of information and information management, including solutions based on interoperability in the Justice and Home Affairs area.[2]

A number of building blocks are now under construction. The Commission has, for instance, proposed a framework for interoperability among EU information systems in the realm of police and judicial cooperation, asylum and migration, and this is now being negotiated among the member states and relevant EU bodies. Interoperability also features as one of the priority dossiers of the current six-month Austrian EU Council Presidency, and the topic should next feature at the September and October meetings of the European Council and the Justice and Home Affairs Council. As discussions are on-going and the proposed measures have great potential, the current negotiations on the framework and the fine-tuning of single components are crucial. Outstanding real and potential obstacles need to be addressed; remaining risks and concerns must be carefully weighed up.

Consequently, there is still a ways to go before the proposal can be adopted and this mammoth task is completed. Connecting different national and supranational systems that were previously rather isolated presents a massive challenge at various levels and is not entirely uncontroversial. Legal, technical and operational issues stand in the way of achieving interoperability and questions about data safety and protection in an increasingly centralised system need to be answered.

This policy paper aims at contributing to the on-going discussions by first providing an overview of the most important EU information systems and taking stock of the current state of affairs, especially key problems and weaknesses. It then outlines the concrete components of the Commission's proposed regulation and how they are designed to remedy the shortcomings of today's information systems architecture. Third, it identifies five key challenges on the road towards interoperability (legal, technical and operational aspects as well as concerns about data protection and safety) and proposes ways to address them.

1. European Council. "European Council meeting (17 and 18 December 2015) – Conclusions" (EUCO 28/15), Brussels, December 18, 2015.
2. Council of the European Union. "Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area" (9368/1/16 REV 1), Brussels, June 6, 2016.

1 . A STROLL THROUGH THE EUROPEAN DATA MANAGEMENT LANDSCAPE

Albeit a bit of a mouthful, interoperability can be broken down as referring to "the ability of information systems to exchange data and enable sharing of information" with the aim of improving "the efficiency and effectiveness of Europe-wide information-sharing tools, by ensuring the technical processes, standards and tools that allow EU information systems to work better together."[3] Before assessing how to achieve interoperability, this section outlines the basic design of the current European data management architecture and identifies some of its key flaws.

At present, five main information systems exist in the EU: three centralised and two decentralised ones (see figure 1). Centralised systems are maintained by the European Commission and make up a central IT and communication infrastructure at EU level that connects the centralised system to national ones. By contrast, decentralised systems resemble information networks that facilitate data exchange across national systems. As with the centralised systems, the Commission provides and administers a common IT and communication software for these networks. However, there is no centralised database; the information itself remains exclusively stored in national databases and is only exchanged bilaterally in response to requests.

Among the centralised EU information systems are:

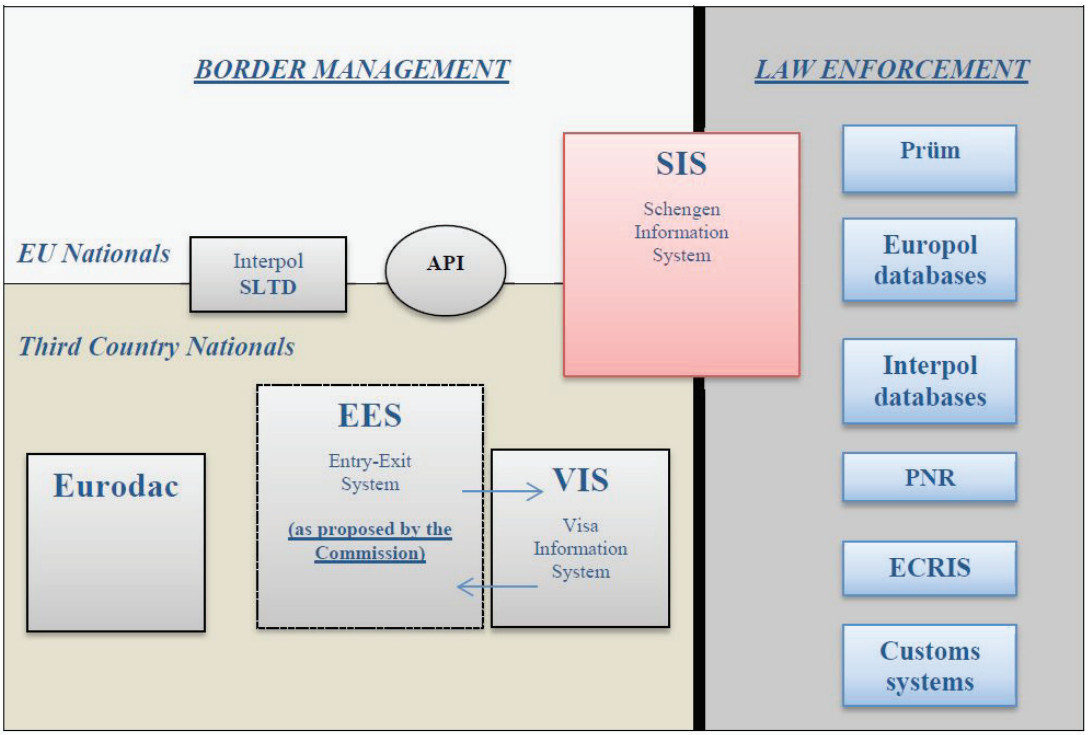
- the **Schengen Information System (SIS)**, the most widely used EU system with a broad range of data on individuals and objects both from the EU and third countries;
- the **Visa Information System (VIS)**, which contains data on short-stay visas of third-country nationals;
- the **European Dactyloscopy System (EURODAC)**, which stores fingerprints of asylum seekers and irregular migrants.

