

Advantages and disadvantages of interoperability of the European  
Union information systems in the areas of borders and security.  
Recommendations for the overcoming challenges.

Marta Miłkaszewicz

A dissertation submitted to Aberystwyth University in partial fulfilment of the requirements  
for the degree of MA/MSc under Alternative Regulations

Department of Information Studies

Aberystwyth University

2019

## Summary

This dissertation aims to identify the advantages and disadvantages of interoperability of European Union (EU) information systems in the areas of border and security and to make recommendations for the identified challenges. Additionally, this dissertation aims to identify the disadvantages and advantages of interoperability, describe the legislative developments in EU in terms of interoperability and identify and describe the borders and security systems which are supposed to interoperate.

This paper is a single method qualitative study. The dissertation's author uses an inductive approach and a thematic analysis method. For the *Literature Review* chapter, the professional literature is analysed. For the *Results* and *Recommendations* chapters, the author uses purposive sampling to retrieve documents produced by the European Union Institutions and documents developed by NGOs, think tanks and academic institutions, which were the most probably to answer on the dissertation's research questions and meet the dissertation's objectives. All of the documents focus on two *Proposals* concerning interoperability: *COM(2017)793* and *COM(2017)794*.

During the document analysis, author categorized the advantages and disadvantages of interoperability of EU information systems in the areas of borders and security into two main categories: data quality (personal data, biometrics) and data protection (data minimization, purpose limitation, data retention, access to data, sharing the data with Third countries). It is noted, that the main issues of interoperability are its implementation and complexity. It is necessary to improve the data quality of the legacy systems prior to implementing interoperability. Moreover, there is a danger of purpose limitation and data minimization. Therefore, to limit this interoperability disadvantage, it is proposed to limit the data stored in the databases and limit the access of law enforcement officials to CIR.

## Table of contents

List of tables .....	6
Abbreviations .....	7
Definitions .....	8
Acknowledgements .....	9
1. Introduction.....	10
2. Literature Review .....	15
2.1. Technical aspects of the interoperability .....	16
2.2. Semantic aspects of the interoperability .....	17
2.3. Political and human aspects of interoperability.....	19
2.4. Security and reliability aspects of interoperability.....	20
2.5. Business and legal aspects of interoperability .....	22
3. Methodology .....	25
3.1. Introduction.....	25
3.2. Limitations to the research .....	25
3.3. Literature review methodology.....	26
3.4. <i>Results and Recommendations</i> methodology .....	29
3.4.1. Sampling method .....	29
3.4.2. Approach .....	30
3.4.3. Method .....	30
3.5. Alternative approaches and methods .....	36
3.6. Ethics .....	37
4. Results .....	39
4.1. Legislative development in the EU in terms of interoperability .....	39
4.2. Data quality, data retention and data subject's access to their own data .....	43
4.3. Data minimization, purpose limitation, access to data, sharing the data with Third countries 45	
5. Recommendations.....	50
5.1. Data quality, data retention and data subject's access to their own data .....	50
5.1.1. To improve the data quality of legacy systems and test automatic data quality checks prior to their entry to operations.....	50
5.1.2. To implement data biometrics standards .....	51
5.1.3. To promote Universal Message Format (UMF).....	52

5.1.4.	To add the requirement of revision and update of the user profiles within central management of the interoperable system .....	52
5.1.5.	Training.....	52
5.1.6.	To clarify the data retention policy .....	52
5.1.7.	To create an EU-wide portal handling requests related to the data access, rectification, erasure, restriction and data’s subject claims for changing decisions based on the data stored in the system .....	53
5.1.8.	To define a valid search mode for the European Search Portal.....	53
5.1.9.	To create a safeguard, that the owners of Interpol data (Third countries) will not have access to the information that their data was accessed and by which country .....	53
5.1.10.	To add a flag in a system, when yellow alerts appear as a result of inconsistencies with data stored in <i>ETIAS</i> .....	54
5.1.11.	To designate eu-LISA and authorities in the Member States as a joint data quality controllers .....	54
5.1.12.	To add child protection objective.....	54
5.2.	Data minimization, purpose limitation, access to data, sharing the data with Third countries	54
5.2.1.	BMS should match the data not to store it .....	54
5.2.2.	To remove unnecessary data from CIR .....	55
5.2.3.	To allow law enforcement access CIR only for “the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case” (Article 22, COM(2017)793).....	55
5.2.4.	To introduce safeguards for protecting the data against unauthorised access.....	56
5.2.5.	To clarify the conditions under which eu-LISA has access to the interoperable databases.....	57
5.2.6.	To remove <i>ECRIS-TCN</i> from MID .....	57
5.3.	System governance .....	57
5.3.1.	To improve the governance of the interoperable systems.....	57
6.	Conclusion .....	59
7.	References.....	63
8.	Appendix.....	72

# List of tables

**Table 1** Documents concerning legislative development of interoperability in the EU ..... 33

**Table 2** Documents concerning advantages, disadvantages of interoperability and recommendations to tackle identified challenges..... 35

**Table 3** Legislative development in EU in terms of interoperability ..... 40

**Table 4** IT systems covered by the technical components of interoperability (European Union Agency for Fundamental Rights, 2018, p. 10) ..... 42

**Table 5** “Authorities’ access to additional personal data through interoperability” (European Union Agency for Fundamental Rights, 2018, p. 10) ..... 46

## Abbreviations

<b>BMS</b>	Biometric Matching System
<b>CIR</b>	Common Identity Repository
<b>CJEU</b>	Court of Justice of the European Union
<b>DPA</b>	Data Protection Authority
<b>ECRIS-TCN</b>	European Criminal Records Information System Third Country Nationals
<b>EDPS</b>	European Data Protection Supervisor
<b>EES</b>	Entry/Exit System
<b>EIF</b>	European Interoperability Framework
<b>ESP</b>	European Search Portal
<b>ETIAS</b>	European Travel Information and Authorisation System
<b>eu-LISA</b>	The European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
<b>Eurodac</b>	European Dactyloscopy database
<b>FRA</b>	European Union Agency for Fundamental Rights
<b>Frontex</b>	European Border and Coast Guard Agency
<b>LE</b>	Law Enforcement
<b>MID</b>	Multiple-Identity Detector
<b>SIS II</b>	Second-Generation Schengen Information Systems
<b>UMF</b>	Universal Message Format
<b>VIS</b>	Visa Information System

## Definitions

---

<b>Alphanumeric data</b>	“Data represented by letters, digits, special characters, spaces and punctuation marks” (COM(2017)794)
<b>Biometric data</b>	“Fingerprint data and/or facial image” (COM(2017)794)
<b>Data minimization</b>	“Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (Regulation (EU) 2016/679)
<b>Personal data</b>	“Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data” (European Commission, n.d.)
<b>Purpose limitation</b>	“Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes” (Regulation (EU) 2016/679)
<b>Third country national</b>	“A person who is not a citizen of the Union within the meaning of Article 20(1) of the Treaty, or a stateless person or a person whose nationality is unknown” (COM(2017)794)

---

## Acknowledgements

I would like to thank Dr Sarah Higgins for the supervision of my dissertation, her guidance and support. They were priceless and without them, I would not be able to reach this point and present my dissertation.

I would also like to thank my parents – Halina and Jan Miłkaszewicz. They are the people I wrote this dissertation for – they gave me motivation and all the support I could have asked for. Dziękuję!

I also would like to mention Dr Anemona Peres and Ms Ingrida Hiunni for the interest and advice – both regarding writing process and overcoming the writer's block.



# 1. Introduction

As Marlene Mizzi, Member of European Parliament said in 2015 “The border-free Schengen Area is one of the most remarkable achievements of the EU - a beacon of European integration bringing people and countries closer together”. Within the Schengen Area, consisting of 26 countries, physical borders were abolished. Free movement is cherished by European Union citizens and visitors. It stimulates the economic growth by enabling people to live, work and travel across the borders. This is one of the four principles of European Union and as Viviane Reding, the EU’s Justice Commissioner said in 2013, “it goes to the heart of EU citizenship” (European Commission: Press Release Database, 2013). The functioning of the Schengen area should be safeguarded. The development of the European Union information systems in the areas of border and security is one way of protecting the freedom of movement. These systems vary in the functions and scope of their work.

*Eurodac* (European Dactyloscopy) was established in 2003. When a person applies for asylum, his or her fingerprints are registered in this database (European Commission: Migration and Home Affairs, n.d.). *VIS* (Visa Information System) stores data of persons who applied for a visa. This data can be exchanged between the Schengen States (European Commission: Migration and Home Affairs 1, n.d.). *SIS* (Schengen Information System) “enables competent authorities, such as police and border guards, to enter and consult alerts on certain categories of wanted or missing persons and objects” (European Commission: Migration and Home Affairs 2, n.d.). In 2016 two proposals were introduced: *EES* (Entry/Exit System) which aims to speed up the border checks of non-European Union nationals entering European Union (Díaz de Mera García Consuegra, A., n.d.) and *ETIAS* (European Travel Information and Authorisation System) which would gather information on visa-exempt travellers prior to their arrival (European Parliament: Think Tank, 2017). One year later, *ECRIS-TCN* (European Criminal Records Information System – Third Country Nationals) was proposed. This system contains criminal records (European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, n.d.). The interoperability of these six European Union information systems in the areas of border and security is currently vividly discussed within the European community. It has been noticed, that interoperability can prevent the appearance of “blind spots”, when one person’s data is recorded under different aliases in disconnected

databases (COM (2017) 794). Already in 2016, the European Commission presented a Communication *Stronger and smarter information systems for borders and security*, which was followed on 16th of May 2017 by the *7th Security Union Report* in which the European Commission committed itself to enhance the EU information systems for security and border management interoperability.

As a follow up to this Report, on 12th of December 2017 the European Commission has published two *Proposals: Proposal for a Regulation on establishing a framework for interoperability between EU information systems (borders and visa)* (COM (2017) 793) and *Proposal for a Regulation on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)* (COM (2017) 794). These *Proposals* should be read together. In their background, authors explain motivation leading to the development of these documents. According to them, the interoperability of EU information systems in the areas of border and security is an answer to the European Union citizens requesting effective border controls and checks, higher internal security and better management of migration. These *Proposals* are currently under discussion, while the European Union Agencies (e.g. European Union Agency for Fundamental Rights, 2017), NGOs (e.g. Meijers Committee, 2017) and EU Institutions (European Parliamentary Research Service, 2017) present their arguments for and against planned interoperability of the above-mentioned systems.

The author of this dissertation intends to join this debate and aims to identify the advantages and disadvantages of interoperability of European Union information systems in the areas of borders and security. The second aim of this dissertation is to provide recommendations for the identified challenges. The interoperability within this research is understood, following Article 2 of Decision 922/2009/EC as: “the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems”.

The key research questions of this dissertation are:

- What are the advantages and disadvantages of interoperability of European Union information systems in the areas of borders and security?

- What are the recommendations for overcoming the identified challenges?

The research sub-questions of this dissertation are:

- Which systems are planned to interoperate?
- How is the interoperability planned to look?
- What are the opinions of EU Institutions and NGOs?
- What are the recommendations of EU Institutions and NGOs (if any)?

The dissertation has five main objectives:

- A literature review to identify the disadvantages and advantages of interoperability;
- A description of the legislative developments in EU in terms of interoperability;
- Identification and description of the borders and security systems which are supposed to interoperate;
- Identification of disadvantages and advantages of interoperability in terms of European Union information systems in the areas of borders and security for refugees;
- Identification of recommendations for tackling the challenges and enhancing the benefits.

The responses on the research questions are provided throughout the dissertation in each of its four main chapters: *Literature Review*, *Methodology*, *Results* and *Recommendations*. The outcomes of each chapter create a basis for the next chapter and they logically complement each other.

The advantages and disadvantages of interoperability are identified in the second chapter of this dissertation – *Literature Review*, which focuses on the professional literature (understood as an overview of texts written by the authors with knowledge and professional experience in this topic). They are grouped into separate sectors: technical, semantic, political/human, security/reliability and business/legal. The dissertation's author, following the Carnegie Mellon Software Engineering Institute (2004, p. 16) identified four themes crosscutting the above-mentioned aspects: the complexity of interoperability and its implementation, lack of links

between funding and control and links between current and legacy systems which affect the work of current systems.

In the third chapter of the dissertation – *Methodology*, the author describes in detail the methods used for the literature search; methods for identification of legislative development of interoperability within European Union; methods for identification and description of European Union information systems in the areas of borders and security which are planned to be interoperable; methods for identification of advantages and disadvantages of interoperability in terms of European Union information systems in the areas of borders and security; and finally methods for identification of recommendations for the challenges and enhancing benefits. This chapter constitutes a solid basis for the *Results* and *Recommendations* chapters, which naturally follow the *Methodology* chapter.

The chapter *Results* reports the results of the dissertation author's research. It presents the historical legislative development of interoperability in the European Union, describes the borders and security systems which will interoperate, and the disadvantages and advantages of their planned interoperability. In the last part of this chapter, the dissertation's author analyses the recommendations for enhancing the potential benefits of interoperability and overcoming its potential challenges. It discusses their applicability to the European Union information systems in the areas of borders and security. Within this chapter, first the findings will be summarized, and only afterwards critically analysed. The trends and patterns will be identified, the meaning of findings highlighted and linked to the research previously presented. To investigate the disadvantages and advantages and present the recommendations, the document analysis would be performed with a focus on:

- Data quality (personal data, biometrics)
- Data protection (data minimization, purpose limitation, data retention, access to data, sharing the data with Third countries)

Based on the *Methodology* and *Results* chapters, the solutions for both overcoming the shortcomings and enhancing the advantages of interoperability within the European Union information systems in the areas of border and security are proposed. They are described in detail in the *Recommendations* chapter. If known, the risks, costs or other barriers of the implementation of the proposed recommendations are drawn out. The recommendations are

based on the evidence (stated in the *Results* chapter). To increase the value of the research, the author of this dissertation refutes proposed solutions and compares them with recommendations proposed by other stakeholders affected by interoperability within the European Union and listed in the *Results* chapter.

This dissertation is focused solely on the European Union information systems in the areas of border and security: *Eurodac* (European Dactyloscopy), *VIS* (Visa Information System), *SIS II: police* (Schengen Information System), *SIS II: immigration control*, *EES* (Entry-Exit System), *ETIAS* (European Travel Information and Authorisation System) proposal and *ECRIS - TCN* (European Criminal Records Information System for third-country nationals) proposal. Its scope does not encompass national efforts leading towards interoperability within national border and security frameworks.

The author of this dissertation hopes, that this research piece will provide additional input into the current debate about the future of the European Union information systems in the areas of border and security interoperability. This is a topic which affects the lives of people who are entering the European Union, whether they are its citizens or not. Their data was processed by the border guards before the concept of interoperability started to be implemented. Interoperability of European Union information systems in the areas of borders and security might enhance the functioning of these systems or increase issues which are already developing. This dissertation aims to provide recommendations for identified challenges. The author of the dissertation hopes that this document will allow decision-makers to make better informed decisions in terms of the future of these systems and their planned interoperability.

