D1.4: Analysis of the legal and regulatory framework

Document Date: 22/03/2019

Work Package 1: End-user requirements and needs

Document Dissemination Level: Public

TRESSPASS - robusT Risk basEd Screening and alert System for Passengers and luggage
Funded by the Horizon H2020 Framework Programme of the European Union for Research and Innovation, Grant Agreement number: 787120

ABSTRACT

The goal of TRESSPASS is to develop, demonstrate and validate a single cohesive risk-based border management concept for air, maritime, and land border crossing points. As part of this goal, this document aims to identify existing legal boundaries to the implementation of risk-based border management approaches as well as to provide inputs for refining the proposed concept according to current legal standards in this document. We present a structured review of the current legal and regulatory framework of the European Union regulating checks on travellers and goods at the frontiers, with a particular focus on its most recent developments.

The analysis is guided by six research questions related to the primary functions of border checks described in TRESSPASS Deliverable D9.6 ('access and egress control function' based on the 'revelatory function'). Chapter 1 introduces the background and aim of the document, chapter 2 presents its methodology, chapter 3 then gives a detailed overview of the legal and regulatory framework, and chapter 4 finally presents a summary and conclusions.

While the legal base for risk-based checks has been introduced into the domain of civil aviation security screening with Regulation (EC) No 300/2008 and the domain of customs checks with Regulation (EU) No 450/2008 (replaced by Regulation (EU) No 952/2013, the Union Customs Code, in 2013), currently, there are no regulations that facilitate risk-based screening of passengers and their goods at EU border crossings. In order for the TRESSPASS concept to be fully compliant with this legal framework, pilots of the concept must either be run independently of regular border checks or seek specifications within the current regulations.

In order for the TRESSPASS concept to be fully compliant with current legal requirements regarding data protection and exchange, the processing of personal information within it will have to be justified appropriately. It will have to be transparent what personal data is processed by whom, how and why, while keeping in line with existing laws restricting data sharing between states and organisations.

Project Information

Project Name	robusT Risk basEd Screening and alert System for PASSengers and luggage
Project Acronym	TRESSPASS
Project Coordinator	National Center for Scientific Research "Demokritos", EL
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Call	H2020-SEC-2016-2017 (SECURITY)
Topic	SEC-15-BES-2017 "Risk-based screening at border crossing"
Funding Instrument	Innovation Action
Grant Agreement No.	787120

Document Information

Document reference	D1.4
Document Title	Analysis of the legal and regulatory framework
Work Package reference	T1.4: Legal and regulatory framework
Delivery due date	28.02.2019
Actual submission date	22.03.2019
Dissemination Level	Public
Author(s)	Céline Delay, Johanna Müller, Slavtcho Groshev (CASRA)
Contributor(s)	Elisa Orru (ALU-FR), Christoph Meier (CASRA), Predrag Mitrovic (ED), Evangelia Michailidou (IAPR), Emmanouil Kermitsis (KEMEA), Artur Zukowski (PBG), Dionysia Ntaliou (PPA), Astrid Hakvoort (RNM), Jeroen van Rest, Mark van den Brink (TNO), Giovanni Vassallo (Z&P)
Document Review Status	☒ Consortium ☒ WP leader ☒ Technical Manager ☐ Quality and Risk Manager ☒ Ethical Advisory Board ☐ Security Advisory Committee ☒ Project Coordinator

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
API	Advance Passenger Information
APIS	Advance Passenger Information System
BCP	Border Crossing Point
Cepol	European Union Agency for Law Enforcement Training
CIS	Customs Information System
CRMF	Customs Risk Management Framework
CRMS	Customs Risk Management System
DPA	Data Protection Authorities
DPO	Data Protection Officer
EC	European Commission
ECRIS	European Criminal Records Information System
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EES	Entry/Exit System
EFTA	European Free Trade Association
EMCDDA	The European Monitoring Centre for Drugs and Drug Addiction
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EU	European Union
eu-LISA	The EU Agency for the operational management of large-scale IT systems
EUR-Lex	Official website of European Union Law and other public documents of the European Union (EU)
Eurodac	European Dactyloscopy
Europol	The European Police Office
Eurosur	European Border Surveillance System
FADO	False And Authentic Documents
Frontex	European Border and Coast Guard Agency
GDPR	General Data Protection Regulation
HCG	Hellenic Coast Guard

IBM	Integrated Border Management
IMO	International Maritime Organization
IAPR	Independent Authority for Public Revenue (Custom Service-General Directorate of Customs and Excise Duty, Greece)
ISPS	International Ship and Port Facility Code
OJ	Official Journal of the European Union
PDPD	Police Data Protection Officer
PIU	Passenger Information Unit
PNR	Passenger Name Record
PPA	Piraeus Port Authority S.A.
PRADO	Public Register Of Authentic Identity And Travel Documents Online
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SBC	Schengen Borders Code
SIRENE	Supplementary Information Request at the National Entry
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Document
SOLAS	International Convention for the Safety of Life at Sea
TCN	Third-Country Nationals
TDAWN	Travel Documents Associated with Notices
TRESSPASS	robusT Risk basEd Screening and alert System for PASSengers and luggage
UCC	Union Customs Code
VIS	Visa Information System

Table of Contents

1 INTRODUCTION

1.1 Background

The goal of TRESSPASS is to develop, demonstrate and validate a single cohesive risk-based border management concept for air, maritime and land border crossing points. The innovation action project addresses border control tasks at regular border crossing points, such as customs and smuggling prevention, immigration control, police searches for suspects, as well as cross border crime and terrorism prevention. Under a newly developed single cohesive concept, related threats will be managed as risks tailored to the specific situational needs of individual border crossing points.

TRESSPASS will:

(1) Develop a single cohesive risk-based tool to be implemented in the overall border management concept.
(2) Apply an ethics and data protection "by design" approach.
(3) Increase passenger trust in risk management model and border control sensitivity analysis and optimisation.
(4) Develop three pivoting pilot demonstrators.
(5) Demonstrate the validity of the single cohesive risk-based border management concept by using red teaming and simulations.
(6) Prepare for the further development of this concept beyond this project by linking to other known risk-based border management projects (in- and outside EU, within EU research frameworks and on national levels), and describe how their results contribute to a single cohesive risk-based border management concept.

As described in TRESSPASS Deliverable D9.6, border checks are conceptualised as *"performing the access and egress control function based on the revelatory function with regard to the movement of persons and the goods they bring along with them (including the means of transport) at the external borders of the EU".*

1.2 Aim of this document

The aim of this report is to identify existing legal boundaries to the implementation of risk-based border management approaches as well as to provide inputs for refining the proposed TRESSPASS concept according to current legal standards, thus allowing it to be developed in full compliance with EU legislation.

We present a review of the EU's current legal framework regulating checks on travellers and goods at the frontiers, with a particular focus on its most recent developments and specific regulatory aspects pertaining to the TRESSPASS pilot use cases.

This document does not aim to present answers to all possible legal and regulatory questions that might arise when implementing the TRESSPASS concept into practice. As noted in the TRESSPASS Deliverable D9.6, *"with regard to public policy, internal security and international relations, we are dealing […] with "indeterminate legal concepts" that cannot be read as continuous with the national legal concepts. They allow a relatively broad interpretation, specific to the legal and socio-political context of the Member States."*

This document does not constitute and can be no substitute for legal counsel. Its content has been created by the authors with project consortium inputs and does not constitute a statement on behalf of the European Commission.

1.3 Input to / Output from this document

- **Inputs** to this report have been conceptual discussions and feedback of partners from Work Packages 1, 2, and 9.
- **Output** from this report will be used as a reference in a variety of tasks and contribute to the high-level definition of the TRESSPASS risk-based border management concept.

2 METHODOLOGY

In order to gather relevant legislation documents, a systematic literature review with the PRISMA [1] statement (see 2.1) in the EUR-Lex database [2] was conducted initially. Two complementary search methods were then applied, namely the use of EUR-Lex summaries (see 2.2) and search engine searches (see 2.3). Selected documents were then added based on consortium partner inputs. The findings of this review are presented in chapter 3.

2.1 PRISMA method

PRISMA is short for **P**referred **R**eporting **I**tems for **S**ystematic **R**eviews and **M**eta-**A**nalyses and consists of a 27-item checklist aimed at improving the reporting of systematic literature reviews (Liberati et al. 2009, Moher et al. 2009).

A systematic review in general *"attempts to collate all empirical evidence that fits pre-specified eligibility criteria to answer a specific research question. It uses explicit, systematic methods that are selected with a view to minimizing bias, thus providing reliable findings from which conclusions can be drawn and decisions made"* (Liberati et al. 2009, p. 2). There are four main characteristics of a systematic literature review (p. 2):

- a clearly stated set of objectives with an explicit, reproducible methodology
- a systematic search that attempts to identify all studies that would meet the eligibility criteria
- an assessment of the validity of the findings of the included studies
- systematic presentation, and synthesis, of the characteristics and findings of the included studies

For the PRISMA method, three process steps can be identified: As a first step, review parameters have to be defined. Second, the literature (in this case the legislation documents) is gathered and assessed for their relevance to the review. The third step entails analysing the documents and then reporting the findings. A detailed checklist guides the literature review process with the PRISMA method[3].

Each of these steps will be described in more detail in the following sections.

2.1.1 Step 1: Definition of review parameters

Key research questions: The following key guiding questions related to the two main functions of border checks ('access and egress control function' and 'revelatory function', see TRESSPASS Deliverable D9.6) helped structure the legal framework review:

- What kind of passenger data is allowed to be processed?
- Is it legal to store passenger data over a certain period of time, within the EU for example? If so, how long can passenger data be stored?
- What possibilities exist for countries to share passenger data?

[1] For more information see: http://prisma-statement.org/

[2] For more information see: https://eur-lex.europa.eu/homepage.html

[3] Available for download here: http://prisma-statement.org/prismastatement/Checklist.aspx

- What possibilities exist to receive passenger data from individuals approaching land borders?
- What are the current rights and obligations of border and customs authorities in the EU regarding checks of travellers and goods?
- What are likely future changes to the rights and obligations of border and customs authorities in the EU regarding checks of travellers and goods?

Literature sources: As outlined above, this document focuses on gathering legislation documents in order to present an overview of the EU's legal and regulatory framework regulating checks on travellers and goods at the frontiers. To this end, this review was restricted to the collection of legislative and regulatory documents from the EUR-Lex database. Table 1 indicates the categories of literature sources that were used for the literature review as well as their descriptions.

TABLE 1: LITERATURE SOURCES AND DESCRIPTIONS

Literature source	Description
Treaties	The EU treaties are binding agreements between EU member countries (EUR-Lex: Treaties currently in force). They set out EU objectives, rules for EU institutions, how decisions are made and the relationship between the EU and its member countries. Every action taken by the EU is founded on treaties.
International agreements	International agreements are the result of a consensus between the EU on the one hand and a non-EU country or third-party organisation on the other hand (EUR-Lex: International agreements and the EU's external competences). These agreements create **rights and obligations** for both the EU institutions and EU countries. They become part of EU law on the date of their entry into force or on another specified date. Legally, international agreements are **secondary** conventions and agreements and must therefore comply with the founding Treaties of the EU. However, they have greater value than 'unilateral' secondary acts, i.e. acts adopted unilaterally by the EU institutions (regulations, directives, decisions, etc.).
Legal acts	EU law is divided into 'primary' and 'secondary' legislation. The treaties (primary legislation) are the basis or ground rules for all EU action (EU: EU law). Secondary legislation – which includes regulations, directives and decisions – are derived from the principles and objectives set out in the treaties. Legislation includes (EUR-Lex: Legal acts): › **binding** legal instruments (regulations, directives and decisions) › **non-binding** instruments (resolutions, opinions) › **other** instruments (EU institutions' internal regulations, EU action programmes, etc.)
Complementary legislation	See legal acts

Preparatory acts and working documents	Documents used to prepare EU legislation, produced during the various stages of the legislative and budgetary process (EUR-Lex: Preparatory documents). Includes COM and JOIN documents / SEC or SWD documents[4].
National transposition measures	Measures taken by member states to incorporate an EU legal act into national law (EUR-Lex: National transposition).
National case law	Case law on national level
Official Journal C series	The Official Journal of the European Union (OJ) is the main source of EUR-Lex content (EUR-Lex: Access to the Official Journal). It is published daily in the official EU languages. It is the official compendium of all EU legal acts. There are 2 series: › **L (legislation)** › **C (information and notices).**
EFTA documents	This collection covers the full text of acts adopted by the EFTA institutions (Surveillance Authority, Standing Committee, Court) and published in the Official Journal from 1994 onwards (EUR-Lex: EFTA documents).

Time frame: The time frame constituted of documents published since 2007, the year of the signing of the Treaty of Lisbon (EU 2007/C 306/01), which set the legal basis for the development of an EU integrated border management policy.

Languages: Systematic document collection and analysis activities focused on publications available in English. In case documents were only available in national languages of consortium members (mainly Dutch, Greek, and Polish), they were translated and the translations approved by consortium members from the respective countries.

Themes: The literature search was based on three key themes (listed in Table 2). More detailed information about the search strings can be found in the Annex 0.

[4] **COM**: Proposals and other acts adopted in the framework of a legislative procedure and further communications, recommendations, reports, white papers, green papers.

JOIN: Joint proposals, communications, reports, white papers and green papers adopted by the Commission and the High Representative.

SWD: Staff and joint staff working documents (impact assessments, summaries of impact assessments, staff working papers). Staff working documents had the identifier SEC prior to 2012 (now used only for internal documents of the European Commission, which are not published on EUR-Lex). SWD documents are published in one language, apart from the summaries of impact assessments, which are published in all the official languages of the EU.

For more information see: https://eur-lex.europa.eu/content/help/faq/intro.html#help5

TABLE 2: KEY THEMES COVERED BY THE PRISMA LITERATURE REVIEW

Themes	Relevant topics
Risk-based border control	› Data-driven risk analysis carried out in advance to the travellers' arrival at BCPs › Behaviour detection and al analysis of travellers conducted at BCPs
Multi-agency cooperation	› Cooperation between different agencies › Cooperation between different EU countries › Cooperation with neighbouring/third-countries
Current and future technologies	› Sensors and data gathering › Data processing and analytics › Data visualisation and reporting

2.1.2 Step 2: Literature collection and evaluation

Eligibility criteria: Only publications from 2007 to present were taken into account. Then, only publications concerning countries within the EU were considered relevant. For analytical and practical reasons, and as the searches were conducted with English search strings, the full publication had to be in English. We removed off-topic publications, such as for example: "Council Regulation (EC) No 40/2008 of 16 January 2008 fixing for 2008 the fishing opportunities and associated conditions for certain fish stocks and groups of fish stocks, applicable in Community waters and, for Community vessels, in waters where catch limitations are required".

Number of publications at different stages of assessment: The number of documents found after the search in the EUR-Lex database was 295. From these, five were out of our date range and 12 not in force. After removing these documents 278 remained. We then excluded off-topic documents, which left us with 143 documents.

