Implementation of Information Security in the EU Information Systems

Maris Järvsoo, Alexander Norta, Valentyna Tsap, Ingrid Pappel, Dirk Draheim

Implementation of Information Security in the EU Information Systems
An Estonian Case Study

Maris J¨arvsoo[1], Alexander Norta[1], Valentyna Tsap[1], Ingrid Pappel[1], and Dirk Draheim[1]

Large-Scale Systems Group
Tallinn University of Technology
Akadeemia tee 15a, 12618 Tallinn, Estonia
{maris.jarvsoo,alexander.norta,valentyna.tsap, ingrid.pappel,dirk.draheim}@ttu.ee

Abstract. In this paper we present the findings of a case-study on IT system security in the area of EU internal security and justice. We have analyzed the implementation of information security for the EU information systems EURODAC, SIS II and VIS in case of Estonia. The analysis comes in a situation, where there are multiple regulations, directives, guidelines; but it lacks a unified standard for the implementation of the member states subsystems. The main finding is that a separate standard is not necessary; however, there is a need for setting minimum requirements, ensuring security of the information systems, that come with appropriate guidelines that help the member states to achieve the minimum requirements. The second finding is that there is a need for greater cooperation and an increased knowledge exchange of the methods used in the member states. Following defined guidelines and exchanging knowledge would help to strengthen the level of security for the entire system.

Keywords: Schengen, GDPR, EU-LISA, EURODAC, SIS II, VIS, IT security, ISO 27001

1 Introduction

In this paper we analyze the implementation of information security in the largescale information systems operated by EU-LISA (European Agency for the Operational Management of large-scale IT Systems in the Area of Freedom, Security and Justice), that help to manage the border crossings and asylum requests to secure the Schengen Area.

Since the formation of the European Union, its main goal has been a free market, freedom of movement and residence. In 1985, the Schengen Area was established and borders between the EU member states exist only on the map. Citizens from member states of the Schengen Area can move freely; border control exists only on the external border of the Schengen Area. Freedom always

comes with responsibilities – the member states have to make sure that travelers from third countries, who are entering the Schengen Area are people with good intentions and without criminal background. This is extremely important, because the entering point to the area might not be the same as the travel destination. Take the Berlin terror attack on 19th of December 2016 as an example – the attacker who was driving the lorry into the crowd in Berlin, Germany, was later found in Milan, Italy. This illustrates how easy it is to travel to another country – even in a situation of heightened security risks. Cooperation is the crucial part in the context of free movement. Therefore, the European Commission has requested the development of information systems that share and control the information of travelers. The main information systems are SIS II (Schengen Information System II) [15], VIS /(Visa Information System) [16] and EURODAC (European Asylum Dactyloscopy Database) [12]. These systems share information between the member states, allowing authorized personnel to process personal data and see if a person is flagged for some reason.

The security of the persons crossing the borders or checked in other circumstances is also of highest priority. Therefore, the information security of the EU information systems is a very important topic. A good learning point are the cases of Danish and Swedish authorities in 2013, where information leaked from their national interfaces. The same hacker was involved in both cases and about 1.2 million records of personal data from the SIS information system were found from the hackers' devices. Hacking took place in the summer of 2012 and was discovered by the Swedes. None of the Danish systems alerted Danish stakeholders about the problems; they learned about it from Swedish officials.

Research Questions We analyze the implementation of information security of the systems SIS II, VIS and EURODAC from the perspective of the Estonian member state systems provider. The questions that we deal with are the following:

(i) What is the exact policy making and management process of the EU information systems? In particular, how are system requirements managed?
(ii) How effective are the current regulations, how many of those are mandatoryand how is the implementation monitored by member states?
(iii) Does the EU need a unified standard on ensuring information security oflarge-scale information systems?