Whereas SIS collects and stores data related to EU and third countries, VIS and EURODAC mostly contain information concerning non-EU citizens. For all these systems, a central data repository exists at EU level, including a communications infrastructure that connects it to national databases. The European Commission or the European Agency for the operational management of large-scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) are responsible for operational management. Member states are entrusted with the maintenance of their own systems that feed the centralised database.

Two further complementary tools are the **Interpol database on Stolen and Lost Travel Documents (SLTD)** as well as the American-initiated **Advance Passenger Information System (API or APIS)**, which records passengers' passport and travel information in advance of flights arriving in the EU.

3. European Commission. "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)" (COM(2017) 794 final), Brussels, December 12, 2017, p. 16.

FIGURE 1 ▪ Schematic overview of the main information systems for border management and law enforcement



Source: European Commission. "Communication from the Commission to the European Parliament and the Council; Stronger and Smarter Information Systems for Borders and Security" (COM(2016) 205 final), Brussels, April 6, 2016, p. 7.

Several decentralised systems also facilitate information exchange in the EU: particularly the **Prüm database network** and the **European Criminal Records Information System (ECRIS)**. Prüm offers a framework for exchanging information related to DNA, fingerprints and vehicle registration.[4] ECRIS by contrast links national criminal databases. It thus provides information on previous convictions and the criminal history of persons registered in the EU. Neither system centralises information. Both act as (IT and communications) platforms at European level that connect the central databases of member states upon request.

Since 2016, these two data processing tools have been further complemented by Passenger Name Record (PNR) data.[5] Similar to the U.S.-led gathering of international passenger information in advance, PNR data comprises passenger information collected by air carriers in the process of booking and check-in.

To date, these remain the most important databases for European law enforcement and border management. Yet, a number of shortcomings and weaknesses persist in the existing data management landscape. Four problem categories (or dimensions of interoperability) can be highlighted in particular:[6]

4. Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, Official Journal of the European Communities L 210, 06.08.2008, pp. 1–11; Council Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA, Official Journal of the European Communities L 210, 06.08.2008, pp. 12–72.
5. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Official Journal of the European Communities L 119, 04.05.2016, pp. 132–149.
6. European Commission. "Communication from the Commission to the European Parliament and the Council; Stronger and Smarter Information Systems for Borders and Security" (COM(2016) 205 final), Brussels, April 6, 2016, pp. 3–4.

1. **shortcomings of existing EU information systems,** calling for improvements;

2. **gaps in the current EU data management landscape,** requiring additional tools and systems;

3. **complexity and lack of compatibility between different EU information systems and their governance frameworks,** resulting in a need to establish a single search interface;

4. **fragmentation of the present EU data management architecture,** calling for greater interoperability among current systems.

These deficits have posed very real challenges to the day-to-day work of police officers and continue to do so, for example in the form of limited access. In order to access the Visa Information System (VIS), police officials must first prove the relevance for each criminal investigation and face a variety of practical and procedural problems depending on national implementation. Similarly, the EU's fingerprint database EURODAC can only be searched after having consulted the national Automatic Fingerprint Identification System (AFIS), Prüm and the VIS. As a result, additional workload and procedural complexity provide significant obstacles.

> "THE DATA QUALITY OF INDIVIDUAL SYSTEMS NOW VARIES WIDELY

Besides this quantitative dimension of searching separate databases with different degrees of access, the data quality of individual systems now varies widely as do the format and type of data they contain. For example, data on EU citizens and third country nationals is now stored in separate databases. Only the Schengen Information System (SIS) stores data about EU citizens, whereas all other EU information systems concern third country nationals.

In the same vein, the European criminal records database contains the criminal history of both EU and non-EU residents, but effective procedures for information exchange are only in place with regard to data on EU citizens. What is more, databases such as SIS may only be searched alphanumerically (by name), not by fingerprints.[7] Yet, identification on a name-basis is less exact and leaves considerable room for document and identity fraud. Finally, data quality differs, because not all member states have the same capacity, for instance for collecting and exchanging (let alone protecting) biometric data. As a consequence, tools like the Prüm framework remain underfed and underused.

However, even if databases are fed sufficiently, practical difficulties remain due to a lack of consistency in the message and input formats. A seemingly simple difference in inserted data across systems such as tagging personal information as either 'surname,' 'last name' or 'family name' may significantly complicate searches and heighten the risk of mismatches and multiple entries. Common minimum standards are not being followed by all member states.

Recent terror attacks have demonstrated the practical ramifications of low or inadequate data quality and the lack of opportunities for systematic, coherent checks of all databases. Despite a European and an international arrest warrant Abdelhamid Abaaoud, who allegedly

7. In June, informal agreement was reached on three according EU regulations on improving the use of SIS, including for example the possibility of using biometric data such as DNA and facial images for identification purposes, see: Bulgarian Presidency of the Council of the European Union. "Schengen information system: agreement between the Council Presidency and the European Parliament." Accessed June 26, 2018.

pulled the strings behind the 2015 Paris attacks, was able to travel unimpededly within the EU as well as exit and re-enter Europe many times between 2013 and 2015. Similarly, Anis Amri, the perpetrator of the Berlin Christmas market attack in 2016, had been denied asylum in Italy and was registered as a terrorist suspect; yet, he could enter Germany and murder twelve people.