## 2. Literature Review

Interoperability is inevitably linked to the development of Information and Communications Technology (ICT). With an increasing number of ICT devices, researchers started to call for interoperability in numerous articles and books. They realised that lack of interoperability will not allow the potential offered by the development of ICT devices to be fully used. However, with time it appeared that nothing comes without a cost, and interoperability, despite its obvious advantages has its drawbacks. This literature review will present the advantages and disadvantages of interoperability according to the professional and research literature. By professional literature the author of this dissertation means all texts written by authors with knowledge and experience in the topic of interoperability. Legal acts are excluded from this overview and will be described in the chapter called *Methodology*. As per reviewed literature, the real risks linked to interoperability lie in its implementation.

As interoperability is a complex issue, this chapter has been divided into separate sections listing the advantages and disadvantages of different aspects of interoperability. However, there can be distinguished general themes which crosscut the described aspects:

- Complexity of interoperability – implementation of interoperability involves considering vast amounts of aspects and liaising with many stakeholders;
- Complexity of interoperability implementation – issues linked to implementation are not limited to technical problems but they often lie in the management and lack of clear leadership;
- Funding and control are not interlinked;
- Problems linked to legacy systems (Carnegie Mellon Software Engineering Institute, 2004, p. 16)

In this *Literature Review*, interoperability has been discussed from the different angles by the authors coming from educational, governmental and business background. However, this document does not identify any iconic text discussing this subject. Each of the mentioned authors is reaching to his/her background and usually to anecdotal knowledge. The author of the dissertation aimed to achieve a broad spectrum of opinions and present their diversity with a focus on the wide topic of this document: public administration.

## 2.1. Technical aspects of the interoperability

The technical aspect of interoperability is usually the one researchers focus upon. Miller (2000) writing for *Ariadne, Web Magazine for Information Professionals* notices that there are various ways of reaching technological interoperability: informal e.g. when companies share the code of their software and formal approaches e.g. standards. In his article, he emphasises mostly standardisation as a way of achieving interoperability. Beydogan (2010) coming from an academic background agrees with the important role of the standardization, however, he also notices that too strong a standardization might affect innovation and in consequence impede market development. According to him entrepreneurs would not risk competing with one dominant standard due to fear of competing with established user perceptions. The U.S. Department of Energy (2016, p. 7) has a different opinion from Beydogan (2010) as it looks more for the market stability and it follows Miller (2000) in its urge for standardisation and points out technological challenges: the need for common standards, need for common interfaces, technological adjustments and a good, stable network. It is visible, that this governmental study considers broader, country perspectives. Seadle (2010), in an article written for the information specialists and concerning archiving in a networked world noticed that limiting efforts to the standards development is not sufficient as it is equally important that all parties agree on their use. As an example, he provides the case of different dates in the USA and in Europe. In the USA the date is written in the following format: month – day – year and in Europe as day – month – year. This format difference creates serious issues while transferring data and its metadata to another system. Researchers from Carnegie Mellon Software Engineering Institute (Meyers, B. et al., 2004) note, that standards might create a false sense of security, as very often they are inconsistent, not fully specified and even though systems are designed with them in mind, they can fail. The American National Research Council (1991) looks into the way standards are developed and adds that regional politics might interfere in this process. According to this research institute, various national bodies are trying to strengthen the positions of companies in their countries. This affects the quality of the standards and very often makes them obsolete even before their announcement. Authors add that this situation might also happen in the case of the development of national standards. Standardization is a broadly discussed aspect of interoperability, as it is one of the means to achieve it. All types of literature sources - related to information management, government

and business pay close attention to it. However, authors related to business also look into another important aspect of interoperable systems – usability. Microsoft Technet (2001) considers the technical aspect of interoperability from the user point of view. Authors of this article noticed, that interoperability usually means the reduction of system complexity for users. This opinion is confronted with the opinion by the report prepared for GridWise Architecture Council (2009, p. 3) and sponsored by an agency of the United States Government. The authors point out that thanks to interoperability new systems can be added up and work together, which might slow down their work and create unpredictable problems. Academic Sheth (1998, p. 2), in his article describing the history of interoperability, also notices this issue and adds that interoperability creates new challenges such as increased use of large amounts of data which leads to the need of additional bandwidths and development of communication methods. When there are many systems which are linked to each other in complex ways, it might be difficult to quickly allow for free, uninterrupted flows of information. Moreover, sometimes problems linked to some of those systems might not be resolvable (Gasser, U. and Palfrey, J., 2007, p. 17). The technical report of Carnegie Mellon Software Engineering Institute (2004, p. 16) complements this discussion with information that interoperability often enforces the coordination of upgrades. Beydogan (2010) adds that this focus on the technological aspect of interoperability might hinder both innovation and development of IPR-protected technologies. From the reviewed articles and reports, it seems that the technical aspect of interoperability causes the biggest number of issues. However, researchers like Meyers et al. (2004) note, that interoperability cannot be limited only to the technical side. This opinion is reiterated by the Carnegie Mellon Software Engineering Institute (2004, p. 10).

## **2.2. Semantic aspects of the interoperability**

Information professionals (Miller, P., 2000) and researchers working for the government (The MITRE Corporation, n.d.) notice that there are two forms of interoperability: syntactic and semantic. In syntactic interoperability, two or more systems communicate with each other and exchange data. The resources which were previously stored separately and available to the limited audience, can now be available for a broader audience. Previously, when someone wanted to integrate the data from one system to another, due to a system's lack of interoperability, he or she had to manually move data from one system to another (Miller, P., 2000). Interoperability assures broaden access to the information, which affects the efficiency



of the systems and people using them. As an information professional, Miller (2000) points out the importance of the semantic notion of interoperability, where the systems will not only exchange the data, but will be also able to work with it. In the systems, as with semantic interoperability, the issues impeding the efficient data transfer such as access restrictions and changes of format are eliminated (Llanes-Padrón, D. and Pastor-Sánchez, J.A., 2017). Researchers from Carnegie Mellon Software Engineering Institute (2005, p. 4) agree with Miller (2000) on the importance of semantics and provide an example of the number “5” which can be understood by one of the systems as the fifth day of the week and by the other as the highest level of risk. The authors notice, that the meaning between systems has to be agreed upon, otherwise systems will not be interoperable. This call for semantic interoperability is reinforced by Veltman (2001 mentioned in Alemu G., Stevens B. and Ross P., 2011, p. 40) who states that “the goal of semantic metadata interoperability is enabling information sharing and exchange through negotiated meanings of the terms and expressions”. There are different ways of achieving it. The Carnegie Mellon Software Engineering Institute (2005, p. 5) proposes standardization and use of mathematics. Alemu, Stevens and Ross (2011, p. 39) develop this idea in their article, and notice that metadata standards such as MARC, Dublin Core etc. and metadata interoperability approaches (e.g. metadata cross-matching, derivation and registries) seem to promote the hierarchical metadata approach, which is controlled by experts. The authors notice that this approach misses the diversity of library users and very quickly gets outdated as above-mentioned tools are rarely updated. The authors provide an example of another interoperability approach based on the collaboration – folksonomy, which is successfully used in e.g. Wikipedia (Alemu G., Stevens B. and Ross P., 2011, p. 39). The major advantages of folksonomies belong their inclusiveness, currency and self-moderation (Kroski E., 2005). Researchers explain that as libraries differ very much from each other, the common metadata hierarchical standard is unlikely to be successfully implemented (Alemu G., Stevens B. and Ross P., 2011, p. 41). Summing up, all researchers which discuss the semantic aspect of interoperability call for limited flexibility, as hierarchical structures become quickly obsolete and not usable. This aspect of interoperability is closely linked to its technical aspect, as it discusses the language ICT systems communicate with.

### 2.3. Political and human aspects of interoperability

Technical and semantic interoperability aspects are very tangible. However, interoperability has also political and human aspect. Gasser and Palfrey (2007, p. 15) in their report emphasise that interoperability brings autonomy, flexibility and choice for users. Increased interoperability leads also to increased access and diversity of services. The authors of a report sponsored by MITRE, a not-for-profit organization which is working together with the American government notice a positive aspect of interoperability. According to them interoperability can positively influence the professional developments of staff members using interoperable systems. Such staff members do not have to remember different ways of searching for information. Moreover, in case of critical situations, more people are able to operate the system (The MITRE Corporation, 2000, pp. 1-2).

However, Miller (2000), as an information specialist, in his article notices that interoperability might have certain unplanned consequences e.g. perceived loss of control or ownership. Academic Sheth (1998, pp. 2-3) has a similar opinion to Miller (2000). In his article he adds that very often interoperable information sources and systems are managed by the different organisational units. The MITRE Corporation (n.d.) provides an example of such a situation. This is called "the double tennis problem", where both players do not perform any action as they believe it is the responsibility of another player. Additionally, it might be possible that affected customers will not know from whom he or she should expect a solution for an evident issue. His or her issue might be bounced around (Gasser, U. and Palfrey, J., 2007, p. 17). Again, this drawback is connected to the implementation of interoperability. It is necessary to write appropriate agreements, which will prevent it. Establishing interoperability of resources might face reluctance from people who used to be responsible for them (Gasser, U. and Palfrey, J., 2007, p. 17). Researchers from Carnegie Mellon Software Engineering Institute (2006, p. 4) note that the owners of the interoperable system are able to control only their own systems, but not the way in which they will be used. Interestingly, Sheth (1998, pp. 3-4) seems to accept this problem and does not propose the solution, but rather creates a typology of autonomy issues. This might mean that issues linked to ownership are common and taken into account while implementing interoperability. Miller (2000), in his article, looks into system usability. According to him, interoperability might have an impact on staff members who might not know how to use systems which are new for them or how to provide service to bigger groups of users

than they used to. Researchers from the Carnegie Mellon Software Engineering Institute (2006, p. 4) looked into another psychologic aspect linked to interoperability. They noticed that, the owners of the interoperable systems might not realise that any change in their systems has an effect on other systems. Moreover, some aspects of their systems might be out of their control and even not visible for them. Therefore, the authors sum up their report with the statement that the management of interoperable systems involves the need for good communication skills, clear leadership and policies (Carnegie Mellon Software Engineering Institute, 2006, p. 8). In the case of international interoperability all the above-listed issues appear magnified by cultural differences. There are also “social exclusion issues of the widespread IT-based dissemination of information” (Miller P., 2000). To limit these drawbacks, it is necessary to support process change and provide training to staff members and users (Miller P., 2000). As will be presented in section below, such training should be related to different aspects of system use such as security and quality of data.

#### **2.4. Security and reliability aspects of interoperability**

Security and reliability are important aspects of interoperability. In the literature, authors look into these aspects from different angles. Authors related to the academic field and writing their report for the American Government (Carnegie Mellon Software Engineering Institute, 2004, p. 5) are concerned about the way interoperability can be implemented. The reliability of interoperability implementation is often dubious. Authors recognise many reasons for this. First of all, the interoperability often has to be compromised during the process of adjusting new system to system which was created earlier. This is caused by the inability of the legacy system to be upgraded (Carnegie Mellon Software Engineering Institute, 2004, p. 5). The authors of the report also notice that when systems were not designed with interoperability in mind (“interoperability by design”), they might not be able to cooperate. As an example, they provide two systems: one was supposed to track hostile and friendly aircraft, another one was responsible for tracking missiles. Unfortunately, at the beginning both systems were not designed to work together and the attempt to make them interoperable failed due to different data characteristics (e.g. frequency of collecting and refreshing) used by the two system (Carnegie Mellon Software Engineering Institute, 2004, pp. 6-7) Authors also look into the different understanding of policies and standards by different software developers. Moreover, it was recognised, that interoperability might be threatened by software upgrades, which might

break it (Carnegie Mellon Software Engineering Institute, 2004, p. 6). The reliability of implementation of interoperability is strongly linked to the technical aspect of interoperability.

On the other hand, authors related to business and government, focus on different aspect of interoperability, which appears after interoperability has been successfully implemented. According to the Gasser and Palfrey (2007, p. 17), the reliability of interoperability depends on the way in which interoperability was introduced. The researchers coming from an educational background and writing research sponsored by the business owner – Microsoft and American Government (Gasser, U. and Palfrey, J., 2007, p. 16 and The MITRE Corporation, 2000, pp. 1-2) highlighted the possible issues with privacy and security. As interoperable systems have more access points to data, it means that there are more ways to both access the systems or to harm them. Similarly, as more people have access to data, they might also have access to the personal data stored in those systems. Authors noted, that it is not really the issue of interoperability but of its implementation (Gasser, U. and Palfrey, J., 2007, p. 16). Authors provide the example of revealing the personal data of users by a third party with which the user is not in any relationship (Gasser, U. and Palfrey, J., 2007, p. 17). When the threats related to the reliability and security are too high, it might be possible that some of the companies will withdraw from the online environment (Gasser, U. and Palfrey, J., 2007, p. 17). The U.S. Department of Energy (2016, p. 7) urges for the creation of the cyber-physical security framework, which will try to predict and prevent any risk of attack or the result of mistakes in the system. It will also create a response to any potential risk and allow for quick system recovery.

Researchers from Carnegie Mellon Software Engineering Institute (2005, pp. 8-9) add that systems need to trust each other that the information processed is of value. This trust is context and time-dependent. According to the authors trust has a broader meaning than security. For example, even if the person uploading information to the system has all necessary rights, the data is correct, and the network is secure, it might be still possible that information retrieved will not be trustworthy for some particular needs. Researchers from Carnegie Mellon Software Engineering Institute (2005, p. 9) emphasise, that it is important to look at the systems as a whole package to make sure they are trustworthy.

## 2.5. Business and legal aspects of interoperability

Gasser and Palfrey (2007, p. 12) pointed out the importance from a business perspective of the notion of the interoperability – the ability to bring innovation. The authors provided an example of the Internet, to which all incompatible networks and systems have adjusted. According to the report, interoperability can boost innovation by the reduction of lock-in effects and entry barriers (Gasser, U. and Palfrey, J., 2007, p. 14). The mix between interoperability and innovation might have an impact on competition, which will result in the improvement of goods quality and lower prices. However, Gasser and Palfrey (2007, p. 14) noticed also that with interoperability the agreements between a few companies may promote only those firms. However, when there is only one platform for a few systems, interoperability might create a risk of homogeneity and hamper innovation. Systems will be evolving only in a way which this one single platform will allow them. Teece (2010, p. 185) noticed, that the “profiting from discovery is (...) difficult”. Therefore, it can be noticed, that companies which dominate the market very often do not innovate as they focus mostly on maintaining the leading position and gathering their own advantages rather than working on the development of the market. Companies which set the standard for others often do not want to change the standard as they were the ones creating it and are often bound to it and the values behind it. It is interesting to notice, that researchers were already posing this argument in the 1991 year (National Research Council, 1991, p. 71). They also added that company which heavily invested into standard development might not be willing to open it for everyone as it can be afraid of strengthening its competitors. It is worth noting, that in this report, authors also noticed that in fact standardisation supports the development of small companies, which can use the benefits of being a part of the network of companies.