After assessing the titles of the remaining documents from the PRISMA search method, we found that the search did not cover all relevant publications of topics of interest[5]. For this reason, we used two complementary approaches:

- We evaluated summaries provided by the EUR-Lex (EUR-Lex: Summaries of EU Legislation), which then led us via links to the respective legislative documents and additional information.
- We also conducted search engine searches for additional missing information. These methods are described in the following.

2.2 EUR-Lex summaries

The advantage of this method is that the summaries contain the most important regulatory information and, additionally, link to the respective regulations. Moreover, the summaries are ordered by topics and sub-topics.

[5] Step 3 of the PRISMA method will therefore not be described here as we did not end up coding the literature findings.

The number of summaries that the website contains is in the thousands. The number of summaries after choosing only relevant topics (customs, human rights, information security, institutional affairs, justice & freedom, security, and transport) was 695 summaries.

Three rounds of filtering were applied to the summaries: a first round based on the title of the summaries (documents left: 276) and a second one based on an examination of the summaries' full text (documents left: 97). In a last round of filtering, we then took into account the regulations for these summaries and were finally left with 27 summaries, which were our starting point for the report. In the course of writing this report, more regulations and corresponding summaries were taken into account where considered relevant.

Eligibility criteria: We did not define a time period for this search to maximise completeness. Additionally, summaries were only available on an EU level.

Theme-based analysis and coding of literature: Eligible summaries were classified and coded according to their relevance to four key themes (listed in Table 3).

TABLE 3: EUR-LEX SUMMARIES - THEMES AND RELEVANT TOPICS

Themes[6]	Relevant topics
Privacy and data protection	› General data protection rules › More specific data protection documents
Border control and management	› Schengen Borders Code › Internal borders › External borders
Information exchange and operational cooperation	› EU information systems › EU agencies
European agenda on security	› Outlook regarding external border control

2.3 Search engine searches

As the EUR-Lex summaries did not cover all relevant topics mentioned in the TRESSPASS proposal, we additionally conducted online searches using the 'Google' online search engine. The following list gives examples of online searches:

- EU border control
- ETIAS
- EIXM
- GDPR guide
- EU factsheets
- Etc.

2.3.1 Step 3: Literature analysis and findings report

The findings from the EUR-Lex summaries and the search engine searches were summarised and integrated into the legal framework review, which is presented in chapter 3. EU law texts behind the EUR-Lex summaries are mostly regulations and directives[7]. The general structure

[6] Information about the pilot countries was sent to us by the respective end-users.

[7] Regulations are *"binding legislative acts"* which must be applied across the EU. Directives, on the other hand, are *"legislative act[s] that set[..] out a goal that all EU countries must achieve. However, it is up*

of chapter 3 is hence that a regulation (or directive) is presented at the beginning of a paragraph. Then, a summary of the regulation follows in order to get a brief overview about what the regulation constitutes of[8]. Here, we also added which article is described. Lastly, more detailed information follows that is not mentioned in the summary but still was thought to be interesting for this report. Again, we also indicated articles, which all reference to the regulation (or directive) that was mentioned in the beginning of the paragraph.

Please be aware that larger text sections directly copied from a source are marked by a square around the text as follows[9]:

Personal data and data processing

Under the regulation, and for the purpose for which they were collected, personal data must be [Article 4]:

- processed **fairly and lawfully**;
- for specified, explicit and **legitimate purposes** and not further processed in a way incompatible with those purposes;
- **adequate**, relevant and not excessive;
- **accurate and up to date**;
- kept in a form which identifies the subject no longer than necessary.
- Further processing of personal data for historical, statistical or scientific purposes is permitted if there are appropriate safeguards about anonymity.
- Personal data may be processed only if it is [Article 5]:
  - necessary for a task carried out in the **public interest**;
  - in compliance with a **legal obligation**;
  - a case where unambiguous **consent** has been given;
  - to protect the **vital interests** of the data subject.

Information from EUR-Lex summaries and the respective legislative instruments were enriched with information from search engine searches.

to the individual countries to devise their own laws on how to reach these goals" (EU: Regulations, Directives and other acts). For more information see: https://europa.eu/european-union/eu-law/legal-acts_en

[8] There are cases where no summary is available. If this is the case, this step is skipped.

[9] Text is mainly copied directly either from EUR-Lex summaries or regulations etc. if the wording itself is important.

3 OVERVIEW OF LEGAL AND REGULATORY FRAMEWORK

The findings of the literature search are divided into five main topics: privacy and data protection (see 3.1), border control and management (see 3.2) information exchange and operational cooperation (see 3.2.3.4), European agenda on security (3.4), as well as pilot cases (see 3.5). If you do not want to engage in reading the comprehensive overview, please skip directly to chapter 4, which summarises the findings and discusses implications for the TRESSPASS risk-based border management concept.

3.1 Privacy and data protection

Citizens in the European Union have the fundamental right to the protection of their personal data (EC: Data protection in the EU) and that right is upheld in specific regulatory documents addressing the processing of personal data by Union institutions, police and criminal justice authorities, as well as further organizations and entities. In 2016, the European Commission adopted the Data Protection Reform to make sure that Europe meets the data protection requirements of the digital age (EC: Protection of personal data)[10]. The reform contained a regulation (directly applicable as of May 25th 2018 in all EU Member States) and a directive (to be implemented in national laws).

The following sections describe each of the following legislative documents in more detail:

- Regulation (EU) 2018/1725[11]: Processing of personal data by the Union institutions, bodies, offices and agencies and of the free movement of such data
- Regulation (EU) 2016/679 or General Data Protection Regulation[12]: Processing of personal data
- Directive (EU) 2016/680[13]: Processing of personal data by police and criminal justice authorities

[10] For more information and a more detailed description on the new European data protection rules see also Lambert (2017).

[11] **Regulation (EU) 2018/1725** of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

[12] **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) (Text with EEA relevance)

[13] **Directive (EU) 2016/680** 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 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

3.1.1 Processing of personal data by Union institutions, bodies, offices and agencies

Regulation (EU) 2018/1725 [14] applies to the processing of personal data by all Union institutions and bodies (including offices and agencies).

General provisions: Personal data constitutes (Article 2):

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

General principles: Under the regulation, and for the purpose for which they were collected, personal data must be (Article 4):

- processed lawfully, fairly and in a transparent manner
- for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate and up to date;
- kept in a form which identifies the subject no longer than necessary;
- processed so that security of the data is ensured.

Processing is only lawful if it is necessary for the performance of a task (in the public interest); for compliance with a legal obligation; for the performance of a contract; or if the data subject has given consent (see also Article 7-8); or it is necessary to protect the data subject's vital interests (Article 5). If the processing is not based on the original purpose anymore, consent from the data subjects' is necessary (Article 6). However, there are some exceptions. Personal data can only be transmitted to recipients established in the EU other than Union institutions and bodies if the transmission is necessary for the performance of a task or for a specific purpose in the public interest (Article 9). Special categories of personal data (e.g. genetic, biometric and criminal offences data) underlie additional restrictions (Article 10-11).

Rights of the data subject: Data subjects have the right to receive transparent information about the processing and the right to have access to their personal data (Article 15-17). They also have the right to be forgotten (Article 19), the right to restriction of processing (Article 20), the right to data portability (Article 22), the right to object (Article 23), and the right not to be subject to a decision based exclusively on automated processing (Article 24).

Controller and processor: Data protection has to be by design and by default (Article 27). Records of processing activities have to be created and maintained (Article 31).

Transfers of personal data to third countries or international organisations: The transfer of personal data to a third country or international organisation can only be made based on an adequacy decision (Article 47), if appropriate safeguards are in place (Article 48) or for some specific situations (Article 50).

[14] **Regulation (EU) 2018/1725** of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

European Data Protection Supervisor: The European Data Protection Supervisor is established in this regulation and is responsible to ensure that Union institutions and bodies respect the data protection rights of the data subjects (Article 52).

3.1.2 Processing of personal data – the General Data Protection Regulation[15]

Regulation (EU) 2016/679[16] (also called General Data Protection Regulation, GDPR[17]) applies to the processing of personal data and the free movement of such data and is usually applicable to personal data processed for border crossing purposes. As mentioned earlier, the directive is part of the Data Protection Reform package. The regulation gives citizens more control over their personal data by expanding and adding rights. The key points of the regulation are summarized below, indicating the respective regulation articles where applicable (EU: Protection of personal data (from 2018) (Summary)). The subsequent text then provides details on further relevant articles of the Regulation.

Citizens' rights

The GDPR strengthens existing rights, provides for new rights and gives citizens more control over their personal data. These include:

- **easier access to their data** [Article 15]— including providing more information on how that data is processed and ensuring that that information is available in a clear and understandable way;
- **a new right to data portability** [Article 20] — making it easier to transmit personal data between service providers;
- a clearer **right to erasure ('right to be forgotten')** [Article 17] — when an individual no longer wants their data processed and there is no legitimate reason to keep it, the data will be deleted;
- **right to know when their personal data has been hacked** [Article 33] — companies and organisations will have to inform individuals promptly of serious data breaches. They will also have to notify the relevant data protection supervisory authority.

Rules for businesses

The GDPR is designed to create business opportunities and stimulate innovation through a number of steps including:

- **a single set of EU-wide rules** — a single EU-wide law for data protection is estimated to make savings of €2.3 billion per year;
- **a data protection officer** [Articles 37, 38, 39], responsible for data protection, will be designated by public authorities and by businesses which process data on a large scale;
- **one-stop-shop** [Recital 127] — businesses only have to deal with one single supervisory authority (in the EU country in which they are mainly based);
- **EU rules for non-EU companies** — companies based outside the EU must apply the same rules when offering services or goods, or monitoring behaviour of individuals within the EU;

[15] For more information on ethical and legal criteria for research see TRESSPASS Deliverable D9.2

[16] **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) (Text with EEA relevance)

[17] For more information see: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

- **innovation-friendly rules** — a guarantee that data protection safeguards are built into products and services from the earliest stage of development (data protection by design and by default) [Article 25];
- **privacy-friendly techniques** such as **pseudonymisation** (when identifying fields within a data record are replaced by one or more artificial identifiers) and **encryption** (when data is coded in such a way that only authorised parties can read it) [Recitals 26, 28, Articles 4, 25, 32];
- **removal of notifications** — the new data protection rules will scrap most notification obligations and the costs associated with these. One of the aims of the data protection regulation is to remove obstacles to free flow of personal data within the EU. This will make it easier for businesses to expand;
- **impact assessments** [Articles 35, 36] — businesses will have to carry out impact assessments when data processing may result in a high risk for the rights and freedoms of individuals;
- **record-keeping** [Article 30] — SMEs (small and medium-sized enterprises) are not required to keep records of processing activities, unless the processing is regular or likely to result in a risk to the rights and freedoms of the person whose data is being processed.

General provisions: The regulation applies when personal data is wholly or partly processed by automated means, or if the data is part of a filing system or intended to form part of a filing system (Article 2). It does not apply to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and threats to public security. It does also apply when the processing is not conducted within the Union but the processor is located in the Union (Article 3). It applies to processing in the case of offering goods or services and in case of monitoring data subjects' behaviour (if it takes place in the Union). In the Regulation, personal data and processing are defined as follows (Article 4):

> Personal data: *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*
>
> Processing: *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."*

Principles: The GDPR sets out six principles relating to the processing of personal data, compliance with which must be **demonstrable** (accountability) (Article 5):

- **Lawfulness, fairness and transparency**: Personal data has to be processed lawfully (see also below), fairly and transparently. This means that during the data collection you need to be transparent about what data you collect and why you are collecting it.
- **Purpose limitation**: Personal data has to be collected for specific purposes. This means that you should clearly state your purpose. It can be further processed, however, for archiving purposes in the public interest, scientific or historical research purposes or statistical is allowed.
- **Data minimisation**: Personal data has to be relevant and limited to what is necessary. This means that you should only collect data that is really needed for your purpose.
- **Accuracy**: Personal data has to be accurate and up-to-date; if not the data have to be erased or rectified.

- **Storage limitation**: Personal data has to be deleted after it is no longer in use. It can be stored longer, however, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- **Integrity and confidentiality**: Personal data has to be processed so that the security of it is ensured. This means that you have to protect the data against unauthorized or unlawful processing, against accidental loss, and destruction or damage.

At least one of the following six specific grounds has to apply in order for the processing to be lawful (ICO: Lawful basis for processing) (Article 6, Recital 40):

- **Consent:** The data subject has to give his/her consent to the processing, which can however be withdrawn at any time. A consent is also needed by the holder of parental responsibility of a child that is younger than 16 years (also Articles 7, 8).
- **Contract:** The processing is necessary for a contract that you have with the individual.
- **Legal obligation:** The processing is necessary for you to comply with legal obligations.
- **Vital interests:** The processing is necessary to protect the life of the data subject or of another person.
- **Public task:** The processing is necessary for you to carry out the performance of a task or for your official functions.
- **Legitimate interest:** The processing is necessary for your legitimate interests.

The processing of special categories of personal data such as race and ethnic origin; political opinions and religious/philosophical beliefs; genetic, biometric and health data; data about the data subjects' sex life or sexual orientation is generally not allowed (Article 9). However, the processing is allowed if, for example, the data subject has given explicit consent to do so; if it is necessary to protect lives; if the data is made public by the data subject or if it is necessary for the public interest. The processing of personal data relating to criminal conviction and offences has to be conducted by official authority (Article 10). Genetic, biometric and health data are specifically defined in the GDPR as follows (Article 4):

> *genetic data: "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question"*
>
> *biometric data: "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"*
>
> *data concerning health: "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"*

Rights of the data subject: Any information about the processing of the data has to be provided to the data subjects in a transparent and easily accessible form (in writing or other means) (Article 12). The information should include: identity and contact details of the processor, the data protection officer, the purposes of the processing, the recipients of the data if there are any, if there is a transfer of the data (Article 13). Similarly, when the data has not been obtained from the data subject itself, the previously mentioned information has to be provided and additionally the period for which the data is stored, that the data subject can access, rectify or erase their data; that the data subject has the right to lodge a complaint; from which source the data originates (Article 14). The data subject generally has the right to access the data about him/her (Article 15); the right to rectification of inaccurate data

concerning him/her (Article 16); the right to erasure or the right to be forgotten where the data is no longer necessary for the purpose or the data subject withdraws his/her consent (Article 17), the right to the restriction of processing (Articles 18, 19); the right to data portability meaning that the data subject receives his/her personal data (Article 20); the right to object at any time to the processing (Article 21); and the right not to be subject to a decision that is based only on automated processing (Article 22). Member States are allowed to restrict some of the rights in respect to fundamental rights by way of a legislative measure (Article 23).

Controller and processor: The controller is defined as follows (Article 4):

> *"[a] natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law"*.

There also exist joint controllers in case two or more controllers jointly determine the purposes and means of processing (Article 26). The controller has to have appropriate technical and organisational measures in place, such as pseudonymisation, that ensure data-protection principles, such as data minimisation (also known as data protection by design and by default) (Articles 24, 25). This also applies for the period of their storage and accessibility.