2 . ADDRESSING THE WEAK SPOTS – EASIER SAID THAN DONE

In late 2015, interoperability became a top priority for European decision-makers. A key trigger was the series of coordinated terror attacks that shook Paris on 13 November, killing 130. Appalled, European Ministers invited the Commission to draw up appropriate proposals, particularly on improving information exchange.[8] They specifically stressed the need to 'ensure' the systematic storage and sharing of data as well as improved links between databases.[9]

Coming shortly after the Paris attacks, the Brussels bombings of 22 March 2016 provided renewed momentum. In their aftermath policymakers reiterated their commitment to "increase as a matter of urgency the systematic feeding, consistent use and interoperability of European and international databases in the fields of security, travel and migration."[10] A first practical step was taken in April 2016 when the Commission presented its *Communication on Stronger and Smarter Information Systems for Borders and Security.*[11]

The document officially recognised "the need to improve the interoperability of information systems as a long-term objective".[12] Although it lacked fully-fledged proposals on how to better connect EU information systems, it sparked widespread discussion and paved the way for interoperability.[13] A high-level expert group was created and tasked with the development of practical

8. Council of the European Union. "Conclusions of the Council of the EU and of the Member States meeting within the Council on Counter-Terrorism", Press Release (848/15), Brussels, November 20, 2015; European Council. "European Council meeting (17 and 18 December 2015) – Conclusions" (EUCO 28/15), Brussels, December 18, 2015.
9. European Council. "European Council meeting (17 and 18 December 2015) – Conclusions" (EUCO 28/15), Brussels, December 18, 2015, p. 3.
10. Council of the European Union. "Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016", Press Release (158/16), Brussels, March 24, 2016.
11. European Commission. "Communication from the Commission to the European Parliament and the Council; Stronger and Smarter Information Systems for Borders and Security" (COM(2016) 205 final), Brussels, April 6, 2016.
12. European Commission. "Communication from the Commission to the European Parliament and the Council; Stronger and Smarter Information Systems for Borders and Security" (COM(2016) 205 final), Brussels, April 6, 2016, p. 2.
13. Council of the European Union. "Outcome of the Council Meeting; 3461st Council meeting Justice and Home Affairs" (8065/16), Luxembourg, April 21, 2016; Council of the European Union. "Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area" (9368/1/16 REV 1), Brussels, June 6, 2016; European Parliament. "European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017" (2016/2773(RSP), Strasbourg, July 6, 2016;
Jean-Claude Juncker. "State of the Union 2016", September 14, 2016. Accessed June 21, 2016.
European Council. "European Council meeting (15 December 2016) – Conclusions" (EUCO 34/16), Brussels, December 15, 2016.

guidance and a strategic vision.[14] On the basis of the group's final report from May 2017, the European Council invited the Commission to draft suitable legislative proposals.[15]

Consequently, two interoperability regulations were proposed in December 2017: one on borders and visa, the other on police and judicial cooperation, asylum and migration.[16] The remainder of this section takes a closer look at the latter and provides an overview of the ways in which it seeks to address current problems through different dimensions of interoperability.

The Commission's legislative proposal is now being discussed within the Council and its preparatory bodies. In particular, it seeks to improve the three main centralised information systems (SIS, VIS, EURODAC) and suggests the creation of three complimentary systems:

- an **Entry/Exit System (EES)** for recording data on short-stay third country nationals (to be in place by 2020);
- a **European Travel Information and Authorisation System (ETIAS),** a mostly automated tool for collecting and verifying travel data of visa-exempt non-EU citizens before their arrival within the Schengen area (comparable to the U.S.-American Electronic System for Travel Authorization);
- a centrally managed **European Criminal Record Information System for third country nationals (ECRIS-TCN system).**

Creating these three new centralised systems aims at filling current information gaps and remedying some shortcomings. For instance, centralising the registration of non-EU citizens entering and exiting the Schengen area will facilitate the detection of over-stayers and the identification of undocumented persons. Central electronic and increasingly automated registration will largely replace manual document stamping and thereby not only minimise the margin for error and fraud but also contribute to improving data quality by applying a coherent framework for data collection (e.g. alphanumeric data, four fingerprints, facial image).

These measures are also designed to mitigate the complexity and fragmentation of EU information systems. The introduction of a centralised database with information on the previous convictions of non-EU nationals would significantly facilitate information exchange and day-to-day police work. It would offer a one-stop-shop solution and speed up the process, where previously each EU country had to be contacted one by one to retain a third country national's criminal history, often leading to technical or procedural problems.

14. European Commission. "Commission Decision of 17.6.2016 setting up the High Level Expert Group on Information Systems and Interoperability" (C(2016) 3780 final), Brussels, June 17, 2017.
15. Council of the European Union. "Final report by the High Level Expert Group on Information Systems and Interoperability" (HLEG)8434/1/17 REV 1), Brussels, May 15, 2017; European Council. "European Council meeting (22 and 23 June 2017) – Conclusions" (EUCO 8/17), Brussels, June 23, 2017, p. 2.
16. European Commission. "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226" (COM(2017) 793 final), Brussels, December 12, 2017; European Commission. "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)" (COM(2017) 794 final), Brussels, December 12, 2017.