When a company is building up its business model on the exclusivity as e.g. Apple, forced interoperability might have a negative effect on the company (Gasser, U. and Palfrey, J., 2007, p. 17). The innovation aspect is not as important in the case of the studies sponsored by the government. U.S. Department of Energy (2016, p. i) in its report emphasizes cost-cutting which is particularly important for public administration. The authors point out that interoperability is ultimately cheaper than customized integration. They also notice, that integrity often involves the development of specially customized device drivers in which the costs are proportional to the total number of devices (U.S. Department of Energy, 2016, p. i). The interoperability will

also reduce the upgrade and installation costs (U.S. Department of Energy, 2016, p. 9). The use of interoperable devices and systems might be cheaper than separate ones. Interoperability allows resources to be shared more freely. Sometimes, to make it happen, it is necessary to fulfil the appropriate legal requirements. Moreover, often, it is necessary to gain appropriate permissions related to the use of personal data and intellectual property rights (Miller P., 2000). It is necessary to mention two main themes which affect interoperability: uncertainty concerning legal developments and legal efforts aiming to force interoperability (especially visible within European Union countries). Unfortunately, as the authors related to business notice, the legal actions usually take an ad hoc approach and are not systematic (Gasser, U. and Palfrey, J., 2007, p. 11 and National Research Council, 1991, p. 73) notice that forced release of intellectual property rights often creates strong feelings from the companies side and quotes an owner of the company, which based on court ruling, had to release part of its protected documentation: "The fact that you have been successful does not by definition, expose you to that loss of your rights" (Gasser, U. and Palfrey, J., 2007, p. 11). This is yet another point of discussion which presents interoperability as a feature which goes much beyond a purely technical issue.

Authors referenced in this literature review agree that successfully implemented interoperability is beneficial. However, all of them draw the attention of readers into different aspects of interoperability, which should be taken into account while implementing it. In this dissertation, these aspects were grouped into five different areas: technical, semantic aspects, political/human, security/reliability and business/legal aspects. However, it is important to notice, that the advantages and disadvantages of interoperability which were described under those areas are interlinked and can often appear in two different categories.

Reviewed authors emphasise the human influence, which is visible in all aspects: technical, security/reliability and business/legal. They also notice the complexity of interoperability and emphasise that its advantages and disadvantages appear in its implementation. The implementation of interoperability involves consideration of many interrelated issues, some of which relate to legacy systems. Authors also notice that funding is not linked to control. The issue of systems control is especially striking and raised by all reviewed authors. The reviewed works also emphasise the importance of trust within systems and their ability to communicate.

Interoperability is a universal term, it is mostly used while discussing IT systems and most of the reviewed works focused on IT systems implemented in business and in military operations. This opens up a research gap, which this dissertation aims to fill in. In professional literature, there has been not much discussion about interoperability of IT systems used for public administration in the EU. This topic is rather discussed only by sources related to the EU itself. The author of this dissertation aims to use the information presented in professional literature to critically evaluate planned interoperability of EU information systems in the areas of border and security and prepare recommendations for identified challenges.

## 3. Methodology

### 3.1. Introduction

The aim of this chapter is to inform readers about the dissertation's research design and methods used. This dissertation is a single method qualitative study, where one data collection technique and the corresponding qualitative procedure are used (Saunders, Lewis and Thornhill, 2016, p. 168). The chosen approach is inductive and philosophy interpretive. The methodological choices were driven by the research questions.

The methods were chosen based on their fit for purpose and within the limits created by the constraints, among which were difficulties linked to gaining access to border and coast guards who are using information systems for processing migrants' data, and persons responsible for the development of legislation aiming to create interoperability of the above-mentioned systems. The thematic analysis of documentary sources has been considered as a method which can support reaching the dissertation's objectives within the allocated time and resources.

To ensure the validity of research in this single method qualitative study with one type of data, the author used the triangulation of documentary sources. Official documents produced by the European Union Institutions, professional IT literature and documents developed by NGOs, think tanks, academic institutions provided a base for a documentary analysis. Different perspectives offered by these resources allowed the author to obtain a broader scope of research results and, at the same time, it was possible for the author to cross-check gathered data. As it appeared not to be possible to analyse all documentary resources linked to the subject of this dissertation, the dissertation's author used purposive sampling, where the author chose to analyse the documents which could potentially support answering the research questions. In the last part of this chapter, the author looked in detail at the methodological procedures used for the dissertation's *Literature Review* and *Results and Recommendations* chapters.

### 3.2. Limitations to the research

Prior to describing the research strategy, it is necessary to present the constraints which affected the process of writing this dissertation. Among them it is possible to list:



- difficulties with reaching the border and coast guards working with analysed IT systems;
- difficulties with reaching experts developing new EU legislation;
- time constraints.

Any research which involves persons working with EU information systems in the areas of borders and security would need to receive consent from the national authorities. For the independent researcher, that would be very difficult to achieve within the time required to submit this dissertation. Additionally, the dissertation's author, while writing this piece of research worked for the European Border and Coast Guard Agency – Frontex, which is responsible for coordinating the work of border and coast guards on the European level. Reaching border and coast guards working on Frontex missions would require receiving the additional consent from the Frontex Executive Director and the need to review the dissertation by the Frontex legal office.

A similar situation relates to reaching experts developing new EU legislation. These are usually national and European level experts, which might be difficult to reach by the independent researcher. Additionally, in the work on the new legislation concerning the planned interoperability, the European Border and Coast Guard Agency – Frontex is engaged and again, performing interviews with Frontex staff members would require passing through the same internal procedure as described above.

### **3.3. Literature review methodology**

In the *Literature Review* chapter, which focused on the professional literature describing the topic of interoperability of information systems, the author first performed a general search for the documentary resources using the following terms:

- “interoperability AND information systems”
- “interoperability AND IT systems”
- “interoperability AND systems –health”
- “interoperability AND advantages”
- “interoperability AND disadvantages”
- “interoperability AND information systems AND advantages/disadvantages”
- “interoperability AND information systems AND disadvantages”
- “interoperability AND information systems AND benefits”

- “interoperability AND information systems AND difficulties”
- “interoperability AND information systems AND drawbacks”
- “interoperability AND information systems AND shortcomings”
- “interoperability AND information systems AND problems”
- “interoperability AND information systems AND issues”

The following databases and search engines were searched through:

- the University of Aberystwyth library catalogue – Primo
- Google.com
- Google Scholar
- Primo Aber Collections
- Library, Information Science & Technology Abstracts (LISTA)
- Library and Information Science Abstracts via ProQuest (LISA)

The dissertation’s author analysed the bibliographies of retrieved documents regarding their fit to the chapter’s objective and browsed through retrieved documents. When the information fitted the chapter’s objective, it has been highlighted and written down in a separate table. Among this first general set of the literature, the author identified Miller’s (2000) article, which focused on the interoperability advantages and disadvantages. Miller in his article identified and described different types of interoperability:

- Technical interoperability
- Semantic interoperability
- Political/human interoperability
- Inter-community interoperability
- Legal interoperability
- International interoperability

Under each type of the interoperability, Miller (2000) noted its advantages and disadvantages. The dissertation’s author decided to follow Miller’s categories and in the MS Word document, categorised already identified advantages and disadvantages of interoperability. Afterwards, a new search was performed. In the already mentioned databases and search engines, the dissertation’s author refined the search themes and following Miller’s types started to look for:

- “advantages AND technical interoperability”
- “disadvantages AND technical interoperability”
- “advantages AND semantic interoperability”
- “disadvantages AND semantic interoperability”
- “advantages AND political interoperability”
- “disadvantages AND political interoperability”
- “advantages AND human interoperability”
- “disadvantages AND human interoperability”
- “advantages AND inter-community interoperability”
- “disadvantages AND inter-community interoperability”
- “advantages AND legal interoperability”
- “disadvantages AND legal interoperability”
- “advantages AND international interoperability”
- “disadvantages AND international interoperability”

The author also used following synonyms of the words advantages and disadvantages: benefits, difficulties, drawbacks, shortcomings, problems, issues. New documents were retrieved. Within these documents, the dissertation’s author analysed their bibliographies and again browsed through the articles/books listed within them. With a bigger number of available documents new themes appeared. Dissertation’s author decided to broaden up the search looking for new terms:

- “advantages AND interoperability AND security”
- “disadvantages AND interoperability AND security”
- “advantages AND interoperability AND reliability”
- “disadvantages AND interoperability AND reliability”
- “advantages AND interoperability AND business”
- “disadvantages AND interoperability AND business”

The search was performed in already mentioned databases and search engines. The synonyms of the words ‘advantages’ and ‘disadvantages’ such as: benefits, difficulties, drawbacks, shortcomings, problems, issues were used. This eventually resulted in reaching the first

objective of this dissertation – identification of advantages and disadvantages of interoperability within professional literature.

### **3.4. *Results and Recommendations* methodology**

#### **3.4.1. Sampling method**

Within the *Results and Recommendations* chapters the documents produced by the European Union Institutions and documents developed by NGOs, think tanks, academic institutions were analysed. The discussions about interoperability within the European Union were initiated in 1995 and up till 2018, the number of documents regarding this topic exceeded the reasonable limit for the master level dissertation.

Therefore, the author of this dissertation decided to sample the resources based on her judgment, taking as a criterion the ability of the document to support answering the dissertation's research questions and meeting the dissertation's objectives (Saunders, Lewis and Thornhill, 2016, p. 301). This type of sampling (heterogeneous purposive sampling) enables the researcher to “collect data to describe and explain the key themes that can be observed” (Saunders, Lewis and Thornhill, 2016, p. 301).

The researcher decided that this sampling method is the most suitable for this research and rejected the following non-probability sampling methods: extreme case sampling, critical case sampling and typical case sampling. In extreme case sampling, research focuses on special cases. In homogeneous sampling, only some subgroups are described. The critical case method focuses on important cases. None of these methods would allow the author to respond on the research questions, which require investigation of a broad scope of materials offering as many potential responses as possible.

One of the sampling methods which could have been used instead of purposive sampling is theoretical sampling. Theoretical sampling is a variation of the purposive sampling. Within this approach, each document is analysed one by one. When a pattern is visible, new documents which seem to fit the core theme are added to it. This process stops, when new data does not bring any more added value and the relationships between data categories and categories themselves are well-developed. (Saunders, Lewis and Thornhill, 2016, p. 194). However, this sampling method is linked to the grounded theory research strategy, which was not used in this dissertation.

### 3.4.2. Approach

This part of the dissertation aimed to reach the four dissertations objectives: legislative developments in EU in terms of interoperability should be described, IT systems in the areas of borders and security which are planned to interoperate should be identified, advantages and disadvantages of their interoperability should be presented and recommendations for interoperability challenges proposed. To fulfil these objectives, the dissertation's author used an **inductive approach**. This approach "involves the search for a pattern from observation and the development of explanations – theories – for those patterns through series of hypotheses" (Bernard, 2011, p. 7) and it appeared to fit the purpose of the dissertation. Only after the careful analysis of the gathered material, it was possible for the dissertation's author to respond to the main research questions. Two other benefits of inductive approach belong to its flexibility in terms of developing new theories from the analysed data (Saunders, Lewis and Thornhill, 2016, p. 147) and its flexibility in terms of changing the direction of the study after the start of the research process (Dudovskiy, n.d.). This flexibility allows the researcher to achieve a broader spectrum of the results, which in case of this dissertation is highly desirable. The gathered data in this dissertation is analysed with a focus on: data quality (personal data, biometrics) and data protection (data minimization, purpose limitation, data retention, access to data, sharing the data with Third countries).

### 3.4.3. Method

As the leading method, the dissertation's author used thematic analysis method, which according to Saunders, Lewis and Thornhill (2016, p. 979) is considered "as a generic approach to analysing qualitative data". It offers relative flexibility as it is not linked either to inductive or to deductive approaches. Researchers who follow this method, first need to familiarise themselves with gathered data, afterwards they code it, search for themes and relationships. With the development of new themes, they reorganise their coded data under each theme. This process helps researchers to realise the connections between different datasets. With time and a higher number of analysed documents, researchers refine the themes and test propositions. This process is not linear, as the researcher needs to constantly come back to the previously coded data and reorganise it to the newly developed themes. It is important to test propositions by providing negative examples and alternative explanations (Saunders, Lewis and

Thornhill, 2016, pp. 579-587). The method was adapted in terms of coding, which was abandoned for the data organisation in a table.

The dissertation's author first performed the search for documents related to interoperability of the EU information systems in the areas of borders and security produced by the European Union Institutions and by NGOs, think tanks and academic institutions. They were retrieved by using EUR-lex databases and using Google.com. During this process sampling described in the above section was used.

As a first step, the author looked for the following terms:

- "interoperability of information systems AND European Union"
- "interoperability of information systems AND legislative development"

The results informed further search, as the author investigated the bibliographies of the positions which possibly could support answering on the research questions. The organisations working on the topic of this dissertation have been identified and the dissertation's author used new search terms:

- "interoperability of information systems AND EDPS"
- "interoperability of information systems AND FRA"
- "interoperability of information systems AND European Commission"
- "interoperability of information systems AND eu-LISA"
- "interoperability of information systems AND European Parliament"
- "interoperability AND opinion AND EDPS"
- "interoperability AND working group AND European"
- "interoperability of information systems AND Meijers"
- "interoperability of information systems AND ECRE"

The European Data Protection Supervisor (EDPS) is supervising and advising EU institutions in terms of data protection issues. The European Union Agency for Fundamental Rights (FRA) is advising EU institutions regarding fundamental rights issues. The European Commission proposes new legislation and implements EU policies. The European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) managed systems which are planned to be interoperable. The European Parliament has a

supervisory role and is scrutinising all EU institutions. The Meijers Committee is a group of experts providing the assessment of new legislative acts in the Area of Freedom, Security and Justice. The European Council on Refugees and Exiles provides comments to the legislative proposals related to migration. These organisations provide different views on interoperability of EU information systems in the areas of borders and security and offer a broad spectrum of opinions, which might be used in the process of reaching this dissertation's objectives.

After this search, dissertation's author extended the search using as keywords the names of the organisations which were producing documents describing the interoperability of EU systems in the areas of borders and security. When the systems which are planned to be interoperable were identified, the author used the following search terms:

- "interoperability AND *Eurodac*"
- "interoperability AND *SIS II*"
- "Interoperability AND *VIS*"
- "interoperability AND *EES*"
- "interoperability AND *ETIAS*"

The above-mentioned search terms were again researched accompanied by the words:

- "AND advantages" (together with a synonym: benefit)
- "AND disadvantages" (together with a synonym: difficulties, drawbacks, shortcomings, problems and issues"

### **Analysed documents**

Retrieved documents are presented in the *Table 1*, which contains the list of documents concerning legislative development of interoperability in the EU which were analysed for the purpose of writing this dissertation.

These documents illustrate the development of interoperability in the chronological way. The majority of these documents are legal acts following each other and establishing succeeding programmes on the European level.

---

**Document name:**

---

Annex 1 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM/2017/0134 final European Interoperability Framework – Implementation Strategy. Interoperability Action Plan.

---

Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM/2017/0134 final European Interoperability Framework – Implementation Strategy.

---

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions COM/2002/0062 final - eEurope Benchmarking Report - eEurope 2002.

---

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM/2010/0245 final A Digital Agenda for Europe.

---

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions COM/2017/0134 final European Interoperability Framework – Implementation Strategy

---

Corrigendum to Commission Decision 2004/387/EC of 28 April 2004 - Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC) (OJ L 144, 30.4.2004) Official Journal L 181, 18.5.2004, p. 25–35.