The processor is *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"* (Article 4). Where the processor carries out the processing on behalf of the controller (a contract or other legal act is needed), he/she also has to have appropriate technical and organisational measures (Article 28). The processor or any other person that acts on behalf of the controller is not allowed to process data except the controller tells them to do so or it is required by Union or Member State law (Article 29).

Each controller has to have a record of his/her processing activities (Article 30). The controller and processor have to cooperate with the supervisory authority whilst carrying out a task (Article 31). Controller and processors have to implement security safeguards for processing: pseudonymisation and encryption of personal data; confidentiality, integrity, availability and resilience; the ability to restore data in case of a technical/physical incident; a process for a regular testing and evaluating the technical and organisational measures' effectiveness (Article 32). In case of a data breach, the controller has to notify the supervisory authority unless it is not likely that the breach will result in a risk to the rights of natural persons (Article 33). If it is likely to have a high risk, the controller has to communicate the breach to the data subject (Article 34).

Before the processing and especially in the context of new technologies, the controller has to carry out an assessment of the data protection by seeking the advice of the data protection officer (Articles 35, 36). The controller and processor have to designate a data protection officer (also Articles 28, 39) where the processing is done by a public authority/body; where the processing requires regular and systematic monitoring of data subjects; where special categories of data and data relating to criminal offences is conducted (Article 37).

Transfers of personal data to third countries or international organisations: Generally, the transfer of personal data that has or will undergo processing after a transfer to a third country/international organisation can only take place if the conditions in this chapter are met (including if they are further transferred) (Article 44). The transfer can take place where the

Commission has approved of the receiving country or international organisation by means of implementing act – no specific authorisation is required (Article 45). The European Commission has so far recognised Andorra[18], Argentina[19], Canada[20], Faroe Islands[21], Israel[22], Guernsey[23], Isle of Man[24], Jersey[25], New Zealand[26], Switzerland[27], Uruguay[28] and the United States of America[29]. If this authorisation by the Commission is not present, data can only be transferred with the appropriate safeguards such as by a legally binding instrument, binding

[18] **2010/625/EU:** Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (notified under document C(2010) 7084) Text with EEA relevance

[19] **2003/490/EC:** Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (Text with EEA relevance)

[20] **2002/2/EC:** Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)

[21] **2010/146/:** Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data (notified under document C(2010) 1130) (Text with EEA relevance)

[22] **2011/61/EU:** Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332) Text with EEA relevance

[23] **2003/821/EC:** Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (Text with EEA relevance) (notified under document number C(2003) 4309)

[24] **2004/411/EC:** Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man

[25] **2008/393/EC:** Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746) (Text with EEA relevance)

[26] **2013/65/EU:** Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557) Text with EEA relevance

[27] **2000/518/EC:** Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance.)

[28] **2012/484/EU:** Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012) 5704) Text with EEA relevance

[29] **Commission Implementing Decision (EU) 2016/1250** of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance)

corporate rules (also Article 47), standard data protection clauses adopted by the Commission or by a supervisory authority (also Article 50), an approved code of conduct or by an approved certification mechanism (Article 46). If none of these apply, the transfer of personal data to a third country can only take place if the data subject has given explicit consent; the transfer is necessary for the performance or conclusion of a contract; the transfer is necessary for important reasons of public interest; the transfer is necessary for the establishment or defence of legal claims; the transfer is necessary for protecting lives; or the transfer is made from a register (Article 49).

Independent supervisory authorities: Each Member State has to establish one or more independent public authorities ('supervisory authority') that independently monitor the application of this regulation (Articles 51-56). Supervisory authorities also promote public awareness, advice, handle complaints, and conduct investigations (Articles 57, 58). They have to write an annual report on their activities (Article 59).

Cooperation and consistency: The lead supervisory authority has to cooperate with other supervisory authorities (Article 60). Supervisory authorities have to cooperate with each other and the Commission (Article 63). They also have to provide each other with information and mutual assistance (Article 61) as well as conduct joint operations where appropriate (Article 62). The European Data Protection Board, which comprises the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, is established as a body of the Union (Article 68). It also acts independently (Article 69). Its tasks are to monitor the correct application of the Regulation, give advice, and issue guidelines (Article 70). The Board also has to write an annual report to the Union (Article 71).

Remedies, liability and penalties: Data subjects have the right to lodge a complaint with the supervisory authority in their Member State (Article 77), a right to an effective judicial remedy against a supervisory authority (Article 78), and a right to an effective judicial remedy against a controller or processor (Article 79). Data subjects also have a right to compensation and liability in case of material or non-material damage (Article 82).

3.1.3 Processing of personal data by police and criminal justice authorities

Directive (EU) 2016/680[30] (also called Data Protection Law Enforcement Directive or Police Data Protection Directive, PDPD) applies to the processing of personal data by police and criminal justice authorities. As mentioned earlier, the directive is part of the Data Protection Reform package, however, it is not directly applicable and Member States are obliged to implement it in their national laws. It lays down the rules for the protection of personal data of victims, witnesses and suspects. The key points of the Directive are summarized below (EU: Protecting personal data when being used by police and criminal justice authorities (from 2018) (Summary)). The subsequent text gives more detail about the respective articles of the directive.

Data

The directive requires that the data collected by law enforcement authorities are [Article 4]:

- processed **lawfully and fairly**;

[30] **Directive (EU) 2016/680** protecting individuals with regard to the processing of their personal data by police and criminal justice authorities, and on the free movement of such data

- collected for **specified, explicit and legitimate purposes** and processed only in line with these purposes;
- **adequate, relevant and not excessive** in relation to the purpose in which they are processed;
- **accurate and updated** where necessary;
- kept in a form which allows identification of the individual for **no longer than is necessary** for the purpose of the processing;
- **appropriately secured**, including protection against unauthorised or unlawful processing.

Time limits

EU countries must establish time limits for erasing the personal data or for a regular **review** of the need to store such data [Article 5].

Individuals concerned ('data subjects')

The directive requires that the law enforcement authorities make a clear distinction between the data of different categories of persons including [Article 6]:

- those for whom there are **serious grounds** to believe they have committed or are about to commit a criminal offence;
- those who have been **convicted of a criminal offence**;
- **victims of criminal offences** or persons whom it is reasonably believed could be victims of criminal offences;
- those who **are parties to a criminal offence**, including potential witnesses.

Information available or provided to data subject

Individuals have the right to have certain information made available to them by the law enforcement (i.e. data protection) authorities including [Article 13]:

- the **name and contact details of the competent authority** which decides the purpose and means of the data processing;
- why their data is being processed;
- the right to **launch a complaint** with a supervisory authority and the contact details of the authority;
- the existence of the right to request **access to and correction or deletion of their personal data** as well as the right to restrict **processing of their personal data**.

Security

National authorities must take technical and organisational measures to ensure a level of security for personal data that is appropriate to the risk. Where data processing is automated, a number of measures must be put in place, including [Article 29]:

- denying unauthorised persons **access to equipment** used for processing;
- preventing the unauthorised reading, copying, changing or removal of **data media**;
- preventing the **unauthorised input of personal data** and the unauthorised viewing, changing or deleting of **stored personal data**.

General provisions: The Directive applies when personal data is processed (wholly or partly automatically, (Article 2) by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences and the prevention of threats to public security (Article 1). The Competent authority is defined as (Article 3):

"(a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by

Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".

Principles[31]: Inaccurate, incomplete or no longer up-to-date personal data is not allowed to be transmitted or made available (Article 7). Processing of personal data is only allowed if it is necessary for the performance of a task (Article 8). The processing of special categories of personal data (racial/ethnic origin, political opinions, religious/philosophical beliefs, trade/union membership, genetic/biometric data[32], data concerning health/sex life/sexual orientation) is only allowed if it is strictly necessary and only if the vital interests of the person or other person is protected or if the data has been made public by the data subject (Article 10).

Rights of the data subject: Information has to be provided to the data subject in a concise, intelligible and easily accessible manner (Article 12). The following information has to be provided: identity/contact details of controller/data protection officer (DPO); purpose/legal basis of processing; the right to lodge a complaint; the right to access (also Articles 14, 15) and rectification/erasure/restriction (also Article 16); data storage period; and categories of recipients (Article 13).

Controller and processor: Member State have to provide for the controller taking into account the nature/scope/context/purposes of processing (Article 19) and to implement appropriate technical/organisational measures (e.g. pseudonymisation) (Articles 20, 29-31). Joint controllers are allowed (Article 21). Processors have to be established where processing is carried out on behalf of a controller (Articles 22, 23). Controllers have to maintain records of processing activities (Article 24) and logs (Article 25).

Transfers of personal data to third countries or international organisations: Transfer by competent authorities to a third country/international organisation can only take place if: the transfer is necessary for the purposes of prevention, investigation, detection or prosecution of criminal offences; the data are transferred to a controller; and the Commission has adopted an adequacy decision (also Article 36) or appropriate safeguards exits (also Article 37) or derogations for specific situations apply (also Article 38) (Article 35).

Independent supervisory authorities: Each Member State has to provide for one or more independent public authorities that monitor the data protection (Articles 41-49).

Cooperation: Supervisory authorities of each Member State have to cooperate with each other (Articles 50, 51).

3.2 Border control and management

Within the Schengen area, EU citizens and legal residents are able to cross borders without being subjected to controls, regulated in the Schengen Borders Code. Rules for controls at

[31] Please be aware that since most of these articles are similar to the General Data Protection Regulation, the articles do not provide many details here. For more information see 3.1.2.

[32] For a definition see Article 3 of Directive (EU) 2016/680 or Article 4 of Regulation (EU) 2016/679 (GDPR), cited above (3.1.2)

external Schengen and EU borders respectively are discussed in the subsequent section of this chapter.

3.2.1 Schengen Borders Code

Border control of the Schengen area is managed by Regulation (EU) 2016/399[33], which is also called the Schengen Borders Code (SBC) (EU: Rules on crossing EU borders (Summary)). The Schengen area today covers 26 countries: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein (non-EU), Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Switzerland (non-EU). The Code defines the rules for the absence of border controls at internal borders of Member States and to any person that crosses the Schengen area's external borders (Article 1). Bulgaria, Cyprus, Croatia and Romania, though not yet full members of the Schengen area, also have to follow the rules concerning the crossing of external borders.

3.2.2 Checks on people

Depending on where a traveller comes from or goes to, they are subject to certain controls at the border crossing point. As will be discussed in the next two subsections, the rules for person checks at internal Schengen borders differ from the ones for external borders.

3.2.2.1 Internal borders

As a general rule, any person can cross internal borders of the Schengen area without checks being carried out on them – irrespective of the person's nationality (Articles 3, 22) (EC: Schengen Area; EU: Rules on crossing EU borders (Summary)). Internal borders include land borders (also river and lake borders), airports for internal flights, as well as sea, river and lake ports for ferry connections (Article 2). However, national police authorities can carry out police checks that are based on specific rules and limitations, i.e. checks must not be equivalent to border checks (e.g. spot checks and not systematic checks) (Article 23).

Temporary reintroduction of internal border control

The Schengen Borders Code allows the temporary reintroduction of internal border controls for a limited period of time (Chapter II) (EU: Rules on crossing EU borders (Summary); EC: Temporary Reintroduction of Border Control). This may be the case if there is a serious threat to public policy or internal security (Article 25, Recital 25):

- **Foreseeable cases/events:** The reintroduction of internal border controls can last up to 30 days for foreseeable cases/events (e.g. sports event). It can also be prolonged but cannot be longer than six months (Articles 25, 26).
- **Cases requiring immediate action:** The reintroduction of internal border controls can last for 10 days for cases in the event of a threat. It can also be prolonged but cannot be longer than two months (Article 28).

[33] **Regulation (EU) 2016/399** of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification)

- **Cases where exceptional circumstances put the overall functioning of the Schengen area at risk:** The reintroduction of internal border controls can take place in exceptional circumstances *"where the overall functioning of the Schengen area is put at risk as a result of persistent serious deficiencies relating to external border control, and insofar as those circumstances constitute a serious threat to public policy or internal security"*. This can last up to two years (Article 29, Recital 30).

Generally, the reintroduction of border control at the internal borders is an exception and should only be used as a last resort (Article 25, Recitals 21-23).

3.2.2.2 External borders

External borders include land borders (river and lake borders), sea borders and their airports, river ports, as well as sea and lake ports (Article 2, SBC). External borders are only allowed to be crossed at border crossing points (BCPs) (Article 5, SBC). Border checks are carried out on persons but may also be carried out on the person's means of transport and objects in possession (Article 8, SBC) (see 3.2.3). During the checks, persons have to show their travel documents, and may additionally be checked against national and European databases (Article 8, SBC) – e.g. the Visa Information System (VIS) (see 3.3.1.1) and Schengen Information System (SIS) (see 3.3.1.2). Travel documents have to be stamped upon entry and exit (Article 11, SBC). Specific rules for the various types of border and means of transport exist (Article 19/Annex VI, SBC). There also exist specific rules on certain categories of persons (Article 20/Annex VII, SBC).

The Schengen Borders Code[34] also determines that Member States should cooperate in executing border checks and are allowed to exchange information (Article 17, SBC). This is necessary to establish an effective and efficient border management at external EU borders which in turn should result in more secure borders and less cross-border crime (EC: European integrated border management).

The integrated border management (IBM)[35] has been established to reach exactly this. It also addresses migratory challenges and potential future threats (e.g. migrant smuggling, human trafficking, and terrorism). The rules for the integrated border management (IBM) are laid out in Regulation (EU) 2016/1624[36], which established a European Border and Coast Guard ('Frontex') as a means to apply the IBM. For more information on Frontex and the IBM see 3.3.2.1. Necessary travel documents and legal possibilities for crossing external borders are described in the following.

[34] **Regulation (EU) 2016/399** of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification)

[35] IBM guidelines: https://europa.eu/capacity4dev/file/21153/download?token=3lOSGDjf

[36] **Regulation (EU) 2016/1624** of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC

3.2.2.2.1 Visa policy

Regulation (EC) No 810/2009[37], also called Visa Code, regulates short stays in Schengen countries (EU: Visa Code; EC: Visa policy). Nationals of non-EU countries[38] need to be in possession of a *uniform Schengen visa*, which allows them to be in the countries a maximum of 90 days in any 180-day period (Article 2). Hence, if a visa has been issued, the person can travel to all 26 Member countries of the Schengen area. The uniform Schengen visa consists of two categories: *short-term visa* and *airport transit visa* (Schengen Visa Info: Schengen Visa Types & Validity). The short-term visa allows a person to stay in the Schengen area for the above-mentioned period. The airport transit visa allows a person to travel through the areas of EU airports (Article 3). The regulation also defines a list of third countries whose nationals need to have an airport transit visa when passing through airports of the Member States (Annex IV). There is also a list of countries for which this requirement is waived (Annex V). The regulation also defines the procedures and conditions for issuing visas.