Further, the draft regulation foresees measures to improve the connectivity of existing EU databases. It concretely lists four corresponding technical components that are to be shared (see figure 2):

- the **creation of a European Search Portal (ESP),** serving as a single search interface from which multiple systems can be checked simultaneously to produce combined results;
- he **establishment of a shared biometric matching service (shared BMS),** for gathering and comparing biometric data from EU information systems;
- the **creation of a multiple-identity detector (MID),** which will check individual identity data across systems and flag multiple or divergent entries as well as indications of possible identity fraud;
- the **establishment of a common identity repository (CIR)** for storing biographical and biometric identity data of third country nationals.

> "THESE TOOLS WOULD FUNCTION AS COMMON BACK-UP COMPONENTS CONNECTING THE DIFFERENT INFORMATION SYSTEMS

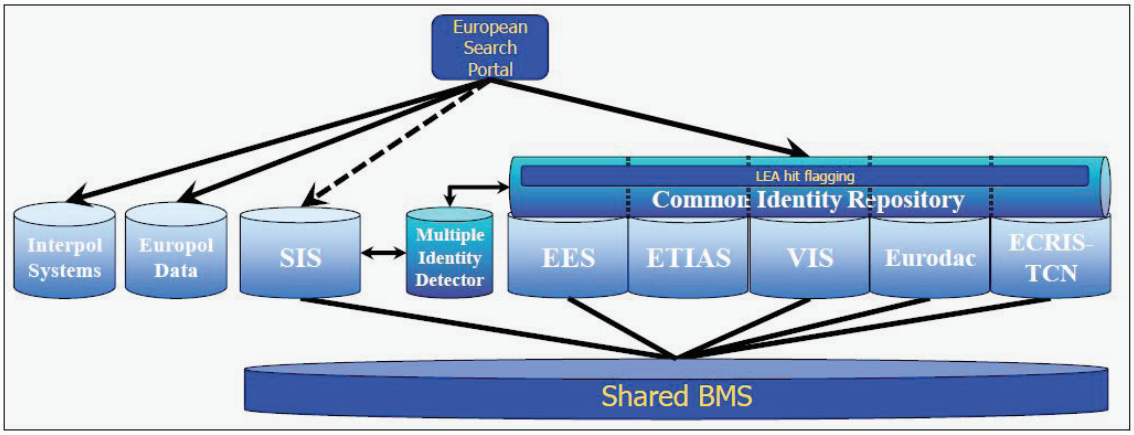
These tools would function as common back-up components connecting the different information systems. While they do not merge individual systems, they could crucially enhance their interoperability as technical bridges between different data silos, that is, if they are designed and implemented properly. A single search interface for police officers and border guards aims at making cumbersome one-by-one queries of multiple isolated databases superfluous and reducing the complexity of different rules and procedures. An ESP thus shows huge potential as an efficiency-maximiser, effectively reducing workload and time investment and minimising margins of error and the likelihood of missing information.

The same holds true with regard to all of these technical components that connect and (part-) automate information exchange. They facilitate access to data by simplifying search procedures and linking information across systems. Such cross-checks enhance data quality and improve among others the correct identification of individuals (e.g. through coherent data sets across databases).

In addition, these interoperability components are intended to include data from the European Police Office (Europol) for the first time. The strict limits on law enforcement access has frequently caused problems even in relevant cases. The Commission's legislative proposal would create a two-step process to enable authorised end-users like border guards and police officers to query the common identity repository (CIR). Although this would facilitate police access, it would not alter the strict access rules. Police officers would only be able to make use of automated searches via the new CIR to find out whether and where data on a particular subject is stored. However, they would still have to make a formal access request.

What's more, the CIR component would on the other hand enable select authorities to search Europol databases simultaneously with the centralised EU information systems. It is expected that this will result in a significant time and efficiency improvement in the daily work of practitioners working in the field of police and judicial cooperation, asylum and migration.

FIGURE 2 ▪ Overview of proposed technical components and the resulting interoperability solution



Source: European Commission. "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)" (COM(2017) 794 final), Brussels, December 12, 2017, p. 6.

The proposed regulation also foresees three additional measures. These are aimed at strengthening the implementation process by individual member states, improving data security and data protection as well as data quality. The legislative proposal thus recommends:

- a **central repository for reporting and statistics (CRRS)** as a tool to correlate anonymous statistical data across systems,
- a **Universal Message Format (UMF)** as EU-wide standard for a common and unified technical language across systems, and
- **automated data quality control mechanisms and common quality indicators** across systems, such as automatic validation rules during data insertion.

All three tools target the cross-national harmonisation and standardisation of procedures and processing related to data collection and exchange. They seek to remedy shortcomings of the current EU information systems through the regular review and streamlining of procedures and the functional operation of databases. Concretely, these components target persistent inconsistencies within and across individual systems that now cause duplication or omission of information as well as incomplete or even incorrect data.

The draft regulation seeks to remedy this in several ways. In particular, the introduction of automated controls could help avoid multiple or incomplete entries of personal information pertaining to the same individual. In conjunction with the other instruments, especially the multiple-identity detector and the more coherent processing of biometric data, these controls should prove crucial in reducing the scope for identity fraud and security gaps. Additionally, they will provide a concrete framework for accessing and feeding common databases.

This is particularly relevant in the light of persistent differences in operational and communication standards among authorities, which so far often pose procedural problems and unnecessary obstacles to EU information exchange. The draft regulation therefore suggests the introduction of universal message standards. These will facilitate the access of EU information systems, because they would enable national law-and-order officials to make more targeted

searches and fewer ambiguous queries. They would likewise enhance communication across borders and authorities irrespective of their technical systems or operational culture.