---

Council Decision 95/468/EC of 6 November 1995 on a Community contribution for telematic interchange of data between administrations in the Community (IDA). Official Journal L 269 , 11/11/1995 P. 0023 – 0025.

---

Decision No 1719/1999/EC of the European Parliament and of the Council of 12 July 1999 on a series of guidelines, including the identification of projects of common interest, for trans-European networks for the electronic interchange of data between administrations (IDA). Official Journal L 203 , 03/08/1999 P. 0001 – 0008.

---

Decision No 1720/1999/EC of the European Parliament and of the Council of 12 July 1999 adopting a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administrations (IDA). Official Journal L 203 , 03/08/1999 P. 0009 – 0013

---

Decision No 922/2009/EC of the European Parliament and of the Council of 16 September 2009 on interoperability solutions for European public administrations (ISA) (Text with EEA relevance). Official Journal L 260, 3.10.2009, p. 20–27.

---

Decision (EU) 2015/2240 of the European Parliament and of the Council of 25 November 2015 establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA2 programme) as a means for modernising the public sector (Text with EEA relevance) Official Journal L 318, 4.12.2015

---

Gatti, R., Carbone, L. and Mezzapesa, V. (2017). State of Play of Interoperability in Europe - Report 2016. [online] Luxembourg: Publications Office of the European Union.

---

Publications Office. (2005). Electronic interchange of data between administrations: IDA programme. [online]

---

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance Official Journal L 316, 14.11.2012, p. 12–33.

---

Vriendt, K. (2017). A new version of the European Interoperability Framework (EIF) – was it worth waiting for? - OpenForum Europe.

---

*Table 1 Documents concerning legislative development of interoperability in the EU*

*Table 2* presents documents concerning advantages, disadvantages of interoperability and recommendations to tackle identified challenges which were analysed. These documents were chosen based on the highest probability to answer dissertation’s research aim. They complement each other and look at both *Proposals* from different perspectives.



The majority of documents were created by sources linked to the European Union and only few of them were developed by the think tanks, NGOs and academic institutions. The dissertation's author was not able to identify more documents providing the alternative points of view. Section 3.4.3 of this dissertation explains the way of document search and focus on listed-above authors.

<b>Document name:</b>	<b>Creator type:</b>
Amber Alert Europe (2017). Interoperability. Amber Alert Europe's Position on interoperability of information systems in the field of migration and security.	Document developed by NGO
Article 29 Data Protection Working Party (2018). Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration.	Document developed by the EU institution
Committee on Civil Liberties, Justice and Home Affairs (2018). Report on the amended 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, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the ETIAS Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]	Document developed by the EU institution
Dimitrova, D. (2017). Connecting the dots in the Area of Freedom, Security and Justice (AFSJ) – Part II.	Document developed by academic institution
European Commission (2017c). Impact assessment accompanying the document 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 – 2017/0351 (COD)].	Document developed by the EU institution
European Data Protection Supervisor. (2018). Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems.	Document developed by the EU institution
European Economic and Social Committee (2018). Opinion. 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 – 2017/0351 (COD)] Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU	Document developed by the EU institution

information systems (police and judicial cooperation, asylum and migration) [COM(2017) 794 final – 2017/0352 (COD)].	
European Union Agency for Fundamental Rights (2017). Fundamental rights and the interoperability of EU information systems: borders and security. Freedoms.	Document developed by the EU institution
European Union Agency for Fundamental Rights. (2018). Interoperability and fundamental rights implications.	Document developed by the EU institution
High-level expert group on information systems and interoperability (2017). Final report.	Document developed by the EU institution
Meijers Committee. (2018). CM1802 Comments on the 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) 12 December 2017, COM (2017) 794.	Document developed by the think tank
Quintel, T. (2018). Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU’s case law on data retention.	Document developed by the academic institution
Privacy International. Privacy International response to consultation on the interoperability of EU information systems for borders and security.	Document developed by the NGO
SIS II Supervision Coordination Group, Eurodac Supervision Coordination Group, Visa Information System Supervision Coordination Group. 2018.	Document developed by the EU institution

*Table 2 Documents concerning advantages, disadvantages of interoperability and recommendations to tackle identified challenges*

While reading the documents, the dissertation’s author highlighted the parts of the documents describing the legislative developments in the EU in terms of interoperability, borders and security systems which are supposed to interoperate, the advantages and disadvantages of interoperability of EU information systems in the areas of border management and security for the refugees and the recommendations for the challenges and enhancing benefits.

Afterwards, the dissertation’s author separated these four big themes and started to organise the data under each of these main categories. In the legislative development in EU in terms of interoperability, the data was organised chronologically starting from the earliest developments. In the description of the borders and security systems, the data was categorised under each system.

Within the advantages and disadvantages of interoperability of EU information systems, the author categorised the data under the main categories: data quality (personal data, biometrics) and data protection (data minimization, purpose limitation, data retention, access to data, sharing the data with Third countries). Each of these categories was divided into subcategories:

advantages and disadvantages. These findings are compared to the findings listed in the *Literature Review*. The cross-reference table can be found in *Appendix*.

Within the 'recommendations' category, the author organised all recommendations coming from European Institutions and NGOs, think tanks and academic institutions. The common themes are identified. These recommendations are organised in a table, in which the first column contains the potential interoperability challenge, the second column under major themes lists recommendations, the third one lists potential risks and costs, the fourth one any possible barriers for their implementation. In the fifth column, the applicable solutions proposed by other stakeholders affected by interoperability within the European Union are presented, which allows to compare them and refute presented recommendations.

### **3.5. Alternative approaches and methods**

The main alternative approach, which could have been used is a deductive approach. Within this approach, the researchers test their hypothesis. Moreover, deduction follows a rigid methodology and allows the creation of alternative theories, but only within the limits of the research design. In the case of this research, it would not be feasible to establish the theory prior to the analyses of the gathered data, which is one of the key foundations of the deductive approach. Therefore, the idea of using this approach has been abandoned and the dissertation's author used more flexible inductive approach.

Another approach, which was considered by the dissertation's author was an abduction. Researchers following this approach look carefully into one fact, which does not follow the scheme and develop a theory explaining this derivation. Afterwards, they carefully test and verify it. However, this approach would not be applicable to this dissertation, which does not focus on separate incidents, but demands careful analysis of data to list advantages and disadvantages and to create plausible recommendations (Saunders, Lewis and Thornhill, 2016, p. 148).

From the methods, which the author considered using, it is important to mention the grounded theory method. In this method, the researchers are working on formulating the theory based on the collected data. Grounded theory has a well-defined process, which should be fully followed without picking elements out of it (Saunders, Lewis and Thornhill, 2016, p. 595). Within this method, the data is constantly analysed and compared. This results in the need to

develop appropriate tools helping to process it (Saunders, Lewis and Thornhill, 2016, p. 595). It is possible to notice, that this method requires systematic work and is rather time-consuming. The chosen thematic analysis method is less prescriptive and offers more flexibility.

Another alternative method which could have been used is template analysis. In this method, the researcher codes only part of the data creating a coding template. Coding templates consist of an initial list of codes and themes. This template is afterwards used as the analytical tool and it can be modified. However, in case of this research, this template would be too constraining as the aim of this dissertation is to provide a broad list of advantages, disadvantages and the recommendations for the identified challenges of interoperability of EU information systems.

### **3.6. Ethics**

For the purpose of writing this dissertation, the following ethical guidelines have been used:

- *DIS Ethics Policy for Research* (Aberystwyth University, 2013)
- *Code of Conduct* (European Border and Coast Guard Agency, 2017)

All the documents which are analysed for the purpose of this dissertation are public. Access to the European Parliament, the Council of the European Union and the European Commission documents is regulated by the Regulation (EC) No 1049/2001 of the European Parliament and of the Council on public access to EU institution documents. The dissertation's author in her research strictly followed the EU institutions' procedures which were created based on the above-mentioned Regulation. All copies of documents that were the basis for this research will be destroyed 6 months after the graduation ceremony. The author focused on the analysis of documentary material to exclude possible conflict of interest and bias related to the author's profession (till 31.07.2018 author worked for Frontex). This issue is further described in the 3.2 *Limitations to the research* part of this chapter.

The detailed methodological description which is used in this chapter aims to present the research done for the purpose of writing this dissertation. Thanks to this description, the readers will be able to see, what steps were performed to achieve the final research result and what could have been potentially improved. The dissertation's author within this chapter presented the alternative solutions and potential methods which could be used for future research in this field.

Based on the content of the *Methodology* chapter, the next researchers will be able to understand the methods used in this dissertation. The dissertation's author used purposive sampling to analyse the documentary resources coming from international institutions, think tanks, academic institutions and professional literature. The choice of the resources to be analysed was motivated by their potential to respond to research questions. All those sources were coded and based on these codes, common themes were identified. These common themes were related to data protection and data quality.

Following thematic analysis the triangulation of documentary sources used aimed to limit potential bias of this dissertation. However, future researchers might use the opportunity of extending the scope of the work and using other methods which might also appear to be valuable. The author of this dissertation hopes, that the work done will be a valuable basis for other research pieces within this topic.

## 4. Results

“Interoperability is not only or primarily a technical choice” (European Data Protection Supervisor, 2018, p. 3). This is a choice, which is motivated by both political and social factors. Within this chapter, the legislative development leading towards the development of two *Proposals* establishing the interoperability of the information systems in the areas of borders and security: *COM (2017) 793* and *COM (2017) 794* is presented. The vision of interoperability described in these documents affects not only the information systems, but also changes the interpretation of the legal principles they were based on. As it was noted by EDPS, these *Proposals* “mark a point of no return” (European Data Protection Supervisor, 2018, p. 3). The interoperability itself is not a new concept within the EU administration and the efforts leading to it were initiated in 1995. Within this chapter, the author introduces in detail the *Proposals*, describes planned interoperable systems and presents the advantages and disadvantages of the interoperability of these systems. This chapter is divided into 3 subchapters:

4.1. Legislative development in EU in terms of interoperability;

4.2. Data quality, data retention and data subject’s access to their own data; and

4.3. Data minimization, purpose limitation, access to data, sharing the data with Third countries.

Each subchapter is finalized with the list of the recommendations aiming to mitigate identified challenges. The recommendations were proposed by NGOs, think tanks, academic institutions and international organisations.

### 4.1. Legislative development in the EU in terms of interoperability

The concept of interoperability appeared for the first time in EU official documents in 1995 in the *Decision 95/468/EC* launching the first Interchange of Data between Administrations (*IDA*) Programme. Its aim was to “promote the development and operation of trans-European telematic networks for data interchange between Member State administrations and/or the Community institutions” (Publications Office, 2005). The follow-on five-year programme *IDA II* had a broader scope than *IDA* and was focused on the consumer protection, health, transport and areas related to Economic and Monetary Union (Publications Office, 2005). The continuation of *IDA II – IDABC* was established based on *Decision 2004/387/EC*. The objective

of IDABC was to deliver pan-European online eGovernment services to EU citizens, public administrations and businesses (Publications Office, 2005). Within its objective, the programme aimed to facilitate the exchange of information and achieve interoperability. This program was replaced in 2009 by ISA (Interoperability Solutions for European public administrations). It was the first time, when the concept of interoperability was defined (*Decision 922/2009/EC*). The ISA2 Programme was a continuation of ISA Programme. ISA2 programme for the first time, calls directly for the “enhanced interoperability among European databases in the basis of the Visa Information System, the Schengen Information System II, the European dactyloscopy system and the European e-Justice Portal” (*Decision (EU) 2015/2240*). It also asked eu-LISA to work within the framework of this programme.

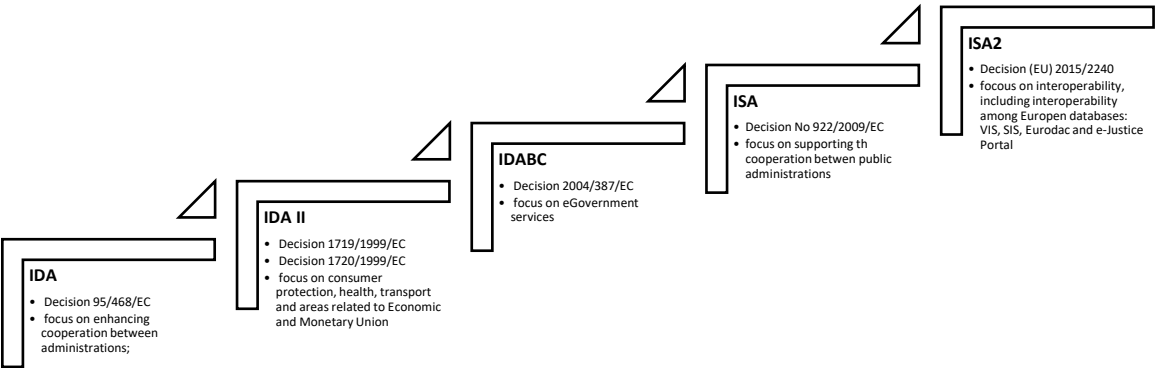


Table 3 Legislative development in EU in terms of interoperability

In 2016, the European Commission published a Communication *Stronger and smarter information systems for borders and security* (COM (2016) 205). Within this Communication, Commission presented the shortcomings of the information systems in area of border and security management. The publication of this document initiated a series of follow-up actions: the Council published a *Roadmap of 6 June 2016* (Council of the European Union, 2016); the European Parliament called for “proposals to improve and develop existing information systems, address information gaps and move towards interoperability, as well as proposals for compulsory information sharing at EU level, accompanied by necessary data protection

safeguards” (European Parliament, 2016). In June 2016, the Commission set up a High-level expert group on information systems and interoperability, which delivered a final report in May 2017 with recommendations how to implement the interoperability within the EU’s information systems. This report was accompanied by the opinions provided by FRA, EDPS and EU Counter-Terrorism Coordinator (High-level expert group on information and interoperability, 2017). Based on this report, the Commission prepared the *Seventh progress report towards an effective and genuine Security Union (COM(2017) 261)*, in which it stated its “new approach to the management of data for borders, security and migration management where all centralised EU information systems for security, border and migration management are interoperable in full respect of fundamental rights” (COM (2017) 794, p. 2). This new approach led to the develop of two *Proposals: COM (2017) 793* and *COM (2017) 794*. It was necessary to develop two sister *Proposals*, as they concern different systems. The *Proposal COM (2017) 793* covers the Schengen *acquis* regarding borders and visas:

- the Visa Information System (*VIS*) – contains data related to short-stay visas;
- the future Entry/Exit System (*EES*) – it will contain the data of third-country nationals visiting the Schengen area for a short stay;
- the proposed European Travel Information and Authorisation System (*ETIAS*) – it will contain the data of the visa-free travellers ahead of their travel to the Schengen area;
- the Schengen Information System (*SIS*) as regulated by *Regulation (EC) No 1987/2006* – contains the alerts on persons (e.g. missing, wanted persons, discreet checks) and objects (e.g. missing, stolen travel documents) (European Commission, 2017b).