To issue a visa, applicants have to provide amongst other things a photograph and their fingerprints (except children younger than 12 years) (Article 13). The data then has to be entered in the Visa Information System (VIS). For more information about the VIS, see 3.3.1.1. If the application is admissible, the visa gets a stamp (Article 20). Figure 3-1 shows the countries which do (purple) and do not (red) require short-stay visas to enter the Schengen area. The light blue countries represent Schengen States and the dark blue EU States not part of Schengen.

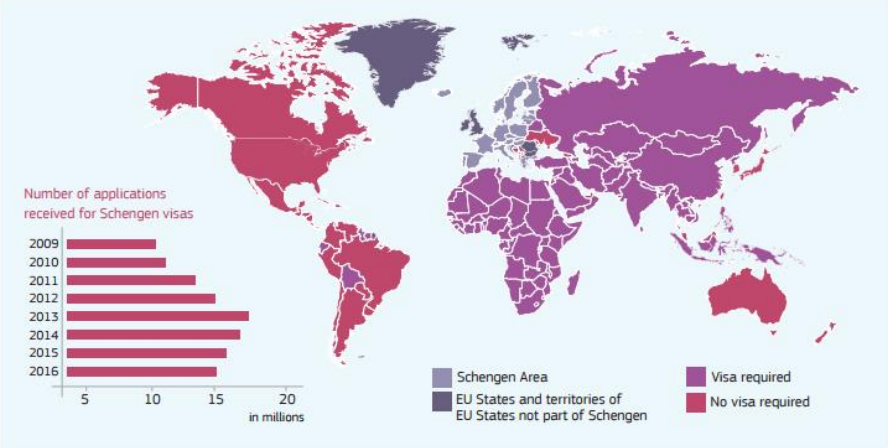

FIGURE 3-1 SCHENGEN VISA (EC: A STRONGER, MORE EFFICIENT AND SECURE EU VISA POLICY).

[37] **Regulation (EC) No 810/2009** of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code)

[38] Annex I of **Council Regulation (EC) No 539/2001** of 15 March 2001 lists the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement

3.2.2.2.2 Local border traffic regime

Regulation (EC) No 1931/2006[39], also called Local Border Traffic Regime, regulates local border traffic at external land borders by allowing the implementation of bilateral agreements between neighbouring Member States so that border residents that frequently cross these borders have a special permit to do so (EU: Local border traffic at external land borders (Summary)). This topic is addressed further in the section on the pilot case Poland (3.5.2).

3.2.2.2.3 Legal immigration

The EU migration policy, which is currently under development, establishes a *"framework for legal migration, taking fully into account the importance of integration into host societies"* (EC: Legal migration and Integration). It covers the entry and residence conditions of various categories of immigrants. Ireland, Denmark and the United Kingdom are excluded from the directives listed in the following.

- **Family reunification**: The aim of Council Directive 2003/86/EC[40] is to set out common rules of law to regulate the admission and residence of family members of non-EU nationals (sponsors) legally residing in Member States, in order to protect the family unit and to facilitate the integration of non-EU nationals.

  Who can apply for family reunification? Non-EU nationals in possession of a residence permit valid for at least one year in an EU country who could apply for long-term residence (Article 3; EU: Family reunification (Summary)). Eligible for family reunification are the sponsors spouse and minor children of the couple, or of one member of the couple, including adopted children (Article 4). Furthermore, EU countries are free to authorise family reunification of first-degree ascendants (e.g. father and mother of the foreign national), unmarried children of age and unmarried partners. The family reunification directive does not apply to family members of EU citizens or non-EU nationals with refugee status or under a temporary form of protection (Article 3).

- **Long-term residents:** Directive 2003/109/EC[41] allows third-country nationals to obtain an *"EU long-term resident"* status after five years of legal and continuous residence in a Member State. It does not apply to third-country nationals who reside in a Member State for studies or vocational training; on the basis of temporary protection / a subsidiary form of protection or while applying for it; as refugees; only temporary as au pair or seasonal worker; or with a legal status governed by the Vienna Convention (Article 3).

  In order to obtain a long-term residence status, third-country nationals have to prove that they have resources sufficient to maintain himself/herself as well as the dependent family members as well as sickness insurance (Article 5). The amendment to this Directive,

[39] **Regulation (EC) No 1931/2006** of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention

[40] **Council Directive 2003/86/EC** of 22 September 2003 on the right to family reunification

[41] **Council Directive 2003/109/EC** of 25 November 2003 concerning the status of third-country nationals who are long-term residents

Directive 2011/51/EU [42] extends the scope, including beneficiaries of international protection.

- **EU Blue Card**: The EU Blue Card, as per Council Directive 2009/50/EC[43] establishes the entry and residence conditions for highly-qualified non-EU nationals who wish to work in a highly-qualified job in an EU country (other than Denmark, Ireland and the United Kingdom), and for their families. In order to apply for a EU Blue Card, a valid work contract or job offer must be presented, proof of necessary qualifications, a valid travel document and / or visa as well as proof of health insurance (Article 5). Depending on the EU country which issues the EU Blue Card, it is valid per standard between one and four years, or for the duration of the work contract if it is shorter than the standard period (Article 7).

  EU Blue Card holders as well as their families can enter and stay in the EU country where the card was issued and pass through other EU countries. They enjoy the same rights as country nationals as far as working conditions, education, social security and freedom of association are concerned (Article 14). After 18 months of legal residence, obtaining visa to move to another EU country is facilitated for EU Blue Card holders (Article 18).

- **Single Permit**: This Directive 2011/98/EU[44] establishes a combined single residence and work permit for legally residing non-EU workers in an EU country. In addition, these workers covered by the directive should enjoy equal treatment provisions compared to nationals in that EU country. Included are non-EU nationals authorised to live or work in the EU, such as (Article 3; EU: Non-EU workers – easier residence and work formalities (Summary))

  - *"non-EU nationals seeking to be admitted to an EU country in order to stay and work,*
  - *non-EU nationals who are already resident and have access to the labour market or are already working in an EU country."*

  With the single permit, non-EU nationals have the right to work, stay and move freely in the issuing EU country (Article 11) as well as the same conditions as nationals regarding working conditions, education, recognition of qualifications, social security, access to goods and services etc. (Article 12)[45]. Not covered by the directive are non-EU nationals who have been granted EU long-term residence (as they are subject to other legislation) (Article 3).

[42] **Directive 2011/51/EU** of the European Parliament and of the Council of 11 May 2011 amending Council Directive 2003/109/EC to extend its scope to beneficiaries of international protection (Text with EEA relevance)

[43] **Council Directive 2009/50/EC** of 25 May 2009 on the conditions of entry and residence of third-country nationals for the purposes of highly qualified employment

[44] **Directive 2011/98/EU** of the European Parliament and of the Council of 13 December 2011 on a single application procedure for a single permit for third-country nationals to reside and work in the territory of a Member State and on a common set of rights for third-country workers legally residing in a Member State

[45] Specific criteria are set by the Directive, based on which EU countries are able to restrict equal treatment on certain issues such as access to education or training, or social security benefits (family benefits or housing) (Article 12).

- **Seasonal workers**: Directive 2014/36/EU[46] sets out the conditions for admission and stay of non-EU citizens admitted temporarily to carry out seasonal work, often in agriculture and tourism and includes the rights to ensure that these workers are not exploited. Considering the EU's ageing population and low birth rate, flexible policies are needed in order to manage migration flows. Thus, EU countries have agreed on a law on seasonal migration, which applies to non-EU workers who reside in a non-EU country and enter the EU for temporary work (Article 3).
- **Intra-Corporate Transferees**: The EU has standard rules to process the transfer applications of multinational companies assigning staff to another country. It has to be ensured that the people concerned are treated fairly during their stay in the EU. In this Directive 2014/66/EU[47], the terms and conditions are set that apply to third-country nationals and their families when they are transferred to work in the EU for more than 90 days. To the self-employed, students or people assigned by employment agencies it does not apply.

  With this directive, a mechanism is provided that allows the transferee to carry out his/her work in various EU countries without having to reapply for admission whenever he/she moves to another EU country, and family members can join (Article 19). In order to be admitted, transferees must have worked with their company for a certain time before the transfer, and provide a work contract as well as evidence that a transfer back is possible once the work assignment ends (Article 5).
- **Students and Researchers**: This Directive (EU) 2016/801[48] defines the EU rules on the conditions of entry and residence of non-EU nationals *"for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing"* (EC: Legal Migration Fitness Check – REFIT initiative). In order to apply for admission, candidates have to provide a valid travel document for the duration of the planned stay, evidence of sufficient resources to cover living costs and return travel costs, and health insurance (Article 7). Based on Directive 2011/98/EU (see "Single permit" in the above), researchers should have the same rights as EU citizens of the respective country (Article 22). Specific conditions apply for family members who want to join researchers (Article 26).

In 2013, a **"Fitness Check"** was launched to evaluate and assess the EU legal migration legislation in order to better adjust legal migration policy to the EU's economic and social needs and to combat labour exploitation (EC: Legal Migration Fitness Check – REFIT initiative). It covers the directives listed in the above. In 2018, the final process steps were undertaken, and the adoption of the report on the Fitness Check is foreseen.

[46] **Directive 2014/36/EU** of the European Parliament and of the Council of 26 February 2014 on the conditions of entry and stay of third-country nationals for the purpose of employment as seasonal workers

[47] **Directive 2014/66/EU** of the European Parliament and of the Council of 15 May 2014 on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer

[48] **Directive (EU) 2016/801** of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing (recast)

3.2.2.2.4 Illegal immigration

As regards illegal immigration, the EU adopted a legal framework in 2002 on smuggling, composed of Council Directive 2002/90/EC[49] defining the facilitation of unauthorised entry, transit and residence and a Framework Decision 2002/946/JHA[50] strengthening the penal framework for these offenses. In May 2015, the Commission published the EU Action Plan against Migrant Smuggling[51] setting out a series of steps to tackle this problem between 2015 and 2020.

The Directive specifies which actions are treated as infringements regarding the facilitation of illegal immigration, and thus which persons should be sanctioned (Article 1):

- *"any person who **intentionally assists** a person who is not a national of a Member State **to enter, or transit across, the territory of a Member State** in breach of the laws of the State concerned on the entry or transit of aliens;*
- *any person who, **for financial gain, intentionally assists** a person who is not a national of a Member State **to reside within the territory of a Member State** in breach of the laws of the State concerned on the residence of aliens."*

The Framework Decision addresses the penalties for such offenses, which can be supplemented by confiscation of the means of transport; prohibition on practising the occupational activity where the offence was committed and deportation (Article 1). Infringements committed for financial gain, as part of activities in a criminal organisation or if lives were endangered, can lead to a maximum prison sentence of at least eight years (Article 1). EU countries who have knowledge of infringements violating another EU country's law on foreigners have to communicate the information to the country concerned (Article 7).

[49] **Council Directive 2002/90/EC** of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence

[50] **2002/946/JHA:** Council framework Decision of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence

[51] **COM(2015) 285 final**: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU Action Plan against migrant smuggling (2015 - 2020)

3.2.2.2.5 Passenger rights[52]

Citizens in the EU are protected by passenger rights when traveling by air[53], rail[54], ship[55], bus or coach[56]. Commission Communication COM(2011) 898 final[57] specifies, that the goal is to have a *"common set of passenger rights guaranteed by law for the four transport modes"* and furthermore to allow *"necessary distinctions due to the specific characteristics of each mode and their markets, related to the industries […] and passengers to ensure proportionality"* (p. 3). The main aspects of passenger rights are *"non-discrimination; accurate, timely and accessible information; [and] immediate and proportionate assistance"* (p. 3).

3.2.3 Checks on goods and aviation and maritime security

When traveling to an EU country, there are restrictions, prohibitions and other provisions concerning potentially dangerous items (depending on travel modality) as well as goods and products, such as animals[58] or animal products[59], plants[60], foods, cash[61] etc. (EU: What can you take with you?). Also, conformance controls regarding provisions on exemptions for products subject to excise duties (alcohol, tobacco) are carried out by competent authorities. In the following, the relevant regulations for customs controls, the domain of aviation security, and maritime security, will be discussed.

---

[52] For more information see: https://europa.eu/youreurope/citizens/travel/passenger-rights/index_en.htm

[53] **Regulation (EC) No 261/2004** of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (Text with EEA relevance) - Commission Statement

[54] **Regulation (EC) No 1371/2007** of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations

[55] **Regulation (EU) No 1177/2010** of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004 Text with EEA relevance

[56] **Regulation (EU) No 181/2011** of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport and amending Regulation (EC) No 2006/2004 (Text with EEA relevance)

[57] **COM(2011) 898 final**: Communication from the Commission to the European Parliament and the Council. European vision for Passengers: Communication on Passenger Rights in all transport modes

[58] For more information see: https://europa.eu/youreurope/citizens/travel/carry/animal-plant/index_en.htm

[59] For more information see: https://europa.eu/youreurope/citizens/travel/carry/meat-dairy-animal/index_en.htm

[60] For more information see: https://europa.eu/youreurope/citizens/travel/carry/animal-plant/index_en.htm

[61] For more information, see: https://europa.eu/youreurope/citizens/travel/carry/alcohol-tobacco-cash/index_en.htm

3.2.3.1 Customs[62]

The main legislation regarding customs controls in the EU is provided by the Union Customs Code, which addresses the risk analyses carried out in order to perform checks on goods. Thus, the Customs Risk Management Framework in place will be looked at in more detail in this section, and a short overview on further relevant regulations for customs checks is given.

3.2.3.1.1 The Union Customs Code

The Union Customs Code (UCC)[63] (Regulation (EU) 952/2013[64]), set in 2013, provides the general rules and procedures for goods imported into or exported from the EU. Together with the supplement regulation Commission Delegated Regulation (EU) 2015/2446[65], it has been amended by Commission Delegated Regulation (EU) 2018/1063[66]. Furthermore, Commission Implementing Regulation (EU) 2015/2447[67] provides the rules for implementing certain provisions of the UCC. The following short summary provides an overview of its most important aspects (EU: EU Customs Code update (Summary)):

The Union Customs Code (UCC) is part of the modernisation of customs and serves as the new framework regulation on the rules and procedures for customs throughout the EU. The UCC and the related delegated and implementing acts:

- rationalise customs legislation and procedures;
- offer greater legal certainty and uniformity to businesses;
- increase clarity for customs officials throughout the EU;
- simplify customs rules and procedures and facilitate more efficient customs transactions in line with modern-day needs;
- complete the shift by customs to a paperless and fully electronic environment;
- reinforce swifter customs procedures for compliant and trustworthy businesses (Authorised Economic Operators[68]).

[62] For more information see: https://ec.europa.eu/taxation_customs/business/customs-controls_en and https://ec.europa.eu/taxation_customs/legislation_en

[63] For more information see: https://ec.europa.eu/taxation_customs/business/union-customs-code/ucc-legislation_en

[64] **Regulation (EU) No 952/2013** of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code

[65] **Commission Delegated Regulation (EU) 2015/2446** of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code

[66] **Commission Delegated Regulation (EU) 2018/1063** of 16 May 2018 amending and correcting Delegated Regulation (EU) 2015/2446 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code

[67] **Commission Implementing Regulation (EU) 2015/2447** of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code

[68] Regulation (EU) No 952/2013 defines "economic operator" as follows (Article 5): *"a person who, in the course of his or her business, is involved in activities covered by the customs legislation"*

The use of electronic data-processing techniques and electronic systems will support the application of the UCC. To underpin the development of the electronic systems, the Commission adopted its Implementing Decision [(EU) 2016/578 of 11 April 2016[69]] establishing the Work Programme for the Union Customs Code[70].