The CRRS aims at cutting through the complexity of the rapidly evolving network of EU information systems, detecting gaps and shortcomings as they emerge. Cross-system analyses of statistical data could help to continuously assess and update the technical and operational architecture. They could also produce unique, novel insights through connecting the dots where national investigations would have focussed on single, case-relevant information alone.

Finally, the draft regulation foresees extensive training for practitioners and especially end-users and suggests giving the Commission implementing powers to ensure the uniform transposition and application of the different interoperability components into national systems.

3 . FIVE TYPES OF CHALLENGE ALONG THE WAY

Although considerable progress has been made since the proposal was introduced in December 2017, much remains to be done before it can be adopted. While the Commission's proposed measures for EU policing are promising in many regards, a number of If's and But's remain. The draft regulation itself recognises that the interoperability components still raise "legal, technical and operational issues including on data protection."[17] This section therefore takes stock of potential stumbling blocks, possible risks and unintended consequences. It identifies five types of challenge: legal, technical and operational as well as data protection and safety.

3.1 Legal challenges

Diverging legal frameworks complicate attempts at harmonisation let alone interconnection. National systems and problems of implementation are likely to continue hindering interoperability at the EU level, even once the Commission's legislative proposal is adopted. One of the most crucial problems so far has been restricted law enforcement access, which is a cross-cutting issue. However, whether and to what extent the measures foreseen by the Commission will ultimately improve European policing and make it more efficient remains to be seen. It might change access rules at the EU level, but it will not significantly alter national legal frameworks and organisational cultures. This is a political question after all.

> "THE REGULATION'S SUCCESS OR FAILURE DEPENDS ON NATIONAL IMPLEMENTATION

The regulation's success or failure thus crucially depends on national implementation. The uneven application of existing legal frameworks governing the respective information systems continues to pose a problem for law enforcement and is unlikely to be solved completely by the draft regulation. Police officers' access to the visa information system and the EU's fingerprint database, for example, varies greatly across member states, and procedural problems often bedevil operational practice.

17. European Commission. "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)" (COM(2017) 794 final), Brussels, December 12, 2017, p. 16.

While the Commission may entice member states with financial and technical support or threaten with infringement proceedings, the Prüm framework shows that the political will of each country remains key. Different legal cultures continue to pose obstacles to information sharing. Certain types of data may, for example, not be used as evidence in some countries. Similarly, national authorities often hesitate to share information because separate judicial traditions might either lead to immediate penal action or give more leeway to decide how to process information. Even where common EU guidelines exist, trust grows only slowly.

Consequently, member states and the EU should ensure that legal frameworks are properly adapted and implemented. Four specific recommendations can be made:

- Member states and the EU should **establish legal clarity regarding which rules and principles apply** in an interconnected architecture, for example through the clear definition of the governance framework, controllership, data protection regimes and access criteria for each database.

- Member states need to **intensify efforts to harmonise national legal frameworks,** in particular criminal and data protection laws.

- Both should **facilitate the full and coherent transposition and application of the different interoperability components** into national and EU systems, including the complete roll-out of technical extensions.

- Both should **reconcile differences in organisational cultures,** for example through adequate training of practitioners or the promotion of exchange programmes.

3.2 Technical challenges

Challenges also remain at the technical level. Once again, national implementation problems become manifest in the slow or incomplete roll-out of single technical components such as missing electronic connections, for example to Europol systems. Particular database extensions, search interfaces or information networks are not always or only insufficiently integrated across EU member states. This lack of technical integration is often the case because existing domestic databases take priority, particularly if capacity is limited.

The Commission's proposed tools have been designed to impose minimal additional burdens on the member states. Notwithstanding the advantage of tasking the EU with the central provision and maintenance of common databases and communication infrastructure, national levels remain key in the successful operation of these instruments. Even if universal messaging formats and automated data controls are provided by the Commission, in the end each member state has to technically integrate these interoperability solutions.

Nonetheless, inefficient technical roll-out is not only a national problem. Persistent fragmentation of databases can likewise be found at EU level. Europol has not completed connections to the visa information and fingerprint database to date and its use of the SIS remains very low. In turn, Europol's internal databases such as the Europol Information System (EIS) and other systems for the purpose of criminal investigation and counter-terrorism remain quite separate from EU information systems.

Needless to say, these technical issues directly affect the operational dimension of European police work and the envisioned interoperability framework. This might perhaps be remedied by the common identity repository, which allows Europol to directly search all these databases. At the same time, the SIS is exempt from this instrument, and a basic tension remains between technically interconnecting police and non-police databases without opening them up too much and altering data protection rules. How to walk this tightrope will be critical.

Last but not least, putting into effect the proposed interoperability solution with all its components and their technical architecture presents a massive task in itself. Eu-Lisa has been mandated to do this with all four main instruments. The simultaneous technical development of these components, as well as their integration into existing structures and data migration across systems, is highly complex. What's more, once the tools have been developed, they need to be rolled out to member states and end-users, and require regular maintenance and permanent technical review. The proposed regulation provides an indication of this mammoth task when it sets an initial 9-year time-scale (2019–2027) with an estimated budget of EUR 461 million in total.[18]

A number of policy options should address these technical challenges:

- Member states and the EU should **make available sufficient technical, financial and human resources** to guarantee the proper and complete implementation of the different components at national and EU level (and the complete roll-out and integration of technical extensions).

- Member states should **ensure adequate practical training of end-users** with regard to the technical management and functional operation of interoperability interfaces and components, including promoting common communication standards and the uniform use of centralised procedures.