The *Proposal COM (2017) 794* concerns the Schengen *acquis* on police cooperation or systems which are not related to the Schengen *acquis*:

- the *Eurodac* system – contains the data of asylum applicants and persons who either crossed the border in an irregular way or irregularly stay in a Member State;
- the proposed European Criminal Records Information System for third-country nationals (*ECRIS-TCN*) – contains the data on previous convictions against third-country nationals done by criminal courts in the EU;
- the Schengen Information System (*SIS*) as regulated by *Council Decision 2007/533/JHA*, (European Commission, 2017b).



The scope of the *Proposals* includes Interpol's Stolen and Lost Travel Documents (SLTD) database and Europol data (European Commission, 2017b).

The main technical components of the *Proposals*:

- the European search portal – the interface allowing to simultaneously search all listed above systems;
- the shared biometric matching service (shared BMS) – it enables the search and comparison of biometric data. Future *ETIAS* is excluded from shared BMS;
- the common identity repository (CIR) – it stores biographical and biometric identity data of third-country nationals listed in *Eurodac*, *VIS*, *EES*, *ETIAS* and *ECRIS-TCN*;
- the multiple-identity detector (MID) – checks whether there are multiple identities belonging to the same person in the multiple systems (*COM (2017) 793* and *COM (2017) 794*).

Different technical components concern different systems. For example, the European search portal concerns also the Interpol databases, the shared biometric matching service applies to the system with biometric data (European Union Agency for Fundamental Rights, 2018)

	Interpol								
	Eurodac	SIS	VIS	EES	ETIAS	ECRIS-TCN	Europol databases	TDAWN	SLTD
<b>ESP</b>	x	x	x	x	x	x	x	x	X
<b>BMS</b>	x	x	x	x		X			
<b>CIR</b>	x		x	x	x	X			
<b>MID</b>	x		x	x	X	x			

*Table 4 IT systems covered by the technical components of interoperability (European Union Agency for Fundamental Rights, 2018, p. 10)*

The *Proposals* contain three additional solutions aiming to enhance interoperability:

- development of a central repository of reporting and statistics;
- creation the Universal Message Format for all systems;
- development of automated data quality control mechanisms and common quality indicators (European Commission, 2017b).

As soon, as the *Proposals* were published, they received a criticism coming from both the European Union institution sources, as well as NGOs and scholar institutions. Several sources, such as authors of the report prepared for LIBE Committee noted, that these *Proposals* do not establish the interoperability, but in fact they describe its technical notion establishing **the interconnectivity** of the systems (SIS II Supervision Coordination Group, Eurodac Supervision Coordination Group, Visa Information System Supervision Coordination Group, 2018, p. 2). *Proposals* do not discuss the remaining interoperability notions.

The *Literature Review* chapter presented the following aspects of interoperability: technical, semantic, political/human, security/reliability and business/legal. Only discussion about all of the aspects can create a full picture of the change which will affect the information systems in the European Union. It will also help to understand possible challenges which are still not discovered. The researchers from the Carnegie Mellon Software Engineering Institute (2004, p. 16) distinguished four crosscutting issues related to interoperability which were described in detail in the *Literature Review* chapter: the complexity of interoperability, its implementation, problems with funding and control and issues related to the legacy system.

This review of the advantages, disadvantages and recommendations proposed by EU Institutions, NGOs and academic sources will be naturally focused on the proposed Regulations as they might shape the way information systems will be interoperable in the 2020 year. All of the researchers emphasized the increase of the efficiency of the systems supporting the work of border management officials which will be a result of the increased system's interoperability. However, they also called for the increased system governance (Committee on Civil Liberties, Justice and Home Affairs, 2018).

#### **4.2. Data quality, data retention and data subject's access to their own data**

Currently, one of the biggest problems of the EU information systems in the area of borders and security is the quality of its data. Per the survey administrated by FRA, for *SIS II* more than 40% of the staff and for *VIS* more than 50 % of the staff noted the wrong matches or inaccurate data (European Union Agency for Fundamental Rights, 2017, p. 30). According to FRA (2017, p. 30), these mistakes might be easier to notice thanks to the interoperability/ interconnectivity of the systems. However, it also notices (European Union Agency for Fundamental Rights, 2017, p. 29), that if the inaccuracies are not corrected on the spot, they might be very hard to rectify

and be transferred between the systems. EDPS (2018, p. 23) supported FRA's opinion and pointed out that the procedure for data's subject to access, rectify, erase and restrict the data is not clear. Moreover, there are additional issues related to the data quality – the ESP will also query Interpol databases, which are fed with the data coming from the national police authorities. It happens that this data is biased and the inserted alerts are based on political, military, religious and racial reasons (European Union Agency for Fundamental Rights, 2018, p. 19). The Meijers Committee (2018, Data retention, para 2.) noticed, the issue with the Article 23 of the Proposal which states: 'The individual file shall be stored in the CIR for as long as the corresponding data is stored in at least one of the information systems whose data is contained in the CIR'. Currently, each system has a different retention period, e.g. *Eurodac* 10, *VIS* 5 years and *SIS II* 3 years with a possibility of extension. The implementation of this article changes the data retention provisions. Additionally, as Privacy International (n.d.) noticed, proper deletion mechanisms for irrelevant data are missing.

FRA and EDPS suggest the following solutions for the above-mentioned issues:

- to develop procedures for the automatic data verification between IT systems allowing to correct data on the spot (European Union Agency for Fundamental Rights, 2017, p. 34);
- to enforce double checks, training and use of electronic readers to minimize the manual entry of data (European Union Agency for Fundamental Rights, 2017, p. 34);
- to use automatic verification against other data available (European Union Agency for Fundamental Rights, 2017, p. 34);
- to use quality standards for captured and matched fingerprints developed by eu-LISA, ICAO requirements for face images; (European Union Agency for Fundamental Rights, 2017, p. 32)
- to develop procedures for addressing the claims of persons who are contesting decisions based on the data stored in a system (European Union Agency for Fundamental Rights, 2017, p. 34);
- to clarify the procedure for the data subject rights of access, rectification, erasure and restriction (European Data Protection Supervisor, 2018, p. 23);
- to add obligation for the MS to inform data subjects about his/her data processing (European Union Agency for Fundamental Rights, 2018, p. 22);

- to add the obligation that data will be removed automatically when the purpose has been served or the justification for storing data is no longer there (European Union Agency for Fundamental Rights, 2018, p. 22).

Diana Dimitrova (2017) noticed that another data accuracy issues are created by the context – data which might be relevant in the immigration context might not be correct in the law enforcement context.

#### **4.3. Data minimization, purpose limitation, access to data, sharing the data with Third countries**

Both EU Institutions, NGOs and academic institutions pointed out, that both the data minimization and the purpose limitation principles might be undermined by both *Proposals* (Quintel, T, 2018, p. 15 and Article 29 Data Protection Working Party, 2018, p. 3). The databases collect the data of Third country nationals who are arriving in the EU. As researchers noticed (Quintel, T, 2018, p. 15), these *Proposals* might blur the boundaries between the migration management and the fight against terrorism. It is important to point out, that these databases were created for different purposes, some of them were implementing migration policies and other are related to law enforcement purposes (Dimitrova D., 2017). Dimitrova provides an example of the interconnectivity between *ETIAS* and Europol database, which mostly contains the data of the criminals and terrorists (2017). *ETIAS* contains the data of persons who would like to visit the Schengen area (Dimitrova D., 2017). The proposed technical solutions such as ESP, CIR, BMS create an impression of equalizing these persons. The discussion about these types of databases can be tracked down to the year 2004. The Committee on Civil Liberties, Justice and Home Affairs in its report from 25 October 2004 underlined that “the setting up of a centralised database would violate the purpose and the principle of proportionality. It would also increase the risk of abuse and function creep. Finally, it would increase the risk of using biometric identifiers as 'access key' to various databases, thereby interconnecting data sets”. (Article 29 Data Protection Working Party, 2018, p. 6). The researchers are concerned that the potential disadvantages outnumber the potential gains such as efficiency and shortening the query time.

FRA similarly to the Committee noticed, that proposed interoperability threatens purpose limitation - currently each system, thanks to its legal framework and compartmentalized nature, is safeguarded against unauthorized use. With interoperability it will change (European

Union Agency for Fundamental Rights, 2017). One of the most important principles of both *Proposals* is the emphasis that law enforcement officers would not access more data than they can do without interoperability. However, this rule has many exceptions. The table below prepared by the European Union Agency for Fundamental Rights (2018, p. 10) presents them:

	Proposed articles	Authority having access to additional data	Additional data
“Checks carried out for any public security or public policy reasons (as decided by Member States)	20	Any police officer who considers it necessary to check an individual, for example, for public order reasons or because of suspicious related to an offence or a crime, if authorized by national law	All identity data stored on the individual in the IT systems without flagging which system(s) contain it
Checks to enforce immigration law	20	Any police officer who considers it necessary to check where the person is stored in one of the IT systems to determine whether the person is lawfully staying or not	All identity data stored on the individual in the IT systems without flagging which system(s) contain it
Persons with a red link (identity fraud)	21 (2)	All authorities entitled to access at least one system	Identity data of the person subject to a red link stored in any of the six underlying systems and flagging which system(s) contains the data
Persons when a manual verification of the identity is required (yellow link)	21(1), 29 (3) and 30 (2)	All authorities entitled to access at least one system when they create or update an entry, as they will need to categorise a link showed as yellow (unclear identity)	Identity data of the person subject to a yellow link stored in any of the six IT systems and flagging which system(s) contain the data
Checks for law enforcement purposes	22(1)	Member State designated law enforcement authorities and Europol can query the CIR for the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case, to see which IT systems include information of a specific person.	List of IT systems in which information on a person can be found.
Systematic check of applicants for international protection against SIS	27(1)(d)	When a <i>Eurodac</i> entry is created or updated, the system will automatically alert the officer in case an applicant for international protection is recorded in <i>SIS</i> with a yellow or red link.	An asylum officer responsible for registration of claims is informed about the presence of an applicant in <i>SIS</i> , including yellow and red links”.

Table 5 “Authorities’ access to additional personal data through interoperability” (European Union Agency for Fundamental Rights, 2018, p. 10)

These exceptions concern mostly CIR. According to the Article 20 of the *Proposals* allows the law enforcement authorities to access CIR to identify people. Member States are charged with

defining precise conditions allowing police officers to do it. This procedure is against Digital Rights Ireland ruling, which stipulated, that whenever EU law interferes with fundamental rights (Article 7 and 8 of the Charter), it should be clear and precise (European Union Agency for Fundamental Rights, 2018, p. 26). The *Proposals* are changing the “cascade system”, which was previously used and replace it with a hit/no-hit system. In which law enforcement officer can search CIR to find whether a person was registered there. He/she receives a result which informs him/her which database contains data subject’s data. He/she can request for its full access. However, the information on which system contains which person’s data is already a piece of information which can bias his/her decisions. Moreover, checking a person’s identity when there is a crime suspected or for a public order offence is prohibited in all systems except for *SIS*. All systems limit the access of law enforcement to "serious crime and terrorism" (European Union Agency for Fundamental Rights, 2018, p. 26). According to FRA (2018, p. 33), this creates a risk of routine checks of a person in CIR regardless of the probability that the person’s data is in the system. Moreover, the more people have access to the data, the bigger risk, that it will be shared with Third countries (European Union Agency for Fundamental Rights, 2018, p. 14).

Additionally, Quintel (2018, p. 14) notices, in case of yellow or red links in MID created for persons with different biographical identities, which are suspected to be unlawfully used by the same person and which require manual verification, the officers have access to the identity file and the data they usually would not have access to.

Quintel (2018, p. 16) also notices, that currently the verification of the access is disregarded, and unauthorised personnel ask colleagues with wider access rights to check the systems for them. They also note the possibility of confusion between the applicable legal instruments, when the law enforcement officer will notice a link to the law enforcement databases. The personnel might not be sure whether the data is processed for law enforcement or migration purposes.

Recommendations by FRA, Committee on Civil Liberties, Justice and Home Affairs and EDPS:

- to limit the access of law enforcement officers to the data stored in CIR only to the situations described in the Article 22 of the *Proposals* (European Union Agency for Fundamental Rights, 2018, p. 35);

- to modify the text of *Proposals* to require law enforcement officers to perform the check in national databases before querying CIR (European Union Agency for Fundamental Rights, 2018, p. 35);
- to strengthen the systems of logs, verifying ex post controls, whether the requests to access the data were valid (European Union Agency for Fundamental Rights, 2018, p.35)
- FRA also proposed to exclude *ECRIS-TCN* from CIR due to the impact it might have on people lives (European Union Agency for Fundamental Rights, 2018, p. 39);
- to amend the *Proposals* to make sure that only the law enforcement officers who have full access to the data systems can search these systems based on hit/no-hit procedure (Committee on Civil Liberties, Justice and Home Affairs, 2018);
- to introduce the necessity and proportionality tests before the implementation of CIR (European Data Protection Supervisor, 2018);
- to remove the DNS & Palm Prints from BMS, moreover it is considered as unnecessary to store the first names of a person's parents, as currently only *ETIAS* will gather this information and therefore it will not be required for the comparison purposes (European Union Agency for Fundamental Rights, 2018, p. 21).

Interoperability as presented in the *Proposals* touches only one technical aspect of interoperability and cannot be considered as providing interoperable solutions. According to the SIS II Supervision Coordination Group, Eurodac Supervision Coordination Group, Visa Information System Supervision Coordination Group (2018, p. 2), the *Proposals* rather present the solutions for interconnectivity. They do not escape the advantages and disadvantages related to interoperability as described by the professional literature. The challenges related to interoperability focus mostly on data quality and the access provided to it.

Current *Proposals* base themselves on the current and planned IT systems, which are not free from the issues. The legacy systems have problems with data quality, which might affect other systems via their interconnectivity. The CIR will offer broader access to the data, than it is currently offered by the systems working on their own.

Moreover, the *Proposals* create interconnectivity between migration and law enforcement tools. This might result in blurring the boundaries between these two different areas. As EDPS

(2017, p. 9) noted: “It may even contribute to creating assimilation between terrorists, criminals and foreigners”.

However, most of the analysed sources appreciate the idea of interoperability and provide recommendations aiming to mitigate listed disadvantages. Properly implemented interoperability might be a useful tool for managing migration and supporting the fundamental rights of persons crossing the border.



## 5. Recommendations

As it was stated in the *Literature Review* chapter, the semantic interoperability allows the systems to work on the exchanged data (Miller P., 2000). Proposals *COM (2017) 793* and *COM (2017) 794* clearly aim to achieve this type of interoperability. This type of interoperability is more challenging than syntactic interoperability, as “it implies a mutual understanding of the meaning of data and information in the communication process” (Sudmans, M. et al, 2016). Within *Results* chapter, many advantages and disadvantages linked to this type of interoperability were identified. This chapter builds up on these findings and proposes the recommendations derived from the analyses of the resources listed in *Table 2*. *Appendix* contains the cross-reference of advantages/disadvantages of interoperability as listed in *Results* with recommendations from *Recommendations* chapter.

Chapter *Recommendations* follows a similar structure as *Results* chapter, with an additional *Systems governance* section. The dissertation’s author added a *Systems governance* to emphasise its general nature and the fact that it was mentioned by the several stakeholders such as FRA and Committee on Civil Liberties, Justice and Home Affairs.