Methodology and Data In service of (i)-(iii) we have conducted an *in-depth review of the relevant EU regulations* (directives, implementing decisions, regulations). We present the outcome of this analysis. Furthermore, we have conducted a systematic expert interview with *the security officer of EU-LISA*. Furthermore, we have conducted systematic expert interviews with the *two key*

IT stakeholders that have been responsible for the Estonian EU information systems for at least three years at the time of the research. We have systematically analyzed[1]the interviews. We present the outcome of this analysis.

Paper Outline We start with a detailed explanation of important backgrounds fact about the EU information systems and their implementation issues in Sect. 2. Section 3 presents our findings with respect to question (i). Section 4 presents our findings with respect to question (ii). Section 5 presents our findings with respect to question (iii). We discuss relevant related work throughout the paper and delve into some selected related in Sect. 6. We finish the paper with a conclusion including some concrete suggestions in Sect. 7.

2 Operations of the EU-LISA Information Systems

2.1 The EU-LISA Information Systems

The EU-LISA authority has been established in 2011 [21]. The authorities' responsibility is the preparation, development and operational management of the information systems SIS, VIS and EURODAC. The systems must be operational 24/7. Furthermore, EU-LISA is responsible for ensuring data and systems continuity, security, integrity, availability, compliance with EU data protection regulations [18–20,11] and training of the national authorities. To serve these tasks EU-LISA needs to collaborate with national systems providers, data protection supervisors and the security officers network.

The *Schengen Information System* (SIS) [15] core function is exchange of information between national border control, police and customs officials. The exchanged information contains alerts about persons, e.g., missing persons and children; also, information about stolen and lost documents and property – money, vehicles, firearms. The EURODAC [12,14] system is an instrument to fulfill the Dublin regulation [8][2], which helps to compare fingerprints, to find out whether a person has already applied for asylum in another member state or whether a person stays illegally in a state. Thus, it helps to avoid outwitting the European law by "asylum shopping" (attempt to get asylum in more than one member state). The purpose of VIS [16] is to improve the visa policy and cooperation between member states; in particular, it facilitates the checks at the external borders of the Schengen Area. It serves the following tasks: proceeding visa applications, controlling persons and their visa against the system, managing asylum requests, identification and checking whether conditions for an entry, stay or residence are fulfilled.

[1] tool-based, standard thematic analysis with NVIVO

[2] formerly known as Dublin Convention

The main parts of the information systems are central databases and uniform national interfaces. Every member state develops, operates, maintains its national systems, which hold copies of the central systems. The national copies are for conducting automated searches on member states' territory. Data is entered to the central system. It is not possible to search data from another member states' national interfaces. A communication infrastructure between central systems and national interfaces enables searches and information transfer. The communication infrastructure provides an encrypted network for the data exchange. Every Member State has the authority and responsibility for operating the national interfaces, assuring security and compliance with the regulations.

2.2 Data Exchange and Protection in the Field of Police and Justice

By its nature, the field of police and justice that requires processing of sensitive personal data –data leakage or other illegitimate use of data might result in violation of privacy or personal harm. The field covers the areas of police and border control, asylum and immigration, judicial cooperation in civil as well as in criminal matters and police cooperation. Therefore, this field needs a tailormade protection method for data protection [4]. The data protection directive 95/46 makes no difference between fields of data usage, therefore data protection in a field of police and justice is not regulated specifically. The directive is not applying outside of the boundaries of community law. Despite of that, the member states have widened the scope of the directive by engagement of the directive to the national law [1,26]. The need for a specific regulation for field was acknowledged already in 1987, by the council of Europe. Since then the provisions have been adopted and in 2005 the Krakow declaration was adopted [13]. Before the Krakow declaration Europol adopted an Eurojust decision in which the detailed framework regarding data protection and operation in police authorities was brought out [1].