- Member states, with EU assistance, should **monitor and review the swift implementation of automated quality controls,** guaranteeing sufficient and high-quality data input as well as regular updating and maintenance of national systems.

3.3. Operational challenges

Operational issues also remain in the way of achieving interoperability. Data quality continues to present a challenge because common minimum standards are not enacted by all member states. Even if the Commission's proposed measures for a universal message format and automated quality controls are good, they hinge on swift, correct, and comprehensive implementation at national and local level. Operational and police cultures or a lack of capacity could still present obstacles to the coherent and consistent use of common standards.

Another hindrance is the lack of data input – another highly political question. Especially with regard to Europol's systems, national authorities still do not share information as much as re-

18. European Commission. "Amended proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration) and amending [Regulation (EU) 2018/XX [the Eurodac Regulation],] Regulation (EU) 2018/XX [the Regulation on SIS in the field of law enforcement], Regulation (EU) 2018/XX [the ECRIS-TCN Regulation] and Regulation (EU) 2018/XX [the eu-LISA Regulation]", Brussels, June 13, 2018, p. 87.

quired. Even if EU systems were perfectly interoperable, this would be of little use to European policing if no or only limited data were available in the respective databases. With regard to Europol, an independent study found that little information was shared because of a "lack of knowledge, time and awareness" among end-users.[19]

While the introduction of centralised search functions and automated tools is a step in the right direction, their proper and effective functional operation depends to a large part on the training of end-users and their willingness to join in. Measures need to be taken to raise the awareness and knowledge of law enforcement officers and security officials with regard to the new interoperable EU information systems, and to encourage and enable them to effectively share information via these databases. Three policy recommendations can be made in particular:

- Member states and the EU should **provide adequate and cross-cultural training and exchange opportunities** for end-users with an emphasis on the feeding and operation of existing and new systems.
- Member states should **dedicate sufficient technical, financial and human resources** to their respective law and order authorities and affected practitioners.
- Member states should **further facilitate, streamline and harmonise their access and exchange procedures** across national authorities and databases so as to ensure the efficient execution of information-sharing requests via central systems.

3.4 Data protection challenges

Interoperability has become something of a contentious buzzword, perhaps evoking fears about data protection. Many EU citizens may be concerned about potential impacts upon their privacy. Although the suggested interoperability solution will for the most part not directly affect EU citizens, since its individual components largely relate to third-country nationals, these remain valid concerns. Does interoperability mean more data will be collected? Does it mean more people will have access to personal information?

> "NO ADDITIONAL INFORMATION WILL BE COLLECTED

The short, official answer to these questions is 'no.' The Commission explicitly stated that "no additional information […] will be collected" and that data access rights will not be altered.[20] What interoperability does mean is "that authorised users (such as police officers, migration officials and border guards) have faster, seamless and more systematic access to the information they need to do their jobs."[21] Data would neither be shared indiscriminately among users nor would it be generically interconnected across systems. On the contrary, the draft regulation aims at fixing current shortcomings to improve targeted use and intelligent access.

Nonetheless, the proposed regulation would substantially alter the European information management architecture as well as the processing of personal data. If access to databas-

19. See Disley, Emma, Irving, Barrie, Hughes, William, and Patruni, Bhanu. "Evaluation of the implementation of the Europol Council Decision and of Europol's activities", Cambridge, 2012, p. 61.
20. European Commission. "Frequently asked questions – Interoperability of EU information systems for security, border and migration management", Strasbourg, December 12, 2017.
21. Ibid.

es is streamlined but the legal frameworks of the underlying systems remain unaltered, this might lead to confusion as to which rules and principles apply.

Data protection concerns also remain in place should the adoption of the interoperability framework be rushed through at the expense of its data protection regime. This is arguably even more vital, because MEPs have already opted for early adoption of the legal bases for other measures such as the Entry/Exit System, the European Travel Information and Authorisation System and the centralised database on third-country nationals' criminal history. If individual components become operational before controllership, access conditions and discrimination safeguards have been clearly defined, this could open the floodgates to abuse and infringement.

Establishing legal clarity with regard to data protection is vital when it comes to law enforcement access to non-law enforcement databases. This should in theory not pose too much of a problem, as the draft regulation mirrors EU data protection laws, including those deriving from the EU Charter of Fundamental Rights as well as from the latest additions: the General Data Protection Regulation (GDPR) and the Data Protection Directive for police and criminal justice authorities.[22] If executed appropriately, interoperability could contribute to a more reliable, more accessible and easier identification of individuals in line with the principles of subsidiarity and proportionality.

However, the strong connection of the interoperability framework to the EU data protection framework has yet to play out in practice. The proposed regulation charges, at EU level, the European Data Protection Supervisor with monitoring processing of personal data, and at the level of the member states mandates the national supervisory authorities created by the GDPR to do so. This could prove problematic, because these designated domestic authorities already lack the financial and human resources to carry out these tasks adequately in all areas.

If concerns are properly addressed, the legislative proposal could also strengthen EU data protection instead of weakening or undermining it.[23] A more streamlined EU information sharing culture with common technical tools and processes renders multiple registrations in different countries and with different authorities superfluous. Instead of providing complete personal information like fingerprints and alphanumeric data several times because of lack of access to the same data already stored elsewhere, a single set of such data would normally suffice and then be made available to authorised users and other systems where necessary.