Each section provides the recommendations to tackling the challenges and enhancing benefits listed in the *Results* chapter:

- Data quality, data retention and data subject’s access to their own data;
- Data minimization, purpose limitation, access to data, sharing the data with Third countries;
- Systems governance.

These recommendations are accompanied by the suggestions coming from the review of professional literature performed in the *Literature Review* chapter.

### 5.1. Data quality, data retention and data subject’s access to their own data

#### 5.1.1. To improve the data quality of legacy systems and test automatic data quality checks prior to their entry to operations

Currently, the legacy systems which are planned to be interoperable are experiencing data quality issues, which concerns both alphanumeric and biometric data (European Union Agency for Fundamental Rights, 2017, p. 30). This problem can escalate when the systems are

interconnected, therefore it is imperative to improve currently stored data, which can be done by standardizing the data collection process. This process should be followed in all data collection places (Skyttberg, N. et al., 2016). The manual data entry should be kept to the minimum and the system should be able to automatically verify the errors such as empty fields or data entered in the wrong fields. Additionally, double checks should be enforced. It is also proposed, that the data entered, when possible, should be verified with the data subject (European Union Agency for Fundamental Rights, 2017, p. 34).

Following these recommendations will improve the quality of the data entered on the system. However, it is also necessary to develop data quality checks to ensure that the data which is already in the system is valid. According to the *Proposals*, these checks will be developed after the new systems will be operational. It is recommended, to develop and test data quality checks prior to the system's operation (European Data Protection Supervisor, 2018, p. 25). It is necessary to make an effort to correct the data in the systems before releasing the systems to the border management officers for use. Additionally, it is necessary to ensure, that all Member States participate in the data quality improvement in the same manner. Otherwise, the system will not be complete, and the flaws will be affecting its overall usability (Committee on Civil Liberties, Justice and Home Affairs, 2018). This recommendation requires diplomatic efforts and finding a way to impose a similar way of working on the European level (Committee on Civil Liberties, Justice and Home Affairs, 2018).

It is also recommended to consider the use of Artificial Intelligence algorithms both as a monitoring tool and as a security key (European Economic and Social Committee, 2018, p. 14).

#### **5.1.2. To implement data biometrics standards**

It is recommended to improve the quality of biometrics stored in the EU information systems in the areas of borders and security by implementing eu-LISA standard for captured and matched fingerprints and ICAO requirements for face images (European Union Agency for Fundamental Rights, 2017, p. 32). Additionally, as in the case of alphanumeric data, the data should be automatically verified and corrected (European Union Agency for Fundamental Rights, 2017, p. 32). Moreover, as currently all systems use different formats of Biometric Fingerprint Files, they should agree on a common file format (European Commission, 2017c, p. 20). It is also suggested to introduce pop-up alerts encouraging officers to perform the manual

verification in case of biometric data with a higher risk of being false, e.g. child's fingerprints (European Union Agency for Fundamental Rights, 2018, p. 14).

### **5.1.3. To promote Universal Message Format (UMF)**

Currently, all systems use their own specific data models to organise and store data. The interface and/or message format are linked to this data model and therefore differ between systems. To facilitate data information exchange, all systems should use UMF, which was created for law enforcement systems on the European level. "UMF is a set of concepts (building blocks) to construct standard data exchanged for interconnecting dispersed law enforcement systems" (Europol, 2014). UMF allows the reuse of systems components and in effect to improve the systems efficiency and the data quality (Europol, 2014). The use of UMF is also recommended for the national databases (High-level expert group on information systems and interoperability, 2017, p. 34).

### **5.1.4. To add the requirement of revision and update of the user profiles within central management of the interoperable system**

It is necessary, that users access rights are updated on the regular basis and they are reviewed on the regular basis (European Data Protection Supervisor, 2018, p. 19).

### **5.1.5. Training**

Currently, many mistakes in the data quality are caused by the border guards' stress, workload and lack of skills. Though, the decisions limiting the workload of the officers lay beyond the scope of this dissertation, the dissertation's author would like to emphasise the importance of the training. Thanks to the training, the officers can learn the naming conventions, ways of transcribing the names into the Latin alphabet, ways of proper collection of biometrics, following person's fundamental rights, and in this way limit the number of errors (European Union Agency for Fundamental Rights, 2017, p. 30).

### **5.1.6. To clarify the data retention policy**

It needs to be clarified that the data should be removed automatically from the system when it has served its purpose or there is no justification to keep it there (European Union Agency for Fundamental Rights, 2018, p. 22).

Moreover, the retention period should be clearly set and procedure for data erasure should be developed. It is also suggested, that the time limits for data preservation should be shorter for minors (except for the cases of terrorism) (Committee on Civil Liberties, Justice and Home Affairs, 2018).

**5.1.7. To create an EU-wide portal handling requests related to the data access, rectification, erasure, restriction and data's subject claims for changing decisions based on the data stored in the system**

Such a system, as proposed by FRA, would be a user-friendly solution for the problems related to the unclear data ownership and procedures related to the data access, rectification, erasure and restriction (European Union Agency for Fundamental Rights, 2018, p. 41). It would also create an easier way to appeal for a change of the decisions which were based on the data stored in the system. It could be also be provided in different language versions, which again would have a positive effect on the system accessibility. In this case, the complicated procedures related to data would happen in the background and users would only receive important information with less bureaucracy. Such a system would help users understand what is happening with their data and provide a platform allowing to inform persons concerned about the procedure and its effect in the written form (European Union Agency for Fundamental Rights, 2018, p. 41).

**5.1.8. To define a valid search mode for the European Search Portal**

Currently, all developed systems considered for interoperability are using different search algorithms. As a result, a person performing the same search in *SIS* and *VIS* will receive different results. It is important to decide upon one, valid search mode (European Commission, 2017c, p. 21).

**5.1.9. To create a safeguard, that the owners of Interpol data (Third countries) will not have access to the information that their data was accessed and by which country**

European Search Portal will query Interpol databases, which are sometimes fed by Third country regimes with biased alerts. Even though, Interpol makes an effort to remove such alerts, they might put a person's life in danger (European Union Agency for Fundamental Rights, 2018, p. 19). Currently, the *Proposals* state, that the data used to launch a query should not be shared with Third countries. However, it does not explicitly say, that the data which national

authority accessed their information should not be shared. This data might provide valuable information, where a searched person is. Therefore, it is recommended to amend the Article 9(5) of *Proposals* and explicitly forbid this practice (European Union Agency for Fundamental Rights, 2018, p. 20).

**5.1.10. To add a flag in a system, when yellow alerts appear as a result of inconsistencies with data stored in ETIAS**

The data added to the planned *ETIAS* system will be self-declared and therefore more prone to errors than the data added by the border management officers. To prevent its negative effect, yellow alerts resulting from differences between data should be flagged (European Union Agency for Fundamental Rights, 2018, p. 37).

**5.1.11. To designate eu-LISA and authorities in the Member States as a joint data quality controllers**

As EDPS noted, the Member States are responsible for the data input and its quality. According to the *Proposals*, eu-LISA will evaluate the data quality and report on it. Moreover, it is responsible for planning actions aiming to improve data quality. Therefore, it is recommended to create a double control system, in which both Member States and eu-LISA have clearly defined responsibilities (European Data Protection Supervisor, 2018, p. 25).

**5.1.12. To add child protection objective**

Interoperable systems can be used for missing children's searches. However, there are two main obstacles preventing it. First of all, not all Member States systematically register missing children in *SIS II*. This prevents sending this data to *Eurodac* and afterwards to the anti-trafficking authorities (European Union Agency for Fundamental Rights, 2017, p. 36). Moreover, as currently this objective does not belong to the scope of the *Proposals*, it threatens the purpose limitation principle (European Union Agency for Fundamental Rights, 2017, p. 36).

**5.2. Data minimization, purpose limitation, access to data, sharing the data with Third countries**

**5.2.1. BMS should match the data not to store it**

As Quintel (2018, p. 15) says, in the case of BMS, there is no legal basis for a new data processing operation. There are different opinions, whether fingerprints constitute personal data.

However, it was noted, that they pose a risk of re-identification of individuals. The storage of templates constitutes a new database, which exceeds the scope of potential interoperability solutions. Therefore, it is proposed to reprogram this tool to match the data not to store it (European Union Agency for Fundamental Rights, 2017, p. 24).

### **5.2.2. To remove unnecessary data from CIR**

CIR stores unnecessary data such as the first names of the parents (only stored in *ETIAS*). This data cannot be compared with any other systems, therefore it is advised to remove it (European Union Agency for Fundamental Rights, 2018, p. 24).

### **5.2.3. To allow law enforcement access CIR only for “the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case” (Article 22, COM(2017)793).**

There are several rationales for this recommendation. First of all, most of the IT systems in the areas of border and management were not created for law enforcement. According to the *Proposals*, law enforcement officials will have the opportunity to use CIR to identify a person, which is a very broad purpose. Moreover, the identification of a person is never a final step and it rather leads to another objective. This type of general objectives is against Digital Rights vs Ireland Court of Justice of the European Union Ruling (European Union Agency for Fundamental Rights, 2018, p. 26).

Moreover, it is stated in the *Proposals*, that the law enforcement officials will keep their original access methods established prior to the implementation of interoperability, but in fact there will be many exceptions to this rule. These exceptions are presented in *Table 5* in *Results* chapter.

The proposed hit/no-hit system allows law enforcement officers to know which system contains someone’s data. According to EDPS, awareness of the data presence in one of the interoperable systems is already personal data and should be treated according to the personal data processing rules. Quintel (2018, p. 14) says, that already right now, the access requirements are often disregarded and law enforcement officers ask their colleagues to access the data they have no access to.

As Quintel (2018, p. 16) noted, “a police officer, checking data for immigration purposes, could discover links to a person in LE databases and easily end up in a situation where it is not clear

which legal instrument applies for accessing the data". *GDPR* is responsible for all immigration and asylum operations and law enforcement falls under *Law Enforcement Directive*, which offers less data protection than the *GDPR*.

The possibility for law enforcement officers to access the databases, can also create the risk of the abuse (Quintel, T., 2018, p. 16). Even though, it is proposed to strengthen the system of ex ante controls, logging information and strengthening the role of DPA, it still creates a risk of abuse (European Union Agency for Fundamental Rights, 2018, p. 34).

Therefore, it is proposed to allow law enforcement officers to access CIR only for "the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case" (Article 22, COM(2017)793). The access should be logged and reviewed. The cascading system is proposed instead of hit/no hit procedure. EDPS stated that cascading systems does not extend unnecessarily the procedure. Moreover, the law enforcement officers should be obliged to first check their national databases before reaching to CIR (European Union Agency for Fundamental Rights, 2018, p. 35).

There are several refuted suggestions. For example, Europol suggested allowing the Member States to grant permission for a law enforcement officer to see their data based on hit/no-hit system (European Union Agency for Fundamental Rights, 2017, p. 24). However, this according to the dissertation's author would create an unnecessary workload and extend the waiting time.

It is important to point out, that The Working Party 293 noted that "there is a risk that the setting up of a centralized database containing personal data and in particular biometric data of all (European) citizens could infringe the basic principle of proportionality" (ECtHR, No. 19522/09, M.K. v. France, 18 April 2013, para. 40. quoted in Article 29 Data Protection Working Party, 2018). Therefore it might be first necessary to perform proportionality tests.

#### **5.2.4. To introduce safeguards for protecting the data against unauthorised access**

*ETIAS* and *EES* offer access to the parts of its datasets via the internet to private persons and carriers. This creates a risk of the unauthorised data use. Therefore, it is necessary to provide safeguards for protecting this sensitive data (European Union Agency for Fundamental Rights, 2017, p. 26).

Additionally, it is important to think holistically about data protection and protect not only central units, communication channels between interconnected databases, but also national border infrastructure (European Union Agency for Fundamental Rights, 2017, p. 26).

It is also recommended to connect ESP to the secure Trans-European Services for Telematics between Administrations (TESTA) networks (European Commission, 2017c, p. 41).

#### **5.2.5. To clarify the conditions under which eu-LISA has access to the interoperable databases**

It is recommended to add to the *Proposals* above-mentioned conditions and to log the access of eu-LISA staff members (European Data Protection Supervisor, 2018, p. 28).

#### **5.2.6. To remove ECRIS-TCN from MID**

In the case of this yellow or red link, the *Proposals* give access to the officers to see the identity file. In this file, the officers can see the data from all systems including *ECRIS-TCN*. It is recommended to remove this database from MID as it might have a disproportional effect on officers' decisions (European Union Agency for Fundamental Rights, 2018, p. 39).

### **5.3. System governance**

#### **5.3.1. To improve the governance of the interoperable systems.**

The IT systems with time will naturally be upgraded. It is necessary to control how the upgrades will influence the overall interoperability of the systems, as most of them were not designed with interoperability in mind. It is recommended for eu-LISA, as an EU Agency evaluating the implementation of interoperability to report annually to EDPS and Commission, report every two years regarding the impact of interoperability on fundamental rights and assess how ex ante controls affected the risk management (Committee on Civil Liberties, Justice and Home Affairs, 2018). This might increase the bureaucracy linked to the systems management, but will also ensure that the interoperability is working well and is supporting the achievement of its objectives.

Additionally, it is proposed for the Member States to designate a central verification authority (including staff with fundamental rights expertise) to monitor the work of border guards and its compliance with fundamental rights principles. This authority can participate in data quality improvement (European Union Agency for Fundamental Rights, 2018, p. 34). The interoperable



systems will be used by the Member States, who will be responsible for the data input. The systems will be managed by the eu-LISA Agency. This might create a perceived lack of control and ownership (Miller P., 2000). This central point would respond to this challenge. Moreover, it should provide statistics from the Central repository for reporting and statistics, as it should remove the risk of producing biased reports suggesting operational actions, as it might happen if operational units would produce such reports (European Union Agency for Fundamental Rights, 2018, p. 34).

The above-mentioned recommendations aim to increase the usability of the interoperable systems and answer on the crosscutting issues, which were presented in the *Literature Review* chapter:

- Complexity of interoperability
- Complexity of interoperability implementation
- Funding and control are not interlinked
- Problems linked to legacy systems (Carnegie Mellon Software Engineering Institute, 2004, p. 16)

The majority of the issues were linked to the data quality and to the data protection. First of all it is necessary to improve the data quality systems which are already in use. Otherwise, the problems which are experienced right now might amplify and have both a negative impact on people's life and discourage border guards from using failing systems. As Quintel (2018, p. 17) says: "The right to the protection of personal data is not an absolute right. However, new processing operations must be sufficiently justified and need to have undergone a necessity and proportionality assessment". The proposed recommendations aim to respond to this call.

## 6. Conclusion

The African proverb says “if you want to go fast go alone. If you want to go far, go together”. Looking carefully into its sense, it is possible to see, that it can concern both the interoperability and the idea standing behind the European Union. The European Union is based on mutual trust and this is also the base for the interoperability efforts. The information systems in the areas of borders and security aim to protect one of the main achievements of the European Union: free movement of people within the Schengen Area. Up till now, all systems were working separately and there were gaps between them causing information to get lost. The terrorist attacks were exploring those gaps and in response, in 2016 the European Commission published a Communication *Stronger and smarter information systems for borders and security*. This Communication marks a starting point for a more serious debate over the information systems and the ways of connecting them. This dissertation aimed to present the advantages and disadvantages of the interoperability of the above-mentioned systems and to provide the recommendations for overcoming the challenges.