The annex of Decision [(EU) 2016/578] contains a description of the electronic systems and the target dates for starting. All electronic systems required by the UCC must be deployed no later than 31 December 2020. Should this deadline be missed, the application of certain legal provisions would have to be postponed and replaced by transitional measures until the systems become available.

The UCC (Regulation (EU) 952/2013) lays down *"the general rules and procedures applicable to goods brought into or taken out of the customs territory of the Union"* (Article 1). It applies uniformly throughout the customs territory[71] of the Union. Customs authorities within the Union are primarily responsible for implementing measures which aim at a) *"protecting the financial interests"* of the EU and its Member States; b) protecting the EU *"from unfair and illegal trade while supporting legitimate business activity"*; c) *"ensuring the security and safety"* of the EU and d) *"maintaining a proper balance between customs controls and facilitation of legitimate trade"* (Article 3). In Article 6 of the regulation, information exchange and the storage of information is addressed. According to these provisions, all information exchange (e.g. declarations, applications, decisions) between customs authorities and economic operators and customs authorities as well as the storage of this information has to be via electronic data-processing techniques[72] (see also Article 16), after drawing up common data requirements.

Customs authorities are allowed to carry out the following tasks for the purpose of customs controls at the premises of the person who holds the goods or his/her representative (Article 48):

> *"verify the accuracy and completeness of the information given in a customs declaration, temporary storage declaration, entry summary declaration, exit summary declaration, re-export declaration or re-export notification, and the existence, authenticity, accuracy and validity of any supporting document and may examine the accounts of the declarant and other records relating to the operations in respect of the goods in question (…)."*

As regards intra-union flights and sea crossings, customs controls are to be carried out on the cabin and hold baggage of persons, *"only where the customs legislation provides for such controls or formalities"* (Article 49); these controls are either security and safety checks, or linked to prohibitions or restrictions. Specific rules on the checks of cabin and hold baggage of persons are laid down in Article 50: the Commission is to determine ports or airports where customs controls and formalities are applied to a) cabin and hold baggage of persons taking a

---

[69] **Commission Implementing Decision (EU) 2016/578** of 11 April 2016 establishing the Work Programme relating to the development and deployment of the electronic systems provided for in the Union Customs Code

[70] For more information see: https://ec.europa.eu/taxation_customs/business/union-customs-code/ucc-work-programme_en

[71] Specified in Article 4 of the UCC

[72] Exceptions are stated in Article 46(3): a) permanently, where the use of electronic data-processing techniques is not appropriate for the concerned formalities and b) temporarily, in the event of failure of the computerised system

flight from non-EU airport to a Union airport (with stopover in a Union airport); taking a flight stopping at a Union airport and continuing to a non-Union airport; using a ship (or similar) departing from or terminating in a non-Union port.Customs Risk Management[73]

As trade with the EU has significantly increased over the past years, and controlling all goods is not a realistic option at border crossing points, targeted controls on the basis of risk assessments are a means to handle the large amounts of import and export goods (EC: Why is risk management crucial?). Customs authorities in the EU apply a risk management approach *"to determine the different levels of risks associated with goods being transported to and from the EU"* (EC: Customs Risk Management). Carrying out a risk assessment helps them to select the goods that might be a threat to the EU's security, and thus decide which goods to check and where. In the UCC, risk management *"means the systematic identification of risk, including through random checks, and the implementation of all measures necessary for limiting exposure to risk"* (Article 5). In short, the CRMF aims at (EC: The measures: Customs Risk Management Framework (CRMF)):

- *"establishing an equivalent level of protection in customs controls for the whole European Union,*
- *a harmonised application of customs controls by the Member States,*
- *a common approach so that priorities are set effectively and resources are allocated efficiently,*
- *a proper balance between customs controls and the facilitation of legitimate trade."*

It is based on a number of principles, which are also stated in Article 46 of the UCC (EC: The measures: Customs Risk Management Framework (CRMF)):

- the identification and control of high-risk goods movements using **common risk criteria** [Article 46(2-4)(6,7)];
- the identification of **priority control areas** subject to more intense controls for a specific period [Article 46(8)];
- systematic and intensive **exchange of risk information** between customs through the customs risk management system (CRMS) [Article 46(2,3)(5)];
- the contribution of Authorised Economic Operators (AEO) in a customs-trade partnership to securing and facilitating legitimate trade; and
- **pre-arrival / pre-departure security risk analysis** based on cargo information submitted electronically by traders prior to arrival or departure of goods in/from the EU **specifically to cater primarily for security and safety risks.**

The customs authorities can carry out any customs control they consider necessary; such as examine goods, take samples, verify the accuracy and completeness of the information in the declaration or notification as well as the existence, authenticity and validity of documents, examine accounts of economic operators and other records, inspect means of transport, luggage and other goods persons carry with them or on them (Article 46(1)). Customs controls should be based on risk analysis using *"electronic data-processing techniques, with the purpose of identifying and evaluating the risks and developing the necessary countermeasures"* (Article 46(2)), based on pre-set criteria. Risk management is applied by customs authorities in order to differentiate between the risk levels of goods which are subject to customs checks, and then to determine whether said goods will be specifically

[73] For more information see: https://ec.europa.eu/taxation_customs/sites/taxation/files/risk_management_infographic_2016_en.pdf

controlled or not (Article 46(4)). Authorities exchange risk information and results of risk analyses where a) the risks are estimated to be significant and an event triggering the risks has occurred and b) an event triggering the risks has not occurred but one authority estimates a threat to present a high risk in another Member State of the EU (Article 46(5)).

In order to establish the common risk criteria, control measures and priority control areas, *"a) the proportionality to the risk; b) the urgency of the necessary application of the controls; [and] c) the probable impact on trade flow, on individual Member States and on control resources"* have to be taken into account (Article 46(6)). The established risk criteria then include *"a) a description of the risk; b) the factors or indicators of risk to be used to select goods or economic operators for customs control; c) the nature of customs controls to be undertaken by the customs authorities"* and d) the duration of said customs controls (Article 46(7)).

Thus, key elements of CRMF are summarized as follows (EC: Customs Risk Management Framework (CRMF)):

a) The common risk criteria and standards: A set of criteria have been adopted by the Commission, which are to be applied in the risk analysis systems of the Member States *"in order to continuously screen electronic advance cargo information for security and safety purposes"* (EC: Customs Risk Management Framework (CRMF)). Article 50 of the UCC states the necessity of risk criteria to be implemented, however the criteria as such are not public. The primary aim of establishing common risk criteria is to identify high-risk consignments or goods that would have a serious impact on the security and safety of the EU, thus also to provide protection at the external frontiers. As customs at the first point of entry into the EU are legally obliged to carry out the risk analysis on all cargo, independent of the EU destination country, all consignments that cross the EU border are screened on the basis of the common risk criteria.

b) Priority Control Areas (PCAs): PCAs allow the EU to *"designate specific areas to be treated as a priority for customs control"*, which means that reinforced customs controls are carried out in these areas, based on *"common risk assessment criteria and real-time exchange of risk information"* (EC: Customs Risk Management Framework (CRMF)). These areas can be placed independently of *"customs procedure, types of goods, traffic routes, modes of transport or economic operators"* (EC: Customs Risk Management Framework (CRMF); Article 46 of the UCC) and the time period of reinforced controls is predetermined. PCAs have been set up on *"counterfeit medicine, drug precursors and the issues of valuation of textiles, smuggling of cigarettes and control of dual-use goods"* (EC: Customs Risk Management Framework (CRMF)).

c) The exchange of risk information: Within the 28 EU Member States, the Common Customs Risk Management System (CRMS)[74] provides *"a fast and easy-to-use mechanism to exchange risk-related information directly amongst operational officials and risk analysis centres"* (EC: Customs Risk Management Framework (CRMF)). A form (Risk Information Form, RIF) has to be filled online and then is made available instantly to all customs offices which are connected to the system. This is an *"effective means of ensuring that a consistent level of customs control is applied at the external frontier of the Union in relation to identified new risks thereby*

[74] For more information on EU Customs IT systems see also: https://pdfs.semanticscholar.org/8243/97189f926f977854e51d06308d84078e223d.pdf?_ga=2.131839567.1397234456.1550830129-183894930.1550830129

offering the necessary level of protection to citizens (…)" (EC: Customs Risk Management Framework (CRMF)).

With regards to the topic of the Customs Risk Management Framework the Second Progress Report (COM(2018) 549 final)[75] and the Staff Working Document (SWD(2018) 380 final)[76] can be consulted for further information. Furthermore, Regulation (EU) No 1294/2013 (Customs 2020) sets out *"a programme to support and modernise the EU's customs union by stepping up cooperation between customs authorities"* (EU: Action programme for customs in the European Union for the period 2014-20 (Customs 2020 (Summary))[77].

3.2.3.1.2 Further customs legislation

As mentioned in the above, there are restrictions, prohibitions and limits concerning the nature, quantity or value for certain kinds of goods carried along when entering or exiting the EU, such as tobacco products, alcoholic beverages, fuel, perfume, coffee, tea, electronics etc. (EC: Customs and tax allowances for travellers). The main corresponding legislation is provided by Council Directive 2007/74/EC[78] (VAT and excise duties), Regulation (EC) 1186/2009[79] (reliefs from customs duties) and Regulation (EC) 1889/2005[80] (cash).

Regulation (EC) No 206/2009[81] lays down the rules of importing products of animal origin. In general, meat and meat products, and milk and milk products are not allowed to be imported (Article 1), however, powdered infant milk, infant food and special foods or special pet feed are allowed under certain conditions (Annex IV, Part 1, (2)). Fishery products are generally approved (Article 2; Annex IV, Part 1, (4)), and of other animal products such as honey, live oysters, mussels or snails, 2kg can be carried along (Annex IV, Part 1, (5)).

---

[75] **COM(2018) 549 final**: Report from the Commission to the Council and the European Parliament – Second Progess Report on the implementation of the EU Strategy and Action Plan for customs risk management

[76] **SWD(2018) 380 final**: Commission Staff Working Document, Accompanying the document: Report from the Commission to the Council and the European Parliament – Second Progress Report on the implementation of the EU Strategy and Action Plan for Customs Risk Management

[77] For more information see: https://ec.europa.eu/taxation_customs/business/customs-cooperation-programmes/customs-2020-programme_en

[78] **Council Directive 2007/74/EC** of 20 December 2007 on the exemption from value added tax and excise duty of goods imported by persons travelling from third countries

[79] **Council Regulation (EC) No 1186/2009** of 16 November 2009 setting up a Community system of reliefs from customs duty (codified version

[80] **Regulation (EC) No 1889/2005** of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community

[81] **Commission Regulation (EC) No 206/2009** of 5 March 2009 on the introduction into the Community of personal consignments of products of animal origin and amending Regulation (EC) No 136/2004 (Text with EEA relevance)

3.2.3.2 Aviation security

Regulation (EC) No 300/2008[82] lays down the common rules and standards on aviation security, for all civil airports in the EU and air carriers providing goods or services via these airports (Article 2). These common rules also apply to Norway, Iceland, Liechtenstein and Switzerland (EC: Aviation Security). Common basic standards for protecting civil aviation are the passenger and cabin baggage screening in order to find prohibited items such as weapons and explosives and prevent them from being carried on an aircraft (Annex, 4.1). The Regulation specifies prohibited articles as *"weapons, explosives or other dangerous devices, articles or substances that may be used to commit an act of unlawful interference that jeopardises the security of civil aviation"* (Article 3).

In order to prevent unauthorized persons and vehicles from accessing the airside and security restricted areas, access controls have to be performed. Persons and vehicles are only allowed to access these areas if they fulfil the required security conditions. In order to obtain a crew identification card or an airport identification card that authorizes access to the security restricted areas, persons, including flight crew members have to successfully complete a background check (Annex, 1.2). Upon entering security restricted areas or critical parts thereof, all persons and their items have to be screened (Annex, 1.3). Furthermore, also vehicles entering security restricted areas have to be examined (Annex, 1.4).

Commission Implementing Regulation 2015/1998[83] was adopted in 2015, laying down the detailed measures for the implementation of the security standards specified in Regulation (EC) No 300/2008, and more specifically, Commission Regulation (EU) No 245/2013[84] specifies rules for the screening of liquids, aerosols and gels at EU airports.

3.2.3.3 Maritime security[85]

Maritime transport provides the main route for European imports and exports to the rest of the world, and with over 400 million passengers per year, it is an important source of employment for the European economy (EC: Maritime – What do we want to achieve?). Among other objectives, the European Commission works actively against piracy and terrorism threats. Its strategic goals and recommendations for the EU were set out in 2009 in the Maritime Transport Policy until 2018 (EC: Maritime Transport Strategy). The

[82] **Regulation (EC) No 300/2008** of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (Text with EEA relevance)

[83] **Commission Implementing Regulation (EU) 2015/1998** of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (Text with EEA relevance)

[84] **Commission Regulation (EU) No 245/2013** of 19 March 2013 amending Regulation (EC) No 272/2009 as regards the screening of liquids, aerosols and gels at EU airports (Text with EEA relevance)

[85] For more information, a compilation of EU legislation on Maritime Security can be found here: https://ec.europa.eu/transport/sites/transport/files/modes/maritime/security/doc/legislation_maritime_security.pdf

corresponding Commission Communication [86] recommends actions to increase competitiveness and sustainability of the maritime sector.

Regulation (EC) No 725/2004 [87] introduces measures for improving the security of international and domestic shipping as well as port facilities against intentional unlawful acts and ensures that the security measures of the IMO[88] (see below) are implemented uniformly (Article 1). Since July 2004, all EU countries have to apply the SOLAS[89] and ISPS Code[90] for international shipping (Article 3). Ships subject to these measures, who wish to enter an EU port, have to provide security information to the national authorities at least 24h in advance, or at the latest when it leaves the previous port (Article 6).

As prohibited goods on board of ships and in port facilities, Annex II (Part A, 1.3) specifies weapons, incendiary devices or explosives that should not be introduced, as well as dangerous substances (Annex III, Part B, 13.13).