This would likewise mean that a single, harmonised data protection framework would apply to the storage, sharing and retention of this data. A further positive benefit with respect to data safety and accountability would be that personal information would not be reproduced and stored in various systems. Especially with a view to increasing transparency, EU citizens exercising their right of access – that is, requesting information on whether personal data related to them is being processed – would benefit from this clear single search opportunity.

22. European Commission. "Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)" (COM(2017) 794 final), Brussels, December 12, 2017, p. 12 ff.
23. See Chapter VII on data protection.

However, to reap the benefits of strengthening data protection across information systems, the EU and its member states must address the outstanding challenges and concerns. They could do this in a number of ways:

- Member states and the EU should **ensure that interoperability components do not become operational before the underlying legal instruments** have clearly defined their

  - purpose, scope and functions,
  - applicable controllership and data protection regime,
  - access criteria and conditions,
  - discrimination safeguards.

- Both need to **lay down concrete safeguards to balance security opportunities with protection of fundamental rights,** warranting that interferences are strictly necessary and proportionate and putting safeguards against potential discrimination or unfavourable decisions into place, especially with a view to personal data held on children among others.

- Both should **ensure adequate practical training of end-users** with regard to the applicable data protection regime(s).

- Both should **guarantee sufficient financial and human resources** for the fulfilment of data protection obligations and compliance monitoring.

- The **EU should be charged with aiding, monitoring and regular reviewing the implementation process** at the (supra-)national levels, especially with regard to the data protection and safety provisions.

3.5 Data safety challenges

Data protection presupposes adequate data safety of the central information systems. How to protect data appropriately if stored in a single place and operationally managed by one entity will be a key question in this regard. The central accumulation of large quantities of highly sensitive personal data, including biographical and (increasingly) more biometric identity data, is an obvious target for cyber criminals and hackers. Although none of the information systems in question contains data on EU citizens, apart from the SIS, a successful attack on one of these servers would represent a massive privacy infringement.

The common identity repository will, for example, bring together information recorded in other central EU information systems on third-country nationals. It will create and store an individual file for each person, and eu-LISA will operate it. Although the SIS is not included, its central server, managed by France in Strasbourg, is arguably vulnerable. If one of these central servers is hacked, the identity of hundreds of thousands of persons could be stolen in one go.

> “
> SUCCESSFUL CYBER ATTACKS WOULD HAVE GRAVE CONSEQUENCES

Given the increasing collection of biometric data – intended to make security checks easier and enhance the correct identification of individuals – successful cyber attacks would have grave consequences. Criminals could steal fingerprint copies, thereby gain access to the personal devices and files of individual users and commit identity theft. Terrorist group ISIS is

already known to replicate stolen fingerprints so as to trick biometric sensors of border and police authorities. Whether a vast biometric database would have helped to expose the Paris attackers who entered the EU on fake Syrian passports seems questionable in light of increasingly sophisticated techniques for fingerprint replication.

These security concerns need to be considered carefully when designing the central databases and their safety measures. The positive effects of the advanced centralisation and interconnection of EU databases on the security of European citizens hinge on adequate data safety and protection from theft and abuse. If databases are designed with only immediate protection from cyber attacks in mind but lack adequate measures for detection, defence and recovery, this has severe implications for overall cyber resilience of an interoperable architecture of EU information systems.

Yet, even once the technological, systemic and procedural preconditions for cyber security and data safety have been established, risks remain concerning zero-day vulnerabilities and social engineering. If end-users are not sufficiently aware of these potential threats and vulnerabilities are not identified and patched up as soon as possible, centrally stored data continues to be vulnerable.

All these challenges and more must be dealt with before European databases can be better connected and have a meaningful, yet proportionate impact on the improvement of police work across the EU. And, of course, potential privacy risks remain, as is the case in all large-scale information systems. At the same time, the proposed regulation has great potential for strengthening not only European information systems and police work but the EU's internal security and the safety of its citizens. To this end, member states and the EU could take a number of measures to guarantee the safety of the centrally stored data:

- Member states and the EU should **guarantee and maintain appropriate investment and training in cyber security and risk resilience** at the levels of technology, infrastructure, process design and functional operation.

- The EU, particularly eu-LISA, should **ensure the highest possible protection of central servers,** including through awareness training, systemic risk detection and patching of vulnerabilities, appropriate cyber defence and emergency protocols, and regular review and update procedures.

- Member states and the EU should **ensure the highest possible protection of stored information** and minimise the risk of exposure to hacking, including through the comprehensive use of end-to-end encryption technologies at all levels of data collection, insertion and exchange.

- Both should **put in place robust monitoring and review mechanisms** and regularly adapt the interoperability framework and its components in response to emerging gaps and changes in the criminal and cyber landscape.

- Both should **make use of EU threat assessments** to anticipate new criminal trends and methods of identity theft and fraud and adapt information systems accordingly.

CONCLUSION: ON THE RIGHT PATH, YET STILL A WAYS TO GO

In light of the migration and refugee crisis as well as the terrorist attacks over recent years, there is no doubt that enhancing information sharing must be a priority target for EU policy-makers. Effectively managing Europe's external borders and strengthening its internal security is not only an operational necessity, it is increasingly important as a political question of the Union's survival as well.

And indeed, the EU has woken up to the challenge and has undertaken the first steps towards an interoperability framework of its information systems. As discussions on the legislative proposal are on-going, this paper has tried to make the complex and highly technical topic more accessible. It has provided an overview of the EU's current landscape of information systems and its weaknesses (shortcomings, gaps, incompatibility and fragmentation). It has outlined the Commission's proposal and the ways in which it seeks to remedy these weak spots. And finally, the paper has pointed out five types of challenge along the way (see table 1).