Throughout the dissertation, all the dissertation’s objective were met. Within the *Literature Review*, dissertation’s author identified the advantages and disadvantages of interoperability. In the *Results* chapter, dissertation’s author described the legislative development in the EU in terms of interoperability and identified and described the borders and security systems which are supposed to interoperate. The disadvantages and advantages of interoperability in terms of European Union information systems in the areas of borders and security for refugees and recommendations for tackling the challenges and enhancing the benefits were presented in the *Results* and *Recommendations* chapters.

In its first part, the dissertation’s author presented the professional literature review aiming to give the context to the debate about the interoperability. The authors discussed were coming from different areas: business, information management, government and academics. It was interesting to see, how they look from the different perspectives on the interoperability issues. The analysis of their work gave the dissertation’s author a new view on the potential advantages and disadvantages of interoperability, which were not mentioned by the authors discussing strictly the interoperability of information systems in the areas of borders and security. In the *Methodology* chapter, the dissertation’s author presented ways of achieving the dissertation’s

objectives. The research questions drove the choice of the thematic analysis as the main method. The dissertation's author analysed the documents produced by the European Union Institutions, think tanks, NGOs, academic institutions and other international organisations. The heterogeneous purposive sampling allowed to focus on the documents which were the most likely to respond to the research questions. The document analysis drove the content of the next two chapters: *Results* and *Recommendations*.

In *Results*, the dissertation's author described the legislative development in EU in terms of interoperability and presented the systems which are planned to be interoperable: *VIS*, *EES*, *ETIAS*, *SIS*, *Eurodac* and *ECRIS-TCN*. These systems derive from different legislative acts: the Schengen *acquis* regarding borders and visas and the Schengen *acquis* on police cooperation or systems which are not related to the Schengen *acquis*. This distinction appeared to be very important as it had an effect on the objectives of the *Proposals* aiming to introduce the interoperability of the above-mentioned systems. The *Proposals COM (2017) 793* and *COM (2017) 794* proposed four main technical components: the European search portal, the shared biometric matching service, the common identity repository and multiple-identity detector. Not all components were affecting information systems in the same way.

These *Proposals* were severely criticized by all stakeholders. The majority of the concerns was concerning data quality, the access to it and purpose limitation. The researchers noticed, that the quality of data interoperable systems strongly depends on the data quality of legacy systems. It was recommended both by the researchers and dissertation's author to focus on improving it prior to making actions aiming to interlink the systems. While performing the literature review, some of the authors noticed the issue of the interoperability complexity (Carnegie Mellon Software Engineering Institute, 2004, p. 16). Users do not always know, where their data is stored and how they access it. As a solution, the dissertation's author proposed, following FRA advice to create an EU-wide portal handling request related to the data access, rectification, erasure, restriction and data subject's claims for changing decisions based on the data stored in the system. (European Union Agency for Fundamental Rights, 2018, p. 41). It is also worth to mention, that the dissertation's author proposed to add one more objective to the *Proposals* – child protection. The interoperable systems provide an opportunity to increase the protection of the most vulnerable persons and it would be beneficial to take it.

Regarding the purpose limitation, the researchers pointed out, the issue of the law enforcement access to CIR. As it was even visible from the existence of two different *Proposals* concerning the same subject, some of the systems were not designed with the law enforcement purpose. Therefore, this easy access of law enforcement officers to CIR was considered as a dubious and there were several calls for its limitation (e.g. Quintel T., 2018, p. 16). The dissertation's author proposed to limit it only to the clearly defined cases. Additionally, it would be beneficial to check whether this database is proportional, as there were rulings in similar cases contesting this type of a centralized databases containing personal data (ECtHR, No. 19522/09, M.K. v. France, 18 April 2013). The dissertation's author proposed also to remove BMS from the *Proposals*. This system creates a new database with fingerprint templates. There is an ongoing discussion whether the templates constitute personal data. However, it was pointed out by Quintel, that they pose a risk of re-identification of individuals (2018, p. 15).

These two new databases: CIR and BMS clearly present the main issue of both *Proposals* – they do not establish interoperability, but barely interconnectivity. The majority of the stakeholders were concerned with the creation of new, centralized databases and proposing new uses for already gathered data (e.g. European Data Protection Supervisor, 2018, p. 11). This tendency creates a risk of function creep. Additionally, as EDPS noticed: “the EDPS is concerned that repeatedly referring to migration, internal security and fight against terrorism almost interchangeably brings the risk of blurring the boundaries between migration management and fight against crime and terrorism. It may even contribute to creating assimilation between terrorists, criminals and foreigners” (European Data Protection Supervisor, 2018, p. 9). The recommendations in this paper, aimed to refocus the *Proposals* and interoperability efforts on supporting the border guards work and protection of Third country nationals. The dissertation's author believes, that by taking part in its ongoing discussion, she can provide additional, supported by other researchers, arguments for increasing interoperability efforts with fundamental rights in mind.

While performing the research, it has been noted, that the number of documents to be analysed was rather limited and biased towards EU perspective. It was also not possible to obtain documents produced by the eu-LISA and concerning the improvement of the EU information systems in the areas of borders and migration. The access to these documents was limited and documents were confidential. This research was based on the documents produced

by other stakeholders, such as international organisations, think tanks or academic. In retrospective, bigger emphasis would be put on the data collection method and combining secondary and primary data analysis.

It has been noted, that the documents produced by NGOs were only referred to the above-mentioned papers. The dissertation's author believes, that for the future research and the improvement of this study, it would be beneficial to research the opinions of NGOs by performing detailed interviews. It is important to know, whether the NGOs notice the importance of both *Proposals*. Additionally, it would be beneficial to gather the detailed data about the current situation in the Member States and the implementation of the procedures related to the current use of the information systems in the areas of borders and security. The reviewed documents gave the impression, that each Member State differs in the way it works. Definitely, the strong point of writing this dissertation was the data analysis and the creation of the comprehensive tables. This helped to analyse the data and not to lose significant findings. Thanks to this method, it was easy to return to the findings and link them to the recommendations and sources. MS Excel table allowed to build up the relationship between the data and this method is recommended for persons who would like to follow this subject and perform deeper research on discussed information systems.

The dissertations discussed the advantages and disadvantages of interoperability of European Union information systems in the areas of borders and security. The importance of interoperability was noted and the current misunderstanding related to how it will be implemented were pointed out. The interoperability can bring the benefit and increase the efficiency of border guards performing the checks in the systems. It can also support Third country nationals visiting the European Union. It can protect the Schengen Area by allowing the Member States to know who is crossing the Schengen area border. However, as always, the issue with interoperability lies in its implementation. It is important that the fundamental rights will not be abused and the systems will not change into a surveillance mechanism. The proposed recommendations aim to mitigate this danger and highlight the voice of the stakeholders who were raising awareness of the issues which need to be corrected prior to the implementation of *Proposals*.

## 7. References

Aberystwyth University (2003) DIS Ethics Policy for Research, Available at: [https://blackboard.aber.ac.uk/bbcswebdav/pid-2360-dt-content-rid-857229\\_1/courses/1\\_DIS\\_DL\\_Central/\\_DIS%20Ethics%20Policy%20for%20Researchv14%281%29.pdf](https://blackboard.aber.ac.uk/bbcswebdav/pid-2360-dt-content-rid-857229_1/courses/1_DIS_DL_Central/_DIS%20Ethics%20Policy%20for%20Researchv14%281%29.pdf) [Accessed 28 Oct. 2017].

Alemu G., Stevens B., Ross P., (2012) Towards a conceptual framework for user-driven semantic metadata interoperability in digital libraries: A social constructivist approach. *New Library World*, Vol. 113 Issue: 1/2, pp. 38-54, Available at: <https://doi.org/10.1108/03074801211199031> [Accessed 14 Feb. 2018].

Article 29 Data Protection Working Party (2018). Opinion on Commission proposals on establishing a framework for interoperability between EU information systems in the field of borders and visa as well as police and judicial cooperation, asylum and migration. Available at: [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=624198](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=624198) [Accessed 20 Dec. 2018].

Bernard, H.R. (2011). *Research Methods in Anthropology*. 5th edition, AltaMira Press.

Beydogan, T. A. (2010). Interoperability-Centric Problems: New Challenges and Legal Solutions. Available at: <https://doi.org/10.1093/ijlit/eqq008> [Accessed 2 Feb. 2018].

Carnegie Mellon Software Engineering Institute (2004). Current Perspectives on Interoperability. [online] Pittsburgh: Carnegie Mellon. Available at: [https://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2004\\_005\\_001\\_14390.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalReport/2004_005_001_14390.pdf) [Accessed 3 Feb. 2018].

Carnegie Mellon Software Engineering Institute (2005). Some Current Approaches to Interoperability. [online] Pittsburgh: Carnegie Mellon. Available at: [https://resources.sei.cmu.edu/asset\\_files/TechnicalNote/2005\\_004\\_001\\_14540.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalNote/2005_004_001_14540.pdf) [Accessed 3 Feb. 2018].

Carnegie Mellon Software Engineering Institute (2006). Topics in Interoperability: Structural Programmatic in a System of Systems. [online] Pittsburgh: Carnegie Mellon. Available at:

[https://resources.sei.cmu.edu/asset\\_files/TechnicalNote/2006\\_004\\_001\\_14741.pdf](https://resources.sei.cmu.edu/asset_files/TechnicalNote/2006_004_001_14741.pdf)  
[Accessed 3 Feb. 2018].

Committee on Civil Liberties, Justice and Home Affairs (2018). Report on the amended 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, Regulation (EU) 2017/2226, Regulation (EU) 2018/XX [the *ETIAS* Regulation], Regulation (EU) 2018/XX [the Regulation on SIS in the field of border checks] and Regulation (EU) 2018/XX [the eu-LISA Regulation]. Available at: <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2018-0347&language=EN#title3> [Accessed 21 Dec. 2018].

Council of the European Union. (2016). Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area. Available at: <http://data.consilium.europa.eu/doc/document/ST-9368-2016-REV-1/en/pdf> [Accessed 4 Apr. 2018].

Díaz de Mera García Consuegra, A. (n.d.). Legislative train schedule towards a new policy on migration. Entry/Exit System (2016 Smart Borders Package). European Parliament. Available at: [http://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-entryexit-system-\(2016-smart-borders-package](http://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-entryexit-system-(2016-smart-borders-package) [Accessed 2 Apr. 2018].

Dimitrova, D. (2017). Connecting the dots in the Area of Freedom, Security and Justice (AFSJ) – Part II. Available at: <https://www.law.kuleuven.be/citip/blog/connecting-the-dots-in-the-area-of-freedom-security-and-justice-afsj-part-ii/> [Accessed 21 Dec. 2018].

Dudovskiy, J. (n.d.). Inductive Approach (Inductive Reasoning). Research Methodology. Available at: <https://research-methodology.net/research-methodology/research-approach/inductive-approach-2/> [Accessed 26 May 2018].

EurActiv.com (2015) Eurodac fingerprint database under fire by human rights activists. Available at: <http://www.euractiv.com/section/justice-home-affairs/news/eurodac-fingerprint-database-under-fire-by-human-rights-activists/> (Accessed: 1 Ap. 2018).

European Border and Coast Guard Agency. (2017). Code of Conduct. Available at: [http://frontex.europa.eu/assets/Publications/General/Code\\_of\\_Conduct\\_applicable\\_to\\_all\\_persons\\_participating\\_in\\_Frontex\\_operational\\_activities.pdf](http://frontex.europa.eu/assets/Publications/General/Code_of_Conduct_applicable_to_all_persons_participating_in_Frontex_operational_activities.pdf) [Accessed 28 Oct. 2017].

European Commission. (n.d.). What is personal data?. Available at: [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en) [Accessed 30 Oct. 2017].

European Commission. (2013) Free movement of people: five actions to benefit citizens, growth and employment in the EU. Available at: [http://europa.eu/rapid/press-release\\_IP-13-1151\\_en.htm](http://europa.eu/rapid/press-release_IP-13-1151_en.htm) [Accessed 2 Apr. 2018].

European Commission: Migration and Home Affairs (n.d.). Identification of applicants (EURODAC). Available at: [https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/identification-of-applicants_en) [Accessed 2 Apr. 2018].

European Commission: Migration and Home Affairs 1. (n.d.). Visa Information System (VIS). Available at: [https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en) [Accessed 2 Apr. 2018].

European Commission: Migration and Home Affairs 2. (n.d.). Schengen Information System. Available at: [https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en) [Accessed 2 Apr. 2018].

European Commission. (2017a). Communication from the Commission to the European Parliament, the European Council and the Council. Seventh progress report towards an effective and genuine Security Union. Available at: [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170516\\_seventh\\_progress\\_report\\_towards\\_an\\_effective\\_and\\_genuine\\_security\\_union\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170516_seventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf), COM(2017) 261 final [Accessed 10 Apr. 2018].

European Commission. (2017b). Frequently asked questions – Interoperability of EU information systems for security, border and migration management. Available at: [http://europa.eu/rapid/press-release\\_MEMO-17-5241\\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-5241_en.htm) [Accessed 10 Apr. 2018].

European Commission (2017c). Impact assessment accompanying the document 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 – 2017/0351 (COD)]. Available at: [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212\\_commission\\_sw\\_impact\\_assessment\\_proposal\\_regulation\\_on\\_establishing\\_framework\\_for\\_interoperability\\_between\\_eu\\_information\\_systems\\_police\\_judicial\\_cooperation\\_asylum\\_migration\\_part\\_2\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_commission_sw_impact_assessment_proposal_regulation_on_establishing_framework_for_interoperability_between_eu_information_systems_police_judicial_cooperation_asylum_migration_part_2_en.pdf) [Accessed 10 Dec. 2018].

European Data Protection Supervisor. (2018). Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems. Available at: [https://edps.europa.eu/sites/edp/files/publication/2018-04-16\\_interoperability\\_opinion\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/2018-04-16_interoperability_opinion_en.pdf) [Accessed 10 Dec. 2018].

European Economic and Social Committee (2018). Opinion. 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 – 2017/0351 (COD)] 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 – 2017/0352 (COD)]. Available at: <https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/interoperability-package> [Accessed 20 Dec. 2018].

European Parliament (n.d.) Legislative Train Schedule: Towards a New Policy on Migration. Entry/Exit System (2016 Smart Borders Package). Available at: [http://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-entryexit-system-\(2016-smart-borders-package\)](http://www.europarl.europa.eu/legislative-train/theme-towards-a-new-policy-on-migration/file-entryexit-system-(2016-smart-borders-package)) [Accessed 20 Dec. 2018].

European Parliament. (2016). European Parliament resolution of 6 July 2016 on the strategic priorities for the Commission Work Programme 2017. Available at: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0312+0+DOC+XML+V0//EN> [Accessed 10 Dec. 2018].

European Parliament. Policy Department for Citizen's Rights and Constitutional Affairs. (2018). Interoperability of Justice and Home Affairs Information Systems. Civil Liberties, Justice and Home Affairs. Available at: [http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL\\_STU\(2018\)604947\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604947/IPOL_STU(2018)604947_EN.pdf) [Accessed 1 Dec. 2018].