Directive 2005/65/EC[91] complements the measures of Regulation (EC) No 725/2004, aiming at establishing an EU framework consisting of common basic rules on port security measures and implementation as well as compliance monitoring mechanisms for them. It applies to people and infrastructure in ports and adjacent areas (Recital 2, Article 6). Member States have to designate a port security authority for each port, responsible for taking the necessary port security measures (Article 5), as well as a port security officer who act as the contact point for issues related to port security (Article 9). Depending on the perceived risk for a port, different security levels can be established (Article 2):

- *"security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times;*
- *security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of a security incident;*
- *security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target."*

[86] **Commission Communication COM(2009) 8 final**: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Strategic goals and recommendations for the EU's maritime transport policy until 2018

[87] **Regulation (EC) No 725/2004** of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (Text with EEA relevance)

[88] For more information see: http://www.imo.org/en/About/Pages/Default.aspx

[89] For more information see: http://www.imo.org/en/about/conventions/listofconventions/pages/international-convention-for-the-safety-of-life-at-sea-(solas),-1974.aspx

[90] For more information see: http://www.imo.org/blast/mainframe.asp?topic_id=897#what and http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx

[91] **Directive 2005/65/EC** of the European Parliament and of the Council of 26 October 2005 on enhancing port security (Text with EEA relevance)

As per this Directive, security organisations have to be able to detect weapons, dangerous substances and devices (Annex IV, (10)); however, more details are not provided.

International Maritime Organization

For the sake of completeness, the International Maritime Organization (IMO) and its main legislative framework, the International Ship and Port Facility (ISPS) Code should be introduced shortly. The IMO is an agency of the United Nations, setting the global standard for the *"safety, security and environmental performance of international shipping"* (IMO: Introduction to IMO). As the main objective, it creates a fair and effective regulatory framework for the shipping industry, which is adopted and implemented universally.

One of these regulatory frameworks, addressing matters of maritime security, is the International Ship and Port Facility (ISPS) Code (IMO: SOLAS XI-2 and the ISPS Code). It has entered into force under SOLAS and provides the basis for a mandatory security regime of international shipping. The main objectives of the ISPS Code are summarized in following (IMO: SOLAS XI-2 and the ISPS Code):

- establishment of an **international framework** that fosters cooperation between Contracting Governments, Government agencies, local administrations and the shipping and port industries, in **assessing and detecting potential security threats** to ships or port facilities used for international trade, so as to implement preventive security measures against such threats;
- determining the respective roles and responsibilities of all parties concerned with **safeguarding maritime security in ports and on board ships**, at the national, regional and international levels;
- to ensure that there is early and efficient collation and **exchange of maritime security-related information**, at national, regional and international levels;
- to provide a **methodology for ship and port security assessments**, which facilitates the development of ship, company and port facility security plans and procedures, which must be utilised to respond to ships' or ports' varying security levels; and
- to ensure that **adequate and proportionate maritime security measures** are in place on board ships and in ports.

In order to reach these objectives, SOLAS contracting governments as well as port authorities and shipping companies are required to appoint security officers and personnel on every ship, in port facilities and shipping companies, who are in charge of implementing security plans and of managing potential threats in this regard.

3.2.3.4 Movement of pets[92]

The non-commercial movement of pets is regulated in Regulation (EU) No 576/2013[93], which aims at facilitating formalities for dog, cat and ferret owners when traveling with their pets. It applies to non-commercial movement of pets into an EU country from another EU or non-EU country.

[92] For more information see: https://europa.eu/youreurope/citizens/travel/carry/animal-plant/index_en.htm and https://ec.europa.eu/food/animals/pet-movement_en

[93] **Regulation (EU) No 576/2013** of the European Parliament and of the Council of 12 June 2013 on the non-commercial movement of pet animals and repealing Regulation (EC) No 998/2003 (Text with EEA relevance)

Due to the adoption of harmonized rules, EU nationals can freely travel with their cats, dogs or ferrets[94] within the EU, given that the animal has a European pet passport[95] with documentation of an anti-rabies vaccination or the animal health certificate (Article 6). It has to have an electronic microchip or a readable tattoo (applied before 3 July 2011) with the code documented in the passport (Article 17). Furthermore, compliance with *"any preventive health measures for diseases […] other than rabies"* must be ensured (Article 6).

Other animals or plants and parts thereof can be carried as well when travelling in EU countries. However, most EU countries have strict rules regarding the transport of endangered species, which means a permit might be required.

3.3 Information exchange and operational cooperation

In order to enable and facilitate the exchange of information between law enforcement authorities within the EU, a variety of instruments are in place. National law enforcement authorities are in need of *"timely access to accurate and up-to-date-information and criminal intelligence"* for the successful prevention, detection and investigation of criminal activities (EC: Information exchange). Together with information exchange, operational cooperation between Member States authorities contributes to *"the realisation of a genuine area of EU internal security"* (EC: Operational cooperation). In the following, legislation texts on information systems currently in place, as well as instruments of operational cooperation will be discussed.

3.3.1 Information systems[96]

Technology and information systems play a crucial role in improving and reinforcing external borders (EC: Visa Information System (VIS)). To this end, this chapter introduces existing and future (planned) information systems.

3.3.1.1 Visa Information System (VIS)

Regulation (EC) No 767/2008[97] establishes the Visa Information System (VIS) and the exchange of its data whilst the Council Decision 2008/633/JHA[98] regulates the access for consultation of

[94] For other pets such as rabbits or canaries, relevant national rules apply.

[95] The specifications for the new pet passport can be found in **Regulation (EU) No 577/2013**. It has to include information such as the location of the microchip or tattoo, the name, species and further characteristics of the pet, the owner's and vet's details, and the details of the vaccination against rabies. However, the existing passport model (issued before 29 Dec 2014) remains valid.

[96] For more information see: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180516_eu-information-systems-security-borders_en.pdf

[97] **Regulation (EC) No 767/2008** of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

[98] **Council Decision 2008/633/JHA** of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences

the VIS by designated authorities and Europol (EC: Visa Information System (VIS)); EC: A stronger, more efficient and secure EU visa policy). The key points of the regulation are summarized below, indicating the respective regulation article in square brackets (EU: VIS Regulation (Summary)). The subsequent text gives more detail about further relevant articles of the Regulation.

What is VIS?

The VIS Regulation defines the purpose and functionalities of, as well as the responsibilities for, the Visa Information System (VIS). It provides the conditions and procedures for the exchange of visa data between the European Union (EU) countries and associated countries applying the common visa policy [Article 2]. Thus, the examination of applications for short stay visas and decisions on extending, revoking and annulling visas, as well as the checks on visas and the verifications and identifications of visa applicants and holders are facilitated.

What data is collected?

Only the following categories of data are recorded in the VIS [Article 5]:

- alphanumeric data on the applicant and on the visas requested, issued, refused, annulled, revoked or extended;
- photographs;
- fingerprint data;
- links to previous visa applications and to the application files of persons travelling together.

Who has access?

- for entering, amending or deleting data, [access] is reserved exclusively to duly authorised staff of the visa authorities [Article 6];
- for consulting data, [access] is reserved exclusively to duly authorised staff of the visa authorities and authorities competent for checks at the external border crossing points, immigration checks and asylum, and is limited to the extent the data is required for the performance of their tasks [Article 6].

The authorities with access to VIS must ensure that its use is limited to that which is necessary, appropriate and proportionate for carrying out their tasks [Article 7]. Furthermore, they must ensure that in using VIS, the visa applicants and holders are not discriminated against [on grounds of sex, race, religion/belief, disability, age or sexual orientation] and that their human dignity and integrity are respected [Article 7].

Use of the data by the visa and other competent authorities

The competent visa authority may consult the VIS for the purpose of examining applications and decisions to issue, refuse, extend, annul or revoke a visa, or to shorten a visa's validity period [with one or several of the following data: application number; names and date, place or country of birth; the travel document; data about the employer; and fingerprints] [Article 15]. It is authorised to carry out searches with some of the data included in the application form and the application file [Article 15]. If the search indicates that data on the applicant is recorded in the VIS, the visa authority will be given access to the application file and linked application files [Article 15]. For prior consultation, the country responsible for examining the application must transmit any consultation requests with the application number to the VIS, indicating the country or countries to be consulted [Article 16]. The VIS will forward the request to the country concerned, which will, in turn, send the response to the VIS, which will then forward the response to the requesting country [Article 16]. For statistical and reporting purposes, the visa authorities are authorised to consult data that does not allow for the identification of the applicant [Article 17].

The authorities responsible for carrying out checks at external borders and within the national territories have access to search the VIS with the number of the visa sticker together with fingerprints [Article 18]. They may search the VIS for the purpose of verifying the identity of the person and/or the authenticity of the visa and/or whether the person meets the requirements for entering, staying in or residing within the national territories [Article 19]. If, based on this search, data on the visa holder is found in the VIS, the relevant authorities may consult certain data in the application file [Article 19]. For identifying a person who may not or may no longer fulfil the required conditions, the competent authorities have access to search with fingerprint data [Article 20]. If that person's fingerprints cannot be used or the search with the fingerprints fails, the relevant authorities may search the VIS with the name, sex, date and place of birth and/or information taken from the travel document [Article 20]. These may be used in combination with the nationality of the person.

Asylum authorities have access to search the VIS with fingerprint data, but solely for the purposes of determining the EU country responsible for the examination of an asylum application and of examining an asylum application [Articles 21, 22]. However, if the fingerprints of the asylum seeker cannot be used or the search fails, the authorities may carry out the search with the data set out above [Article 22]. Each application file is stored in the VIS for a maximum of five years [Article 23]. Only the country responsible has the right to amend or delete data it has transmitted to the VIS [Article 24].

Data protection

The responsible country provides the persons concerned with information on the identity and contact details of the controller responsible for the processing of the data, the purposes for which the data is processed within the VIS, the categories of the recipients of the data, the period of retention of the data and the right to access, correct and delete the data [Articles 37, 38]. In addition, the country must inform the persons concerned of its obligation to collect the data. Any person is entitled to receive information on how to bring an action or a complaint before the competent authorities or courts of the country concerned if he/she is refused the right of access to, or the right of correction or deletion of, data relating to him/her [Article 38; Article 40]. Data in the VIS is not to be communicated to third countries or international organisations unless indispensable for attesting a third-country national's identity in individual cases [Article 31]. The communication may be made when a set of conditions are met, with due respect to the rights of refugees and persons requesting international protection [Article 31].

General provisions: Designated authorities can access the VIS data if it is believed that they will help to prevent, detect or investigate terrorist and other serious criminal offences (Article 3). Europol can also access the data for the performance of their task. The details concerning the access for consultation are described in the following Decision.

Entry and use of data by visa authorities: When the visa authority receives an application, it has to fill out the application file (Article 8) with the following information: application number; status information; surname (at birth); first name; sex; date, place and country of birth; nationality; place and date of application; type of visa; details about the person paying for the visa; destination and purpose of travel; date of arrival/departure; residence; occupation and employer; a photograph and fingerprints (Article 9). Additional information is added when the visa has been issued (Article 10), discontinued (Article 11), refused (Article 12), annulled/revoked (Article 13), or extended (Article 14).

Access to data by other authorities: Border guards can search the data using the visa sticker number in combination with fingerprints in order to verify the identity of a visa holder at external border crossing points (Article 18). If the data indeed is recorded, border control authorities can then also access the status and data from the application form; photographs,

and visa validity and situation. The conditions for asylum authorities accessing VIS data are described in the above (Summary).

Operation and responsibilities: A management authority is responsible for the operational management of the central VIS (Article 26). Article 27 defines the location of the VIS and Article 28 the relation to the national systems. Each Member State has to ensure that the data are collected and transmitted to the VIS lawfully; and that the data are accurate and up-to-date (Article 29). VIS data can in exceptional cases be kept in national files on an individual case basis (Article 30). VIS data generally is not allowed to be transferred or made available to a third country or national organisation except when it is necessary to prove the identity of third-country nationals for the purpose of return (Article 31). Each Member State has to ensure the data's security by physically protecting the data and prevent unauthorised access of the data (Article 32). Anyone who has suffered damage after the unlawful processing can get a compensation from the responsible Member State (Article 33). Data processing records within the VIS have to be kept by each Member State and the Management Authority (Article 34).

Rights and supervision on data protection: The implementation of the regulation is supervised by the National Supervisory Authority (Article 41) and the European Data Protection Supervisor (Article 42) who also cooperate with each other (Article 43).

As mentioned in the previous Regulation, the VIS can also be accessed to prevent, detect and investigate terrorist and other serious criminal offences, which is laid down in Council Decision 2008/633/JHA[99] (Article 1). It allows law enforcement authorities (e.g. authorities responsible for tackling terrorism or serious criminal offences such as drug or human trafficking) in the Schengen Area and Europol to access the VIS. The key points of the Decision are summarized below, with information regarding the relevant legislation articles (EU: Rules for access to the EU's Visa Information System (VIS) (Summary)).

Access

Access to the VIS data applies on a case-by-case basis with reasoned written or electronic requests [Recital 8; Article 4]. The designated authorities may only consult the VIS if it is necessary or if there are reasonable grounds for believing that such a search would substantially **help in preventing, detecting or investigating serious crime** [Recital 8; Article 5]. This may happen, for example, in cases of terrorism or with persons linked directly or indirectly to terrorist or other serious criminal offences.

Type of searches

Searches in the VIS are limited to specific data, for example [Article 5]:

- **surname, first names, sex** and date, place and country of birth;
- current **nationality** and nationality at birth of the visa applicant;
- type and number of the **travel document**;
- [destination and duration of **intended stay**];
- **purpose of travel**, and intended date of arrival and departure;
- intended border of **first entry** or transit route;

[99] **Council Decision 2008/633/JHA** of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences

- **fingerprints**;
- **type of visa** and number of the visa sticker;
- details of the person who has issued an invitation for the visa applicant, etc.

If the search using any of the above data is successful, the authorities may in addition access other data, such as **photographs** [Article 5].

Data protection

When processing personal data in line with this decision, each EU country has to ensure an adequate level of data protection. [Personal data can only be processed if they serve to prevent, detect, investigate and prosecute terrorist or other serious criminal offences]. Only in urgent cases and for the purpose of preventing and detecting serious offences, personal data may be transferred to non-EU countries or to international organisations. However, in such cases, the consent of the EU countries that entered the data must be obtained [Article 8]. EU countries must also ensure the security of the data accessed in VIS during their transmission to the designated authorities [Article 9].

Europol can access VIS in cases where it is necessary for them to perform a task (Article 7). If data security during the transmission of data to designated authorities (Article 9) is not ensured and a person has suffered damage, he or she can receive compensation (Article 10). Data subjects have the right of access, correction and deletion of their data in the VIS (Article 14).

3.3.1.2 Schengen Information System (SIS II)

Regulation (EC) No 1987/2006[100] establishes the second-generation Schengen Information System (SIS II) whilst Council Decision 2007/533/JHA[101] complements the Regulation (EC: Schengen Information System). The original SIS has been operational since the 1990's, however it has been replaced by the SIS II in 2013 as it offers enhanced and additional functionalities (EC: Questions and Answers: Schengen Information System (SIS II)). In a nutshell, it is a *"large-scale information system containing alerts on persons and objects"*, consisting of the following technical architecture (EU: Second generation Schengen Information System (SIS II) – former 1st pillar regulation (Summary); Article 4):

- *"a **central system** ("Central SIS II");*
- *a **national system** (the "N.SIS II") in each Member State (the national data systems that will communicate with the Central SIS II);*
- ***a communication infrastructure** between the central system and the national systems providing an encrypted virtual network dedicated to SIS II data and the exchange of data between the authorities responsible for the exchange of all supplementary information (SIRENE[102] Bureaux)."*

[100] **Regulation (EC) No 1987/2006** of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

[101] **Council Decision 2007/533/JHA** of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

[102] For information about the SIRENE manual see **2008/333/EC:** Commission Decision of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document number C(2008) 774)

The key points of the regulation are summarized below, indicating the corresponding legislation articles (EU: Second generation Schengen Information System (SIS II) – former 1st pillar regulation (Summary)).