Since the 9/11 terror attack in the USA, transmission of information from one field to another has increased so that information collected for specific purposes might be transmitted to another field and used for other purposes. This is a risk in terms of data protection and is not in accordance to the principles of integrity and human rights. The more officials and authorities have access to the information, the higher is the risk of entering the incorrect data that might affect the person in other situations; for example, the visa application process might be more difficult if the SIS II contains a note about the person or the police might use expired information during the discretion process. These problems can be solved by applying strict access management processes, e.g., task-oriented access [28].

With the new EU data protection regulation GDPR (General Data Protection Regulation) [20], the focus lays on the minimization of collected data. Therefore,

data protection should be implemented by design, e.g., by measures such as "data protection by default". The GDPR contains a directive regarding data processing for prevention, investigation, detection and prosecution of criminal offences as a tailor-made tool for the police authorities [20].

2.3 Data Exchange and Protection Requirements

Exchange of the supplementary information of SIS II and VIS, between Member States and Central units goes according to the SIRENE (Supplementary Information Request at the National Entries) manual [9]. EURODAC data was transferred between the central unit and the member states by using the TESTA II (Trans-European Services for Telematics between Administrations) infrastructure [7], which is, basically, a virtual private network for public administrations. TESTA II was upgraded to a sTESTA. In 2006 and in 2013, the fourth generation was brought into live with TESTA-ng. TESTA can be used to exchange both classified and unclassified information. In case that the communication infrastructure cannot be used, the member states can use other sufficiently secured channels. To make sure that information can be transmitted to the authority, a security plan must contain the communication control protocol, where the requirements of the accepted authorities are listed [15].

According to the EU-LISA IS regulations [12,15,16], it is prohibited to make data available to the third parties such as international organisations or third countries. Member states shall have the independent supervisory authority that assures the lawfulness of the data processing procedures and helps to solve requests regarding personal information held in the information system. The national supervisory authority conducts an audit once in every four years. Similarly, the EU data protection supervisor conducts an audit once in every four years with respect to the central systems. To ensure a coordinated supervision, the national supervisory authorities and the EU data protection supervisor meet every half year to discuss problems, exchange information and unify the regulation.

3 Policy and Management

In this section, we analyse the policy making and management process of the EU information systems.

3.1 Document analysis

Management of the Information Systems The overall security measures of the EU are covered by the EU regulation 2017/46/EC [11]. The regulation sets areas of responsibilities for different groups and authorities of the EU. Altogether, the it brings out nine different authorities and groups with their areas of responsibilities. The authorities are listed hierarchically, which means, that lower authorities and group reports to higher and some of the responsibilities

are fulfilled together. Every authority monitors the execution of some areas of the strategies or policies and creates the frameworks within the service providers or national authorities must work in. Access to cryptology measures is given by the directorate of general human resources and security; and the access is asked by the system owners. Five of the nine authorities are creating strategies, frameworks and policies; three groups, i.e., system owners, data owners and LISOs (Local informatics security officers), provide input for the guiding documents. The last group, i.e, the users, is obligated to follow the rules and recommendations.

The NIS (Network and Information Systems) directive [18] came into force in May 2018. The NIS directive requires the usage of information security standards, however, leaves open the choice of the standard. The aim of the NIS directive is to gain a commonly high level of security of network and information systems across the EU. Therefore, the directive focuses on public-private cooperation and sets the requirement for the member states to establish an information security strategy. The main concerns are security incidents and their surveillance. Every member state must have a CERT (Computer Emergency Response Team) managing information security incidents. To equalize the level of security, the NIS directive sets reporting obligations to the member states. The commission evaluates the execution of the directive after every two years. In addition to the CERTs, each member state has to name an authority as contact point for the EU Commission. The contact point is also responsible for evaluation and application of the directive. The reporting obligation expands on every service provider – public or private – who operates with the critical infrastructure and internationally vital services. The NIS directive points out that it needs a common ground and understanding of the systems' security.