European Parliament: Think Tank. (2017). European Travel Information and Authorisation System (ETIAS) - Think Tank. Available at: [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI\(2017\)599298](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2017)599298) [Accessed 2 Apr. 2018].

European Parliamentary Research Service (2018). Interoperability between EU information systems for security, border and migration management. Available at: <http://www.statewatch.org/news/2018/feb/ep-briefing-interoperability-analysis-of-commission-impact-assessment-2-18.pdf> [Accessed 2 Apr. 2018].

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (n.d.). ECRIS-TCN. Available at: <https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn> [Accessed 6 Jan. 2019].

European Union Agency for Fundamental Rights (2017). Fundamental rights and the interoperability of EU information systems: borders and security. Freedoms. Vienna. Available at: <http://fra.europa.eu/en/publication/2017/fundamental-rights-interoperability> [Accessed 2 Apr. 2018].

European Union Agency for Fundamental Rights. (2018). Interoperability and fundamental rights implications. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST\\_8037\\_2018\\_INIT&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_8037_2018_INIT&from=EN) [Accessed on 1 Nov. 2018].

Europol (2014). Universal Message Format: Faster, cheaper, better. Available at: <https://publications.europa.eu/en/publication-detail/-/publication/3b2cc49f-72bb-419f-8742-eb21cd15e35c/language-en> [Accessed 19 Dec. 2018].

Gasser, U. and Palfrey, J. (2007). Breaking down digital barriers: When and How ICT Interoperability Drives Innovation. Berkman Publication Series. Available at:

<https://cyber.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf> [Accessed 12 Dec. 2017].

GridWise Architecture Council (2009). Reliability Benefits of Interoperability. Available at: [http://www.gridwiseac.org/pdfs/reliability\\_interoperability.pdf](http://www.gridwiseac.org/pdfs/reliability_interoperability.pdf) [Accessed 13 Jan. 2018].

High-level expert group on information systems and interoperability (2017). Final report. Available at:

<http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=32600&no=1> [Accessed 20 Sep. 2017].

Kroski, E. (2005). The Hive Mind: Folksonomies and User-Based Tagging. Available at: <http://web20bp.com/13z2a6019/wp-content/uploads/2013/03/The-Hive-Mind-Folksonomies-2005.pdf> [Accessed 4 Mar. 2018].

Lewis, G. and Wrage, L. (2004). Approaches to Constructive Interoperability. Pittsburgh: Carnegie Mellon: Software Engineering Institute. Available at: <https://www.sei.cmu.edu/reports/04tr020.pdf> [Accessed 13 Jan. 2018].

Llanes-Padrón, D. and Pastor-Sánchez, J-A (2017) Records in contexts: the road of archives to semantic interoperability, Program, Vol. 51 Issue: 4, pp. 387-405. Available at: <https://doi.org/10.1108/PROG-03-2017-0021> [Accessed 15 Feb. 2018].

Meijers Committee. (2018). CM1802 Comments on the 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) 12 December 2017, COM (2017) 794. Available: [https://www.commissie-meijers.nl/sites/all/files/cm1802\\_comments\\_on\\_com\\_2017\\_794.pdf](https://www.commissie-meijers.nl/sites/all/files/cm1802_comments_on_com_2017_794.pdf) (Accessed 7 Dec. 2018).

Meyers, B. et al. (2004). SOSI: System of Systems Interoperability. Available at: [https://resources.sei.cmu.edu/asset\\_files/Presentation/2004\\_017\\_001\\_23607.pdf](https://resources.sei.cmu.edu/asset_files/Presentation/2004_017_001_23607.pdf) [Accessed 5 Jan. 2018].

Miller, P. (2000). Interoperability: What Is It and Why Should I Want It? Ariadne.ac.uk. Available at: <http://www.ariadne.ac.uk/issue24/interopability> [Accessed 7 Nov. 2017].

Microsoft Technet. (2001). Why Is Interoperability Important?. Available at: <https://technet.microsoft.com/en-us/library/bb463148.aspx> [Accessed 13 Jan. 2018].

The MITRE Corporation. (n.d.). Develop and Evaluate Integration and Interoperability (I&I) Solution Strategies. Available at: <https://www.mitre.org/publications/systems-engineering-guide/se-lifecycle-building-blocks/systems-integration/develop-and-evaluate-integration-and-interoperability-iampi-solution-strategies> [Accessed 20 Jan. 2018].

The MITRE Corporation. (2000). A Guide to Understanding Emerging Interoperability Technologies. Washington: The MITRE Corporation. Available at: [https://www.mitre.org/sites/default/files/pdf/bollinger\\_interop.pdf](https://www.mitre.org/sites/default/files/pdf/bollinger_interop.pdf) [Accessed 13 Feb. 2018].

Mizzi, M (2015) Schengen: finding the balance between security and freedom of movement. Available at: <http://eptoday.com/schengen-finding-the-balance-between-security-and-freedom-of-movement/> (Accessed 2 April 2018).

National Research Council. (1991), Intellectual Property Issues in Software, National Academies Press, Washington. Available from: ProQuest Ebook Central. [3 March 2018].

Ncoic. (n.d.). What is Interoperability? [online] Available at: <http://www.ncoic.org/what-is-interoperability> [Accessed 7 Oct. 2017].

Nygård, A. (2017). PAD - "Fundamental rights and the interoperability of EU information systems: borders and security". [email].

Quintel, T. (2018). Connecting personal data of Third Country Nationals: Interoperability of EU databases in the light of the CJEU's case law on data retention. [online]. Available at: <https://poseidon01.ssrn.com/delivery.php?ID=620116007095115072105064068068127067035074090016037034077026114100120007078005080068098110016004116055039006023123026111003076098025029084039109017080024002031127091056016001007008123089028106068086109013123096007093077122025125096108092064072087125031&EXT=pdf> [Accessed 15 Dec. 2018].

Privacy International. Privacy International response to consultation on the interoperability of EU information systems for borders and security. Available at: [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20171019\\_privacy\\_international\\_response\\_to\\_consultation\\_o](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/20171019_privacy_international_response_to_consultation_o)

n\_the\_interoperability\_of\_eu\_information\_systems\_for\_borders\_and\_security\_en.pdf  
{Accessed 20 Dec. 2018}.

Proposal for a Regulation No COM(2017)793 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. Available at: [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212\\_proposal\\_regulation\\_on\\_establishing\\_framework\\_for\\_interoperability\\_between\\_eu\\_information\\_systems\\_borders\\_and\\_visa\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_proposal_regulation_on_establishing_framework_for_interoperability_between_eu_information_systems_borders_and_visa_en.pdf) [Accessed 7 Jan. 2018].

Proposal for a Regulation No COM(2017)794 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). Available at: [https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212\\_proposal\\_regulation\\_on\\_establishing\\_framework\\_for\\_interoperability\\_between\\_eu\\_information\\_systems\\_police\\_judicial\\_cooperation\\_asylum\\_migration\\_en.pdf](https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171212_proposal_regulation_on_establishing_framework_for_interoperability_between_eu_information_systems_police_judicial_cooperation_asylum_migration_en.pdf) [Accessed 7 Jan. 2018].

Publications Office. (2005). Electronic interchange of data between administrations: IDA programme. Available at: <http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=LEGISSUM:l24147a> [Accessed 7 Nov. 2017].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [Accessed 7 Nov. 2017].

Saunders, M., Lewis, P. and Thornhill, A. (2016). Research methods for business students. 7th ed. Pearson Education Limited.

Seadle, M. (2010). Archiving in the networked world: interoperability. Library Hi Tech, Vol. 28 Issue: 2, pp. 189-194, Available at: <https://doi.org/10.1108/07378831011047604> [Accessed 18 Feb. 2018].

Skyttberg, N. et al. (2016). How to improve vital sign data quality for use in clinical decision support systems? A qualitative study in nine Swedish emergency departments. Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4893236/> [Accessed 5 Jan 2018].

Sheth, Amit. (1998). Changing Focus on Interoperability in Information Systems: From System, Syntax, Structure to Semantics. Available at: [https://www.researchgate.net/publication/220040889\\_Changing\\_Focus\\_on\\_Interoperability\\_in\\_Information\\_SystemsFrom\\_System\\_Syntax\\_Structure\\_to\\_Semantics](https://www.researchgate.net/publication/220040889_Changing_Focus_on_Interoperability_in_Information_SystemsFrom_System_Syntax_Structure_to_Semantics) [Accessed 20 Feb. 2018].

SIS II Supervision Coordination Group, Eurodac Supervision Coordination Group, Visa Information System Supervision Coordination Group. 2018. Available at: [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST\\_10484\\_2018\\_INIT&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10484_2018_INIT&from=EN) [Accessed 16 Dec. 2018].

Sudmanns, M. et al. (2017). Semantic and syntactic interoperability in online processing of big Earth observation data. Available at: <https://www.tandfonline.com/doi/full/10.1080/17538947.2017.1332112> [Accessed: 3 Jan 2018].

Teece, D. (2010). Business Models, Business Strategy and Innovation. Long Range Planning, [online] 43(2-3), pp. 172-194. Available at: <http://www.businessmodelcommunity.com/fs/root/8jig8-businessmodelsbusinessstrategy.pdf> [Accessed 3 Mar. 2018].

U.S. Department of Energy. (2016). The National Opportunity for Interoperability and its Benefits for a Reliable, Robust, and Future Grid Realized Through Buildings. [ebook]. Available at: <https://energy.gov/sites/prod/files/2016/03/f30/Interoperability%20and%20National%20Benefits%20Through%20Buildings-031616.pdf> [Accessed 13 Jan. 2018].

## 8. Appendix

<i>Results chapter:</i>	<i>Recommendation chapter:</i>
Advantage / Disadvantage of interoperability of EU information systems in the areas of border and migration	Recommendations aiming to tackle the challenges and enhance the benefits of the interoperability

### Data quality, data retention and data subject's access to their own data

Problems with data quality (wrong matches / inaccurate data) which might be either magnified or easier to spot thanks to the interoperability (European Union Agency for Fundamental Rights, 2017, p. 30 and European Data Protection Supervisor, 2018, p.23)	<p>5.1.1. To improve the data quality of legacy systems and test automatic data quality checks prior to their entry to operations (European Union Agency for Fundamental Rights, 2017, p.30):</p> <ul style="list-style-type: none"> <li>• Standardization of the data collection process (Skyttberg, N. et al., 2016);</li> <li>• Avoiding manual data entry, automatic error verification, double checks, data verification with data subject (European Union Agency for Fundamental Rights, 2017, p.34);</li> <li>• Development of the data quality checks prior to the Proposals implementation (European Data Protection Supervisor, 2018, p.25);</li> <li>• Ensuring that all Member States make an effort to improve the data quality (Committee on Civil Liberties, Justice and Home Affairs, 2018);</li> <li>• Use of Artificial Intelligence algorithms as a monitoring tool (European Economic and Social Committee, 2018, p.14).</li> </ul> <p>5.1.2. To implement data biometrics standards</p> <ul style="list-style-type: none"> <li>• To implement eu-LISA standard for captured and matched fingerprints and ICAO requirements for face images (European Union Agency for Fundamental Rights, 2017, p.32);</li> <li>• Common choice of Biometric Fingerprint File (European Commission, 2017c, p.20);</li> </ul>
---	---

- 
- Introduction of pop-up alerts in case of biometric data with a higher risk of being false (European Union Agency for Fundamental Rights, 2017, p.14).

5.1.3. To promote Universal Message Format (UMF) (Europol, 2014 and High-level expert group on information system and interoperability, 2017, p. 34)

5.1.4. To add the requirement of revision and update of the user profiles within central management of the interoperable system (European Data Protection Supervisor, 2018, p. 19)

5.1.5. Training (European Union Agency for Fundamental Rights, 2017, p. 19)

5.1.8. To define a valid search mode for the European Search Portal (European Commission, 2017c, p. 21)

5.1.10. To add a flag in a system, when yellow alert appear as a result of inconsistencies with data stored in *ETIAS* (European Union Agency for Fundamental Rights, 2017, p. 37)

5.1.11. To designate eu-LISA and authorities in the Member States as a joint data quality controllers (European Data Protection Supervisor, 2018, p.25)

5.1.12. To add child protection objective (European Union Agency for Fundamental Rights, 2017, p. 36).

---

Unclear procedure for data's subject to access, rectify, erase and restrict the data (European Data Protection Supervisor, 2018, p. 23)

5.1.7. To create an EU-wide portal handling requests related to the data access, rectification, erasure, restriction and data's subject claims for changing decisions based on the data stored in the system (European Union Agency for Fundamental Rights, 2017, p. 41)

---



ESP will query Interpol databases, which might contain biased data (European Union Agency for Fundamental Rights, 2018, p. 19)	5.1.9 To create a safeguard, that the owners of Interpol data (Third countries) will not have access to the information that their data was accessed and by which country (European Union Agency for Fundamental Rights, 2018, p. 20)
Different retention periods in the interoperable systems (Meijers Committee, 2018, Data retention, para 2.)	5.1.6 To clarify the data retention policy (European Union Agency for Fundamental Rights, 2017, p.22) <ul style="list-style-type: none"> <li>To shorter time limits for data preservation in the case of minors (Committee on Civil Liberties, Justice and Home Affairs, 2018)</li> </ul>

**Data minimization, purpose limitation, access to data, sharing the data with Third countries**

Potential undermining data minimization principle (Quintel, T, 2018, p. 15 and Article 29 Data Protection Working Party, 2018, p. 3).	5.2.1. BMS should match the data not to store it (European Union Agency for Fundamental Rights, 2017, p. 24)
	5.2.1. To remove unnecessary data from CIR (European Union Agency for Fundamental Rights, 2018, p.24)
	5.2.6. To remove ECRIS-TCN from MID (European Union Agency for Fundamental Rights, 2018, p. 39)
Potential undermining purpose limitation principle (Quintel, T, 2018, p. 15 and Article 29 Data Protection Working Party, 2018, p. 3).	5.2.3. To allow law enforcement access CIR only for “the purposes of preventing, detecting and investigating terrorist offences or other serious criminal offences in a specific case” (Article 22, COM(2017)793) (European Union Agency for Fundamental Rights, 2018, p.26)
Broader access of law enforcement officers to the data in CIR (European Union Agency for Fundamental Rights, 2018, p. 10)	5.2.4. To introduce safeguards for protecting the data against unauthorised access (European Union Agency for Fundamental Rights, 2017, p.26)
	5.2.5. To clarify the conditions under which eu-LISA has access to the interoperable databases (European Data Protection Supervisor, 2018, p. 28)

---

## System governance

---

Need for increased system governance  
(Committee on Civil Liberties, Justice and  
Home Affairs, 2018)

5.3.1. To improve the governance of the  
interoperable systems

- Annual reporting of eu-LISA to EDPS and Commission on the implementation of interoperability and reporting every two years on the impact of interoperability on fundamental rights (Committee on Civil Liberties, Justice and Home Affairs, 2018)
  - Designation of Member States a central verification authority (European Union Agency for Fundamental Rights, 2018, p.34)
-