Alerts issued in respect of non-EU nationals for the purpose of refusing entry and stay

SIS II will only contain those categories of data supplied by each of the Member States, which are necessary for alerts for refusing entry or stay. SIS II only stores the following information on persons for whom an alert has been issued: surname(s) and forename(s), **name(s)** at birth, aliases, specific physical characteristics, place and date of birth, **sex**, **photographs, fingerprints**, **nationality**(ies), whether the person concerned is **armed, violent or has escaped**, **reason** for the alert, authority issuing the alert, a reference to the decision giving rise to the alert, [action to be taken,] and link(s) to other alerts issued in SIS II [Article 20]. It will also include the action to be taken in the event that there is a "hit" (i.e. if a competent national authority finds an alert in SIS II concerning a non-EU national on whom they have carried out a check). Photographs and fingerprints will be used to confirm the identity of a non-EU national who has been located as a result of an alphanumeric search made in SIS II [Article 22].

Access to and processing of data in SIS II

Authorities responsible for **border control** and other **police and customs checks** [as well as visa authorities] within the Member State concerned have a right to access alerts [Article 27]. By extension, it is also be possible for national judicial authorities to access the system for the performance of their tasks [Article 27]. In any case, users will only be able to access data that is required for the performance of their tasks [Article 28].

[The alerts entered in the SIS II can only be kept for the time that is required to achieve whatever purposes they were entered (otherwise they need to be erased)], and a Member State issuing an alert shall review the need to keep it within **three years** of its entry in SIS II [Article 29]. It will only be possible to copy data for technical purposes [Article 31]. Such copies, which lead to off-line databases, may be retained for no more than 48 hours [Article 31]. It will not be possible to use data for administrative purposes [Article 31].

A Member State issuing an alert will be responsible for ensuring that the **data are accurate, up-to-date and lawfully entered** in SIS II [Article 34]. Only the Member State issuing an alert will be authorised to modify, add to, correct, update or delete data that it has entered [Article 34]. If a Member State other than that issuing an alert obtains evidence suggesting that an item of data is incorrect, it will inform the Member State that issued the alert as soon as possible. The Member State that issued the alert will check the communication and, if necessary, correct or delete the item in question without delay [Article 34].

Data protection

Processing of **sensitive categories** of data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and data concerning health or sex life) will be **prohibited** [Article 40]. Any person will have the right to request **access to data** relating to him/her (personal data) that has been entered in SIS II, and to have factually **inaccurate personal data corrected or unlawfully stored personal data deleted** [Article 41]. Regarding the exercise of their rights of correction and deletion, individuals will be informed about the follow-up as soon as possible, and in any event no later than three months from the date of their application for correction or deletion [Article 41]. [If an alert has been issued for a person, he or she has the right to be informed about it (Article 42)]. It will be possible for any person to bring an action before the competent courts or authorities to access, correct, delete, or obtain information or compensation in connection with an alert relating to him/her [Article 43].

Each Member State has an authority that manages the operation and information exchange (Article 7). To ensure that the data is secure, Member States have to protect the data by for

example denying unauthorised persons access to read, copy, remove or modify the data in the SIS II (Article 10). The SIS II can produce alerts for third-country nationals to refuse entry and stay (Chapter 4). Member states can only process data in order to refuse entry into or stay into Member States' territory (Article 31). The data is not allowed to be transferred to third countries or international organisations (Article 39).

Council Decision 2007/533/JHA[103] complements the Regulation. Key points are summarized below, indicating the respective Decision articles (EU: Second generation Schengen Information System (SIS II) – former 3rd pillar decision (Summary)). The subsequent text gives more detail about the respective articles of the Decision but only includes articles that are different from the regulation or are additionally added.

What is different in the Decision?

The decision defines the **categories of data** (alerts on persons and objects) to be entered in the system [Article 20] for supporting operational cooperation between police and judicial authorities in criminal matters [Article 2], the purposes for which these data are to be entered, the criteria and procedures for entry and processing of these data, and the authorities that will have a right to access these data [Articles 20, 40]. The decision also includes specific provisions on data processing and protection with respect to these categories of data [Article 20].

Alerts included in SIS II

The decision specifies that the following categories of alerts will be included in SIS II, in order to support operational cooperation between police and judicial authorities in criminal matters: **alerts on persons wanted** for arrest for surrender purposes on the basis of a European Arrest Warrant and persons wanted for extradition purposes [Chapter V]; need to be ascertained; **alerts on persons sought to assist with a judicial procedure** [Chapter VII]; **alerts on persons or vehicles, boats, aircraft and containers** for discreet or specific checks for the purposes of prosecuting criminal offences and for the prevention of threats to public security [Article 36; Article 37]; **data on objects sought for the purposes of seizure** or use as evidence in criminal proceedings [Chapter IX]. [These include: motor vehicles, boats, aircrafts, trailers, firearms, stolen documents, identity papers, vehicle registrations[104] and number plates, banknotes, and means of payment (Article 38)].

Access to and processing of SIS II data

Rules on access to SIS II data in the decision are the same as those in the regulation. However, the decision also provides for access to SIS II data by specifically authorised staff of **Europol** [Article 41] and national members of **Eurojust** and their assistants [Article 42]. These bodies may only access the specific data that they require for the performance of their tasks [Article 43]. The decision adds additional safeguards by reducing this period to one year for alerts on persons for discreet or specific checks. The decision also contains specific provisions on the maximum periods for retaining alerts on objects (5 or 10 years depending on the type of alert) [Article 45].

A Member State can flag an alert in cases where an action is to be taken, however if this action (giving effect to an alert) is incompatible with national law, it can require that the action should not be taken in its territory (Article 24). Data about wanted persons on the basis of a

[103] **Council Decision 2007/533/JHA** of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)

[104] **Regulation (EC) No 1986/2006** of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates

European Arrest Warrant can be entered into the SIS II at the request of the judicial authority of the Member State (Article 26). Data can also be entered on the basis of arrest warrants between the EU and third countries. Data about missing persons can also be entered into the SIS II at the request of the competent authorities (Article 32).

Generally, transfer of personal data to third parties is prohibited (Article 54), however, the exchange of data on stolen or lost passports with Interpol is allowed (Article 55).

3.3.1.3 European Travel Information and Authorisation System (ETIAS)

Regulation (EC) No 2018/1240 [105] establishes the European Travel Information and Authorisation System (ETIAS), which regulates the procedure for third countries whose citizens can enter the Schengen area without needing a visa (Article 1, Recital 5) (EC: ETIAS – The European Travel Information and Authorisation System). This concerns 61 visa free countries[106] (listed in Annex II of Council Regulation (EC) No 539/2001)[107] (Article 2). ETIAS is expected to be fully functional by 2021.

General provisions: ETIAS consists of three parts: the information system (developed by eu-LISA, see 3.3.2.2) (Article 6), the central unit (established within Frontex, see 3.3.2.1) (Article 7), and the national unit (Article 8). Also, within Frontex, a screening board witch an advisory function is established (Article 9). Additionally, a fundamental rights guidance board also with an advisory function is established (Article 10). Its purpose is to assess the processing of applications and the implementation in regards to data protection and non-discrimination. The ETIAS can query the Interpol Stolen and Lost Travel Document (SLTD) database[108] as well as the Interpol Travel Documents Associated with Notices (TDAWN) database (Article 12). Only authorized staff (Article 50) have access to the ETIAS, as well as border authorities (Article 47), carriers (Article 45), and immigration authorities (Article 49) (Article 13). The processing of personal data in the ETIAS has to be non-discriminative on the grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation (Article 14).

---

[105] **Regulation (EU) 2018/1240** of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226

[106] From https://www.schengenvisainfo.com/etias/: Albania, Andorra, Antigua and Barbuda, Argentina, Australia, Bahamas, Barbados, Bosnia and Herzegovina, Brazil, Brunei, Canada, Chile, Colombia, Costa Rica, Dominica, El Salvador, Georgia, Grenada, Guatemala, Honduras, Hong Kong S.A.R, Israel, Japan, Kiribati, Macao S.A.R, Macedonia, Malaysia, Marshall Islands, Mauritius, Mexico, Micronesia, Moldova, Monaco, Montenegro, Nauru, New Zealand, Nicaragua, Palau, Panama, Paraguay, Peru, Saint Kitts and Nevis, Saint Lucia, Saint Vincent, Samoa, Serbia, Seychelles, Singapore, Solomon Islands, South Korea, Taiwan, Timor Leste, Tonga, Trinidad and Tobago, Tuvalu, Ukraine, United Arab Emirates, United States of America, Uruguay, Vanuatu, and Venezuela.

[107] **Council Regulation (EC) No 539/2001** of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement

[108] For more information see: https://www.interpol.int/INTERPOL-expertise/Border-management/SLTD-Database

Application: Applicants for the ETIAS can fill out an online application (Article 15). The following data has to be provided for the ETIAS: surname (family name), first name(s) (given names(s)), surname at birth, first name(s) of the parents, other names (alias(es), artistic name(s), usual name(s)); date, place and country of birth, sex, current nationality and other nationalities; type, number and country of the issue of the travel document; the date of issue and expiry; home address or city and country of residence; email address and phone numbers; education and current occupation; in which Member State they first intend to stay; whether the person has been convicted of criminal and terrorist offence in the past and whether the person has stayed in war or conflict zone (Article 17). Minors only have to give surname and first name(s); home and email address; phone number of parental authority. The application also includes a declaration of authenticity, completeness, and correctness of the person's data.

Examination of application: The ETIAS system automatically compares the data against SIS, EES, VIS, Eurodac, Europol data (Article 29) and Interpol SLTD and TDAWN databases (Article 20). Where there is no hit, the travel authorisation is issued (Article 21). Where there is a hit the document is further processed manually (Article 22). It is then decided whether to issue a travel authorisation or not (Articles 26, 36, 37). For this, also additional information from the applicant (e.g. interview) can be requested (Article 27). The applicant gets not of the decision within 96 hours after the application (Articles 30, 32, 38).

ETIAS watchlist: The ETIAS watchlist[109] is made of data about persons who are suspected of having or going to have taken part in terrorist or criminal offences (Article 34). The list contains information about surname and other names; date and surname at birth; travel document; home, email address and IP address; phone number; name, addresses and phone number of a firm or organisation (Article 35). A Member State or Europol can enter the data into the ETIAS watchlist.

Access: Border authorities can consult the ETIAS to know whether or not a traveller has a valid travel authorisation, whether it will expire within the next 90 days, and whether there were false hits (Article 47). Designated authorities of Member States can consult the data if it is necessary for the purposes of prevention, detection or investigation of a terrorist or other serious criminal offence and there is a reasonable belief that the consultation of the ETIAS will help to achieve the previously mentioned (Article 52). However, the search is limited to only names of a person; number of the travel document; home, email and IP address and phone numbers (to narrow down the search also nationality, sex and age can be used). Europol can also access the ETIAS if the consultation is necessary to support action by Member States (Article 53).

Data protection: The application and its data are only allowed to be saved for the validity of the travel document or five years from the last decision of refusal annulment or revocation of the travel authorisation (Articles 37, 40, 41) and then has to be deleted automatically (Article 54). It can be stored an additional three years with the explicit consent of the traveller for the purpose of facilitating a new application. The data in the ETIAS system has to be up-to-date so that is accurate (Article 55). If they are not accurate, they have to be erased. Regulation (EU) 2016/679 applies in the context of assessing applications, by border and immigration

[109] For more information see: https://www.etiasvisa.com/etias-news/what-is-the-etias-watchlist-for-europe

authorities. People have the right of access to, rectification, completion, and erasure of their personal data as well as the restriction of processing (Article 64). Stored data is generally not allowed to be transferred to a third country, international organisation or any private party except to Europol, Interpol in certain circumstances (Article 65). In case of an exceptional urgency (e.g. terrorist offence) or for the prevention, detection or investigation in cases of criminal offence, however, it is allowed to transfer data to a third country. Data protection is supervised by the supervisory authority (Article 66) and the European Data Protection Supervisor (Article 67).

3.3.1.4 Entry/Exit System (EES)

Regulation (EU) 2017/2226[110] establishes an Entry/Exit System (EES), which applies to non-EU nationals crossing the EU's external borders for a short stay and replaces the current system of manual stamping of passports. The EES is part of the recent Smart Borders package[111] and amends the Schengen border code as regards the use of the Entry/Exit System[112]. The following summarizes the Regulations' key points (EU: Smart borders: EU Entry/Exit System (Summary)). The subsequent text gives more detail about the respective articles of the Regulation.

Subject matter

The regulation creates the **EES**, a common electronic system which [Article 1]:

- **records and stores the date, time and place of entry and exit** of non-EU nationals crossing the EU's borders;
- automatically **calculates the duration of authorised stay** of such non-EU nationals, and **generates alerts** to EU countries when the authorised stay has expired.

The system **replaces the requirement to stamp the passport** of non-EU nationals, which is applicable by all EU countries [Recital 7].

Scope

The EES applies to **travellers** subject to a visa requirement as well as those exempted from it and admitted for a short stay of up to 90 days in a 180-day period, who cross the external borders of the Schengen area. The EES will also record data on non-EU nationals whose entry for a short stay has been refused.

The EES will operate at the external borders of the EU countries which apply the Schengen *acquis* in full and at the borders of EU countries which — at the time the system will start its operations — will not yet apply the Schengen *acquis* in full, but will have successfully gone through the Schengen evaluation

[110] **Regulation (EU) 2017/2226** of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011

[111] For more information see: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/smart-borders_en

[112] **Regulation (EU) 2017/2225** of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System

procedure and have obtained passive access to the VIS and full access to the Schengen Information System [Recital 10, Article 4].

Data storage and accessibility

The EES will store data on **identity, travel documents** as well as **biometric data** [Article 15]. The data will be kept for **3 years for those travellers who respect the short stay rules**, and **5 years** for those who exceed their authorised period of stay [Recital 32-34, Article 34].

The data stored will be accessible to border authorities, visa-issuing authorities and authorities responsible for monitoring whether a non-EU national fulfils the conditions of entry or residence [Articles 23, 24, 26]. For the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences designated law enforcement authorities and Europol may request the consultation of EES data [Recital 29, Articles 9, 29, 30, 31].

Technical architecture

The EES comprises [Recital 16, Article 7]:

- **a central system** which will operate a computerised central database of biometric and alphanumeric data (a mix of letters and numbers);
- **a national uniform interface** in each participating country;
- **a secure communication channel** between the EES central system and the central system of the VIS;
- **a secure and encrypted communication infrastructure** between the EES central system and the national uniform interfaces (identical interfaces for all EU countries connect their border infrastructures to the EES central system);
- **a data repository** to obtain customisable reports and statistics;
- **a web service** to enable non-EU nationals to verify their remaining authorised stay.