Cooperation The NIS directive [18] recommends a higher level of cooperation between the relevant authorities in the member states and EU authorities such as ENISA (The European Union Agency for Network and Information Security). It also suggest to consult with the interest groups in policy making and improving. Regarding SIS II, which is the largest information system in EU, the SIRENE manual [10] was created; in order to set the boundaries to the operations by the member states. SIRENE bureaus are the main contact points to every official operating with information entered to SIS II. Through the SIRENE bureau the cooperation with EUROPOL, EUROJUST and INTERPOL is organized. All SIRENE bureaus are cooperating with each other, in particular, to solve the issues on why information has been entered [10].

3.2 Interview Analysis

Management of the Information systems The EU-LISA security officer finds that despite the requirement of compiling security plans and setting the specific rules inside the State, there are member states that are not able to conduct the

specific security plan. Some of the states are able, but not willing; therefore. the quality of the security plans is lacking behind; and based on them it is difficult to make management decisions. To help member states to raise the level of security knowledge and ability to develop the measures themselves, EU-LISA is working on a security and continuity management system, together with the business continuity plans and security incident management procedure; in order to make them more acceptable to the member states. That would grow their knowledge about preventing incidents and avoiding them to happen. The templates are being renewed together with the EU Commission, to ensure that their requirements are still satisfied. The requirement from the NIS directive is that all of the member states would use a standard to help them prepare the security of the systems and therefore those templates are being renewed to be compliant with relevant ISO requirements. The member states are aware of the need for the security plan, but the need for them is taken more as a requirement, that shall be done, but not as a strategic planning paper, that could help them to increase the level of security. The member states are rather following the internal state requirements and standards, as, e.g., the ISKE [23] standard in Estonia.

From the member state perspective, the management of the systems is bureaucratic, but they also see, that large-scale information systems need some level of written bureaucracy to ensure continuity. There could be less paperwork, which would help to work faster with the developments. Every aspect shall be discussed to ensure a joint understanding, but the accepting rounds could be shorter. Each larger change needs to go through a change management group for final agreement, but before that discussions occur in working groups, after that in advisory groups, from which the first is focusing on the business side of the system and another is a technical group. The process through each group is long and takes a lot of time.

Cooperation The cooperation between member states and the central coordination organization is not as good as it should be. The cooperation is based on the required meetings and paperwork, that shall be done, but there is no open discussion, to help the whole EU system to improve. To start an open discussion the security officers network (SON) was created, where every member state could share the experience and therefore help out the others that are falling behind or could gain the knowledge needed to improve their own systems. The attitude is hard to brake; therefore, the SON is still working as a mandatory meeting, not as the open discussion round. Required security plans are presented, but some member states are trying to write the paper as superficial as possible or as they assume the EU-LISA would like to see it, to prevent further questions and discussions. The reality might not be compliant with the information presented on the paper. According to the EU-LISA experience, some of the member states are working hard to be independent and not give any information out to the EU, which makes ensuring the security of the central

system much harder, because of the lack of knowledge on what is going on in the member state systems.

The cooperation between member states has been getting better over the time. Unofficial meetings have started occurring, where the developments are discussed. Usually, the highlights are brought up in there, but there is a chance to ask for help if needed. There are also working e-mailing lists. Despite that the communication could be better. The knowledge exchange is not working in daily bases, but the meetings initiated by the member states could be a starting point for that. The cooperation between some of the member states is better than the whole picture. The example in here is the Estonian-Finnish collaboration in testing the systems.

The inhibitors for the active cooperation are the official meetings, where the officials of the EU Commission are also present including to the member state representatives and EU-LISA. Those meetings are controlled and participants are holding back their thoughts. The presence of the EU Commission official is restraining the member states, which was the reason of starting the unofficial meetings. The cooperation between the EU-LISA and member States are mostly good and the necessity is understood, but there have been problems over the time regarding the communication – where one party is not understanding the responsibilities or the central control has trouble in understanding the situation of member states; and therefore the advice they are giving is not suitable. Therefore, the member state specialists are hoping that the inner process will be better soon.