TABLE 1 . Five types of implementation challenges and policy options

	CHALLENGES	POLICY OPTIONS
Legal	• differences in national legal frameworks and cultures inhibit information sharing • uneven national implementation of existing legal frameworks • restricted law enforcement access to EU information systems	• establish legal clarity through the precise definition which rules, principles and procedures apply • continue and intensify the harmonisation of national legal frameworks, in particular criminal and data protection laws • reconcile differences in organisational cultures through adequate training and exchange programmes • make available financial and human resources to ensure the transposition into national and EU systems
Technical	• slow or incomplete roll-out of single technical components • slow or incomplete technical integration at the national and EU level • factual complexity and magnitude of technical realisation across EU and national levels	• make available sufficient technical, financial and human resources to guarantee the correct and complete implementation at the national and EU level • ensure adequate practical training of end-users with regard to the technical management and functional operation of interoperability interfaces and components • monitor and review the implementation of automated quality controls, data input and the regular updating and maintenance of national systems

Operational	• lack of data quality due to different national standards, lack of capacity or knowledge • lack of data input due to lack of trust, capacity or awareness	• provide adequate and cross-cultural training and exchange opportunities for end-users • dedicate sufficient technical, financial and human resources to affected authorities and practitioners • harmonise access and exchange procedures for the efficient execution of information-sharing requests via central systems
Data protection	• legal uncertainty due to multiple legal bases and frameworks governing different databases • early adoption and implementation of measures without clear definition of underlying legal framework and data protection regime • shortage of human and financial resources in national supervisory authorities	• ensure that interoperability components do not become operational before the underlying legal instruments have clearly defined their purpose, scope and functions • define safeguards to balance the security opportunities with the protection of fundamental rights • ensure adequate data protection training of end-users • make available sufficient financial and human resources for the fulfilment of data protection obligations and compliance monitoring • charge the EU with aiding, monitoring and regular reviewing the implementation process
Data safety	• higher risk of cyber attacks • increasing collection and reliance on biometric data without sufficient or adequate safeguards at all levels to prevent identity theft and fraud	• guarantee investment and training in cyber security and risk resilience at the levels of technology, infrastructure, process design and functional operation • ensure the highest possible protection of central servers • ensure the highest possible protection of information • put in place robust monitoring and review mechanisms and adapt systems to the criminal and cyber landscape • make use of EU threat assessments and reports to anticipate new criminal trends

Both the EU and its member states are called upon to address these challenges. The practical merits of the proposed remedies for shortcomings within the EU information landscape hinge on national implementation as well as support, coordination and oversight from the EU. Not surprisingly, an important cross-cutting measure will be the adequate and sufficient provision of technical, financial and human resources to enable the proper and complete implementation of the different components at national and EU level.

A thorough multi-level effort will also be key when it comes to monitoring and guaranteeing the proper and proportionate functioning of the improved data management architecture and its components, once the draft regulation has been adopted. This is, as always, also a question of political will. With regard to data safety and protection, a close eye should also be kept on the proposed EU "Cybersecurity Act" that is being negotiated in parallel.[24] It could directly impact cross-border data flows, giving it a direct role in the interoperability context.

The European Council and the Justice and Home Affairs Council will next meet on 20 September and 11 October respectively to further discuss internal security cooperation and information exchange. When and how the draft regulation for interoperability is adopted and applied is ultimately up to them. However, time is of the essence in a globalised world where criminal and cyber landscapes constantly change.

While the concrete stipulations of the framework should obviously not be rushed, and potential challenges and stumbling blocks addressed beforehand, policymakers should aim at early adoption of the definitive proposal. This would be an excellent first step in improving the fragmented landscape of EU information systems as they have developed over recent decades. At the same time, it would be just the start of a much longer journey towards a European interoperability architecture that is secure, proportionate, fully functional and operational.

ON THE SAME TOPIC

- Valentin Kreilinger, "A watchdog over Europe's policemen: The new joint parliamentary scrutiny group for Europol", Policy Paper No. 197, Jacques Delors Institute Berlin, June 2017
- Jacques Delors, António Vitorino, Pascal Lamy, Enrico Letta, and Yves Bertoncini, "The EU and our collective security: Stronger together", Tribune, Jacques Delors Institute, June 2016
- Jacques Delors, António Vitorino, Yves Bertoncini and the members of the Jacques Delors Institute's 2015 European Steering Committee, "Schengen is dead? Long live Schengen!", Tribune – Viewpoint, Jacques Delors Institute, November 2015
- Yves Bertoncini and António Vitorino, "'Schengen', terrorism and security", Tribune – Viewpoint, February 2015

24. European Commission. "Proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act')" (COM/2017/0477 final – 2017/0225 (COD)), Brussels, September 13, 2017.

Managing Editor: Henrik Enderlein ▪ The document may be reproduced in part or in full on the dual condition that its meaning is not distorted and that the source is mentioned ▪ The views expressed are those of the author(s) and do not necessarily reflect those of the publisher ▪ Jacques Delors Institut – Berlin cannot be held responsible for the use which any third party may make of the document ▪ Original version ▪

NOTRE EUROPE JACQUES DELORS INSTITUTE
Hertie School of Governance
Friedrichstraße 194, D – 10117 Berlin
info@delorsinstitut.de
www.delorsinstitut.de