3.3 Summary of Findings

The document analysis and interviews show that there are multiple levels of decision makers, which makes the decision process time consuming. Forms are created for the tasks, procedures of usage are set, but the importance and usage are still unclear. Documents such as the security plan (that should be helpful for member states in planning their security strategy; that should be helpful for the central decision makers for seeing the continuity process and give a hand if necessary) are not fulfilling their purpose, because they are seen as a bureaucratic procedure. On the other hand, some level of bureaucracy for managing the systems with the capacity as those is necessary. The level shall be looked over and updated.

The cooperation between member states is still weak, but it has started to develop. The specialists see that the cooperation between the member states will increase organically and that cannot be pushed, because by pushing it might lose its focus. Cooperation between the member states is evaluated as quite good and

the need for an organization as EU-LISA is seen, but it has its problems. The main problems are communication problems, whenever one party is not able to understand the needs of the other. The biggest problem is with the EU Commission, which is seen as a biggest inhibitor of cooperation. In the official meetings where the EU Commission is present, the member states are holding back their thoughts and are not willing to open discussions.

EU-LISA also sees the problems and on their side the main problem is lack of communication. The regulated reports are given, but the knowledge exchange and unofficial communication is not working. EU-LISA tries to change the attitude and by creating SONs to induce the cooperation.

4 Ensuring Security in Data Exchange and Operation

This section deals with the question of how effective the current regulations are, how many of those are mandatory and how the implementation by member states is monitored.

4.1 Document analysis

Data Exchange and Measures The aim of the GDPR regulation is to unify the requirements of the data regulations across the EU. According to the GDPR information can be processed only by the competent authorities and according to the rules set by the EU. The work of the authorities is controlled by the independent data protection officers, whose role is ensure that personal information is used only within the frames of the regulations and the rights of the data subject are not affected. GDPR is particularly relevant from the IS development perspective, because it encourages the privacy by design approach [19,20]. All the information systems and their management shall be compliant with the principles of data protection set in those regulations. Regarding the information systems, used in the case, the personal data protection is vital, because of the nature of the systems. The collection of the data, storing and management has to be in correlation with the regulations. Data leakages shall be recorded, fixed and reported to the data protection authorities and their recommendations shall be considered. On the other hand, the data protection officers are the help for the data subject, whenever data subject needs the consultation, the authorities shall give it and regarding the deletion and correction of the data authorities shall observe the rights of the data subject are fulfilled [10,12,15,17,20,19,16].

The information exchange in case of the systems used in the field of internal security and justice is according to the system regulations through the information exchange interface, which allows the secure communication with other authorities. The information exchange goes through the TESTA network, which enables also the exchange of the classified information due to the encryption possibilities. The supplementary information exchange in SIS II is organised through SIRENE bureaus, where the information exchanged shall be on

the specific forms. In all cases the other channels may be used only in extremely urgent cases or if the information systems are not operational.

Information Security and Measures The NIS directives' aim is to achieve an equally high level of the information security all over the EU. To achieve that goal, it is important for all member states to follow similar approaches regarding information system security. The NIS directive brings out the need for standardized minimum requirements and guidelines to achieve the outcome. The other important steps to gain the equally high level of security is the cooperation, information exchange and similar requirements for the public and private authorities who operate with the information systems regarding vital services. The NIS directive proposes that every member state shall have a national strategy for information security and policies to exploit. In addition to the national paperwork, the incidents shall be handled through the CIRT (Cyber Incident Respons Team) or CERT. In addition, the CIRT and CERT are reporting to the EU, therefore there is a shared incident knowledge allover the EU. The NIS recommends that the member states take into use some of the internationally accepted information security standards, to be able to equalize the level of security[18].

The system regulations bring up the need to put the managerial requirements and polices in place. The polices shall include access management policies (which must be implemented for the physical locations where the information is held or where the systems are located) and digital security measures, which include the access to the systems and logging process. Another measure that helps to prevent the manipulation of the information across the state borders is that the owner of the information entered to the system is the member state that enters the information at the first place; and the other member states shall transmit the information that should be implemented to the owner of the information [15–18].

4.2 Interview analysis

Data Exchange and Measures The specialists see the existing information exchange network as secure in general. The information is moved through defined channels according to the defined protocol in the interface control document. The protocol itself arises more concerns. Despite the existing interface control document, the member states implement the sending of the forms differently and that can cause problems. Those problems are raised in the working group meetings and implementation details of the forms are being discussed. Solving those problems can be a slow process. The physical environment security is in accordance to the regulations, which is controlled by the local data protection authorities.

Information Security and Measures The security plans are mandatory, but the quality of the papers is low. This has many reasons: some of the states do not have enough knowledge to develop the complex security plans and systems, whereas some of the states are not willing to share the information to avoid questions and suggestions for improvement from the side of the EU. The variety in the quality is making the evaluation of the overall systems' security difficult. The member states do not have an overview about the others' security measures and do not know, whether and what international standards are used. The security measures required by the EU are comprehensive.

The specialists from the member state see the security rules as strict, in particular, the process described in the interface control document. Responses to some of the questions must pass multiple levels of contacts, because of the right to access rules. Every level of contact has the information they are allowed to process and therefore it is not possible to get the answers from just one level for some questions.

Specialists view some aspects as over-regulation. For example: whenever the report of data usage and handling has to be done, the member states must create their own reports, which will be combined by EU-LISA later, to present it to the EU Commission, despite they have access to all the information stored by member states and they could to it themselves. This situation has been brought up at the working groups for many times, but the obstacle are regulations which are not allowing EU-LISA to operate with the information that is held by member states. Member states have all proposed that they would give the mandate to EU-LISA to manage the information for creating the reports, to lower their own administrative burden, but until now, that has not been changed.

4.3 Summary of Findings

On the one hand security requirements by the EU are comprehensive, but grant enough freedom for the member State to choose the measures suitable for their inner legislation. This leads to a situation where it lacks overview about the used security measures, despite the evaluations conducted. The evaluations are member state specific and are not compared to see their compatibility to each other. Request brought out in NIS directive should give a clearer overview, if all member states would use the internationally accepted standards. On the other hand, some aspects are over-regulated, which leads to the administrative burden.

5 Usage of Standards

This section approaches main question of paper, i.e., whether the EU needs a unified standard on ensuring information security of large-scale information systems in case of the EU information systems.

5.1 Document Analysis

The first time that the need for the usage of internationally accepted information security standard is pointed out in the NIS directive is in its article 19, where it recommends to adopt standards to reduce the amount of the different approaches; but the directive does not detail out, which standard should be used [18]. The information systems' regulations use similar requirements for the systems security, but those requirements are high level and are not setting guidelines how to fulfill the requirements. The term "standard" is used in SIRENE manual [10], where the basic requirements as acceptability, continuity, confidentiality and access are described.

International standards such as ISO27001 [24], guidelines as ISO27002 [25] and baseline standards as the German IT-Grundschutz [6] and the Estonian ISKE [23] are used. The ISO standards are rather applied to the information management systems and their requirements, the polices that shall be implemented in the organization and less to the security of the systems itself; whereas the baseline standards are applied to both. The ISO requirements are in accordance to the requirements set by the EU regulations – requiring risk assessment, policies for access and operation of the systems. The base line standards evaluate the information systems based on the information stored in the systems, the users and the field of usage in addition to the managerial policy requirements.

5.2 Interview Analysis

The variety of standards, that could be used at state level is not the question. A problem is when a member state is not using any; then it is not possible to say whether it is moving in a right direction or whether its security work is consistent.

Specialists brought out the Estonian ISKE standard. The official audits are still in progress, but as the specialists see, ISKE measures are suitable for assuring the minimum-security requirements. The audit is completed for the EURODAC system and the results showed that ISKE is suitable and covers all the requirements set for the systems' security. On the other hand, it is hard to see, what other member states are using and if those standards or other security methods are suitable; and this is hindering cooperation. In addition to the cooperation there cannot be a certainty of the security of the other member states' systems if the security measures are not clearly stated. The specialists see the similar grounds in securing the systems as a good solution to increase the level of overall security. The problem, the specialists brought out for creating a standardized approach to systems security is the over-regulation. There are many regulations already in place, creating a new one might cause problems with existing internal state regulations and the capability of developing the systems according to the new regulations. The new regulation setting the specific requirements would be micromanaging by the EU Commission and therefore the

member states are not able to develop according to their insights. Overall, requirements shall be acceptable and feasible for all the member states. The EU Commission cannot require high level security if some member states are not able to comply with them; on the other hand, some member states are capable for more, and because of the requirement they cannot develop higher level security for the information system.

5.3 Summary of Findings

The NIS directives' request for using the internationally accepted security standards would help to make the security evaluation clearer; but none of the interviewees brought out specific preference and need for all the member states to follow the same standard.

The interviewees would like to have a best practice example which shall be followed; but it should not become an official standard, to avoid the growing bureaucracy. They see the example as guideline and minimum requirements, but it should not be a standard that shall be followed line by line. The guideline should be flexible and mandatory only for the less capable parties. More capable member states can design their methods that are more than set on the minimum level.

6 Related Work

A similar research has been conducted by RAND corporation [27]. The analysis includes the same regulations as in this paper. The authors come up with similar results: even though there are many regulations, policies, and directives – they might not improve the overall security of the systems and instead can slow down the progress in IT. Change is needed in the form of less regulations, updated standards and more open communication and information sharing among states' specialists. The societal expectations have grown and the technologies have evolved; therefore, the existing systems and their regulations are getting outdated.

An analysis of the connection between European migration policies and digital technologies is provided by [22]. The analysis encompasses the EU information systems SIS II, VIS, EURODAC. The case of Italy and Spain is treated, two countries that are perceived as EU 'gatekeepers' in the last years. The research delves into compliance/non-compliance with surveillance systems in the southern European member states. Furhermore, it carves out differences between the two countries regarding their overall migration policies.

Discussion of compliance strategy of Schengen border states with respect to Eurodac regulations are treated independently by several authors [5,2,3,29]. The research delves into the political and legal dimension of the compliance, whereas we treat the information security perspective in this paper.

7 Conclusion

There is a great amount of bureaucracy in the management of the EU information systems, which in some amount is necessary to operate such large-scale systems. The decision making goes through multiple levels of authorities and therefore the process is slow. The cooperation is mostly based on necessity or covered with the requirements of the regulations, but the knowledge exchange is still weak. The security requirements are comprehensive and give some amount of freedom to choose exact methods; but on the other hand they are bureaucratic and cause the administrative burden to the member states. The data exchange process is detailed and well regulated by an interface control document. Accepting already existing internationally accepted standards is preferable and gives a better overview of the security measures used. A unified standard is not necessary, but guidelines and examples should exist to gain a mandatory/minimum acceptable level. Through cooperation and knowledge sharing, the overall level of security can be raised by implementing those measures and thus the NIS directive expectations can be reached.

References

1. Alonso Blas, D.: Ensuring effective data protection in the field of police and judicialactivities: some considerations to achieve security, justice and freedom. ERA Forum
   11(2), 233–250 (Aug 2010)
2. Aus, J.: Supranational governance in an area of freedom, security and justice –eurodac and the politics of biometric control. Tech. Rep. DEI Working Paper, no.72, Sussex University Institute (2003)
3. Aus, J.: Eurodac – a solution looking for a problem? European Integration OnlinePapers **10**(6), 1–26 (2006)
4. Boehm, F.: Information Sharing and Data Protection in the Area of Freedom, Security and Justice – Towards Harmonised Data Protection Principles for Information Exchange at EU-level. Springer (2012)
5. Brouwer, E.: Eurodac: Its limitations and temptations. European Journal of Migration and Law **4**(2), 231–247 (2002)
6. Bundesamt fu¨r Sicherheit in der Informationstechnik (BSI): IT Security Guidelines– IT-Grundschutz in brief. BSI, Bonn (2007)
7. Commission Staff Working Paper: First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit. Commission of the European Communities, Brussels (2004)
8. Conventions signed between Member States: CONVENTION determining theState responsible for examining applications for asylum lodged in one of the Member States of the European Communities. Official Journal of the European Union (L 254), 1–12 (1997)
9. Council of the European Union: SIRENE Manual. Official Journal of the EuropeanUnion (L 38), 1–24 (2003)
10. European Commission: COMMISSION IMPLEMENTING DECISION (EU) 2015/219 of 29 January 2015 replacing the Annex to Implementing Decision 2013/115/EU on the

Sirene Manual and other implementing measures for the second generation Schengen Information System (SIS II). Official Journal of the European Union (L 44), 75–116 (2015)
11. European Commission: COMMISSION DECISION (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. Official Journal of the European Union (L 6), 40–51 (2017)
12. European Council: COUNCIL REGULATION (EC) No 2725/2000 of 11 December2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. Official Journal of the European Union (L 316), 1–10 (2000)
13. European Data Protection Supervisor: DECLARATION. In: Spring Conference ofEuropean Data Protection Authorities. pp. 1–2. Krakow (2005)
14. European Data Protection Supervisor: Eurodac Supervision Coordination Group Second Inspection Report. Secretariat of the Eurodac Supervision Coordination Group, Brussels (2009)
15. European Parliament and Council: REGULATION (EC) No 1987/2006 of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II). Official Journal of the European Union (L 381), 4–23 (2006)
16. European Parliament and Council: REGULATION (EC) No 767/2008 of 9 July2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation). Official Journal of the European Union (L 218), 60–81 (2008)
17. European Parliament and Council: REGULATION (EU) No 603/2013 of 26 June2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013. Official Journal of the European Union (L 180), 1–30 (2013)
18. European Parliament and Council: DIRECTIVE (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union (L 194), 1–30 (2016)
19. European Parliament and Council: DIRECTIVE (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Official Journal of the European Union (L 119), 89–131 (2016)
20. European Parliament and Council: REGULATION (EU) 2016/679 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). Official Journal of the European Union (L 119), 1–88 (2016)
21. European Parliament, Council of the European Union: REGULATION (EU) No1077/2011 of 25 October 2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice. Official Journal of the European Union (L 286), 1–17 (2011)
22. Fragapane, S., Minaldi, G.: Migration policies and digital technologies in Europe: a comparison between italy and spain. Journal of European Integration **0**(0), 1–17 (2018)

23. Government of the Republic of Estonia: Infosu¨steemide turvameetmete su¨steem.Riigi Teataja (252) (2009)
24. ISO/IEC 27001:2013: Information technology – Security techniques – Informationsecurity management systems – Requirements. International Standardization Organization (2013)
25. ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls. International Standardization Organization (2013)
26. Marquenie, T.: The police and criminal justice authorities directive – data protection standards and impact on the legal framework. Computer Law & Security Review **33**(3), 324 – 340 (2017)
27. Robinson, N., Gaspers, J.: Information security and data protection legal and policy frameworks applicable to european union institutions and agencies. Tech. rep., RAND Corporation (2014)
28. Rull, A., Ta¨ks, E., Norta, A.: Towards Software-Agent Enhanced Privacy Protection, pp. 73–94. Springer (2014)
29. Trauner, F.: Asylum policy – the EU's 'crises' and the looming policy regimefailure. Journal of European Integration **38**(3), 311–325 (2016)