The **eu-LISA agency** has the responsibility for **developing and operating the system** [Article 5], including for adapting the VIS so as to ensure the **interoperability** between the EES central system and the VIS central system [Articles 7, 8] [see 3.3.1.1].

General provisions: The EES alerts Member States when the authorised stay has expired and thus allows to identify overstayers (Article 6). As it is connected to the VIS (Article 7), visa-related data can be retrieved and imported into the EES in order to create or update the EES record (Article 8). Only national authorities of the Member States (border, visa and immigration authorities) have access to the EES in order to enter, amend, erase or consult data (Article 9). Additionally, the access is limited to the purpose that is pursued and has to be necessary and appropriate (Article 10). The automated calculator within the EES indicates the maximum duration of authorised stay for third-country nationals and for the competent authorities (Article 11). The EES includes an information mechanism that automatically identifies overstayers and then creates a list that is available to the competent national authorities (Article 12). There is also a web service to enable third-country nationals to check their remaining authorised stay (Article 13).

Entry and use of data by competent authorities: Border authorities create new files for third-country nationals that apply for the first time and update files where a file has been created previously (Article 14). Border authorities have to enter the following data: surname (family name), first name or names; date of birth; nationalities; sex; type, number and expiry date of travel document; facial image (taken live, Article 15) (Article 16). Each time a third-country national crosses any external border, border authorities have to add data such as the border crossing point of entry and exit. Border authorities also have to create files for visa-exempt

third-country nationals with the following data: surname (family name), first name or names; date of birth; nationalities; sex; type, number and expiry date of travel document; facial image (taken live, Article 15); and fingerprint data (Article 17). They also have to enter personal data of third-country nationals who have been refused entry (Article 18), where the authorisation for short stay is revoked/annulled/extended (Article 19), and in case of rebuttal of the presumption that a third-country national does not fulfil the conditions of duration of authorised stay (Article 20). Border authorities have access to the EES in order to verify the identity and previous registration of third-country nationals, and for updating and consulting EES data to the extent that is required for carrying out border checks (Article 23).

Use of the EES by other authorities: Visa authorities can consult the EES in order to examine visa applications (Article 24). The use of the EES is also allowed for examining applications for access to national facilitation programmes (Article 25). Immigration authorities can also consult the EES in order to verify the identity of a third-country national (Article 26). Border or immigration authorities can access the EES with fingerprint data only or in combination with facial image in order to identify if a third-country national has been registered previously in the EES under a different identity or if he/she no longer fulfils the conditions for entry and stay (Article 27). Where necessary and in individual cases, data retrieved from the EES can be kept in national files (Article 28).

Procedure and conditions for access to the EES for law enforcement purposes: Access to the EES for law enforcement purposes has to be submitted in form of a reasoned request (Article 31). Designated authorities can access the EES only if the consultation is necessary for preventing, detecting or investigating offences; the consultation is necessary in a specific case; and there is evidence that the EES will considerably help in the prevention, detection, or investigation in question (Article 32). Similar restrictions apply to the access to EES data by Europol (Article 33).

Retention and amendment of the data: Data in the EES can be stored for three years after the exit or the refusal of entry record (Article 34). If there is no exit record, the data can be stored for a period of five years after the expiry of the unauthorised stay. In both cases, the data has to be erased automatically. Responsible Member States have the right to amend EES data by rectifying, completing or erasing the data (Article 35).

Development, operation and responsibilities: Each Member State have to ensure that the data collected in the EES is processed lawfully, that only authorised staff have access, and that the data are accurate and up-to-date (Article 39). A Member State can keep the data which that State entered in national files (Article 40). The data in the EES is not allowed to be transferred to any third country, international organisation or private entity (Article 41). However, it can be transferred in individual cases where it serves the purpose of return, or where there is an exceptional case of urgency (e.g. imminent danger due to terrorist or other criminal offence) and the transfer is necessary for the prevention, detection or investigation of such offences. Member States have to ensure data security (Article 43) to prevent security incidents (Article 44).

Rights and supervision on data protection: Third-country nationals whose data is recorded in the EES have to be given the following information: the fact that EES can be access by Member States and Europol for law enforcement purposes; the obligation on visa-exempt third-country nationals too have their fingerprints taken; all third-country nationals to have their facial image recorded; that the collection of data is mandatory in order to enter and that

otherwise the entry will be refused; the right to receive information about the remaining duration; the fact that the data may be transferred to a third country; the right to access the data; the data retention period; the right to erasure of overstayers from the list; and the right to lodge a complaint (Article 50). The supervision of data protection is handled by the supervisory authority (Article 55) and the European Data Protection Supervisor (Article 56) and their cooperation (Article 57).

3.3.1.5 Passenger Name Record (PNR)

Council Directive 2004/82/EC[113] requires carriers to collect and transmit passenger data the Member States' authorities whilst Directive (EU) 2016/681[114] regulates the use of passenger name record (PNR) data in order to prevent, detect, investigate and prosecute terrorist or other serious criminal offences (EC: Passenger Name Record; EC: Closing security information gaps: new EU rules on Passenger Name Record (PNR) data). It also regulates the transfer from airlines to Member States and the processing of these data by Member States' competent authorities. The following summarizes the PNR Directive's key points, indicating the correspondent legislation articles (EU: Use of passenger records to prevent terrorism and serious crime (Summary)). The subsequent text then gives further details.

What are PNR data?

They consist of **booking information** stored by airlines in their reservation and departure control systems. The information collected includes [Annex I]:

- travel dates;
- travel itinerary;
- ticket information;
- contact details;
- means of payment used;
- baggage information.

Scope

Each EU country must establish a **Passenger Information Unit (PIU)**. A PIU is responsible for [Article 4]:

- collecting, storing and processing the data, as well as transferring the data or the results of the processing to the competent national authorities;
- exchanging PNR data and the results of processing with other EU countries and Europol.

Airlines must provide PIUs in EU countries with the PNR data for **flights entering or departing from the EU**. It also allows — but does not require — EU countries to collect PNR data concerning selected intra-EU flights [Article 2].

Processing

The data collected may only be **processed to prevent, detect, investigate and prosecute terrorist offences and serious crime** [Article 1]. [The PIU has a data protection officer (DPO) appointed as a single

[113] **Council Directive 2004/82/EC** of 29 April 2004 on the obligation of carriers to communicate passenger data

[114] **Directive (EU) 2016/681** of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime

point of contact for data subjects that is responsible for monitoring the processing of PNR data and implementing relevant safeguards (Article 5)]. Data should only be processed in the following cases [Article 6]:

- for a pre-arrival assessment of passengers against **predetermined risk** criteria and relevant law enforcement databases;
- for use in specific **investigations/prosecutions**;
- as input in the development of **risk assessment criteria**.

Transfer and exchange of data [Articles 8, 9]

- EU countries should not be able to access the database of airline companies.
- **PNR data are sent by the airline to the PIU of the EU country concerned** [Article 8]
- When necessary and relevant, an EU country must supply PNR data on an identified person to the competent authorities of another EU country.
- PNR data may be transferred to a **non-EU country under certain specific conditions**.

Storage

- Data provided by airline carriers must be stored in a database by PIU for **5 years from the time of its transfer** to the EU country in which the flight is landing or departing [Articles 12, 13].
- **After 6 months the transferred data must be 'depersonalised'** to mask out certain information including; name; address and contact information; all payment information including billing address [Article 12].
- Disclosure of the full PNR information after this 6-month period has expired is only permitted if: it is reasonably believed to be necessary in order to respond to requests for PNR data made by competent authorities or Europol — on a case-by-case basis and; it has been approved by a judicial or other national authority competent under national law to verify whether the conditions for disclosure are met [Article 12].

General provisions: The Directive applies to extra-EU flights (Article 1). However, a Member State can also apply this Directive to intra-EU flights if they notify the Commission in writing (Article 2). Where a notification is given, all the provisions of this directive then apply to intra-EU flights and to PNR data from intra-EU flights as if they were extra-EU flights and extra-EU PNR data. PNR is defined as (Article 3)

> *"a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, departure control systems used to check passengers onto flights, or equivalent systems providing the same functionalities".*

Responsibilities of the Member States: Each Member State has to produce a list of the competent authorities that can work with PNR data (Article 7). Air carriers are obligated to transfer data to the PIU's of the respective Member State(s) (Article 8). In case advance passenger information (API; see more information below) data is available from air carriers (Annex I), these have to be transferred too. The PNR data has to be transferred electronically and within 24 to 48 hours before the scheduled flight departure time. Exchange of PNR data between Member States can also happen if a response to a specific and actual threat related to terrorist or other serious criminal offences is necessary (Article 9). Europol can request PNR data for the performance of its tasks but only on a case-by-case basis (Article 10). PNR data can be transferred to third countries on a case-by-case basis for the purpose of preventing, detecting, investigating and prosecuting criminal offences and if there are appropriate safeguards in place (Article 11). Passengers have the rights of access, rectification, erasure,

restriction and the right for compensation (Article 13). The PIU has to keep records of the processing for about five years as well.

The EU has until now concluded PNR agreements with Australia[115] and the United States[116] that allow air carriers to transfer PNR data to these third countries (EC: Passenger Name Record (PNR)), while a PNR agreement with Canada is pending[117].

Advance Passenger Information System (APIS)

As opposed to PNR, which contains information described in the above, such as travel dates and itinerary, ticket information, means of payment used etc., the APIS is an *"electronic data interchange system"* (U.S. Customs and Border Protection: Advance Passenger Information System Fact Sheet) allowing carriers the transmission of the following kind of passenger data to border control authorities (EC: advance passenger information (API)):

> *"the number and type of travel document used, nationality, full names, the date of birth, the border crossing point of entry into the territory of the Schengen Member States, mode of transport, departure and arrival time of the transportation, total number of passengers carried on that transport, the initial point of embarkation"*

The data is handed to the authorities after the passengers' check-in. API data can be retained after a flight's arrival for 24 hours, but cannot be exchanged between Member States. Upon request, also law enforcement authorities can have access to API data (EC: EU information management instruments).

In 2017, the AIRE (Airlines International Representation in Europe) suggested the EU to implement an interactive Advance Passenger Information (iAPI) System, which should allow for a validation of a passenger's acceptance to travel into the EU, and specifically provide *"a single interface for API data submission, EES and ETIAS validation"* (AIRE: EU Smart Borders Package Entry-Exit System / ETIAS / API).

3.3.1.6 European Dactyloscopy (Eurodac)

Regulation (EU) No 603/2013[118] regulates the access to the EU database of the fingerprints of asylum seekers by law enforcement authorities in order to prevent, detect or investigate serious criminal offences. The key points of the regulation are summarized below (EU:

[115] **Agreement** between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service

[116] **Agreement** between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security

[117] For more information see https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3220284

[118] **Regulation (EU) No 603/2013** of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice

Eurodac: European system for the comparison of fingerprints of asylum applicants (Summary)).

What does the Regulation do?

It expands Eurodac, which is an EU-wide biometric database containing fingerprints of asylum applicants and non-EU/EEA[119] nationals for comparison between EU countries. The aim is to [Article 1]:

- make it easier for EU countries to determine responsibility for examining an asylum application by comparing the fingerprints of asylum applicants and non-EU/EEA nationals against a central database; and
- enable law enforcement authorities, subject to strict conditions, to consult Eurodac for the investigation, detection and prevention of terrorist of serious criminal offences [Articles 5, 6].

Each EU country must take the fingerprints of all asylum applicants and those apprehended while trying to cross a border irregularly (e.g. non-EU/EEA nationals or stateless persons entering without valid documents) over the age of 14 and, within 72 hours, transmit the data to Eurodac [Article 14]. When an asylum-seeker or non-EU/EEA national has been found to be present illegally in an EU country, then that EU country can consult Eurodac to determine whether the individual has previously applied for asylum in an EU country or has previously been apprehended when trying to unlawfully enter the EU [Chapter IV]. Fingerprint data should be erased once asylum applicants, non-EU/EEA nationals or stateless persons obtain citizenship of an EU country [Recital 23, Article 13]. This regulation allows national police forces and Europol to compare fingerprints linked to criminal investigations with those contained in Eurodac [Article 1]. However, due to the fundamental right to privacy, law enforcement agencies are only allowed to use Eurodac for comparisons [Recital 31; Articles 20, 21]:

- if there are reasonable grounds that doing so will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence; and
- only as a last resort after several other checks have been carried out first.

No Eurodac data may be shared with non-EU countries.

3.3.1.7 European Criminal Records Information System (ECRIS)

Council Decision 2009/316/JHA[120] set up the European Criminal Records Information System (ECRIS) whilst the Council Framework Decision 2009/315/JHA[121] regulates the exchange of criminal records between Member States (EC: European Criminal Records Information System (ECRIS)). The key points of the Council Framework Decision are summarized in the following (EU: Exchange of information on criminal records between EU countries (Summary)).

Objectives

The objectives of the framework decision are to [Article 1]:

[119] EEA (European Economic Area): Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom, Iceland, Norway and Liechtenstein.

[120] **Council Decision 2009/316/JHA** of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA

[121] **Council Framework Decision 2009/315/JHA** of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States

- set an obligation for an EU country convicting a national of another EU country to transmit information on such conviction to the country of his nationality;
- define the obligations of the EU country of which the person is a national to store the received information on convictions as well as the procedures which that EU country is to follow when replying to requests for information about its nationals;
- establish a set of rules for the development of a computerised system of exchange of information on convictions.

Designation of authorities

EU countries must designate central authorities to carry out the tasks related to the exchange of information [Article 3].

Registration of convictions and storage information

A convicting EU country must register the nationality(ies) of the person convicted [Article 4] and notify the EU country(ies) of his/her nationality about details of the conviction, including information on [Article 11]:

- the convicted person;
- the nature and content of the conviction; and
- the offence that led to the conviction.

The EU country of which the convicted person is a national must store information sent to it in order to reply to requests for information on convictions of its nationals [Article 7].

The reply should:

- include information on convictions on its territory, in other EU countries and non-EU countries [Article 7] and
- be done within 10 working days, or 20 if the request was made by a person concerning their own criminal record [Article 8].

Exchanges of information [Article 11]

- The information can be exchanged for the purpose of criminal proceedings or for any other purposes, e.g. pre-employment screenings. While the replies to requests for the purpose of criminal proceedings are obligatory, those for other purposes should be done in accordance with national law.
- When a central authority of an EU country receives a request for information from any relevant national authority, it may in turn ask for information from another EU country, in particular from the country of nationality of the person concerned.
- When a central authority of an EU country receives a request from a national of another EU country regarding their own criminal record, it must ask for information from the EU country of his/her nationality and include them in the issued certificate.

Recently, a regulation has been proposed[122] that will extend ECRIS (exchange of criminal record information) to ECRIS-TCN, which will allow authorities to identify which other Member States hold criminal records on the third country nationals (TCNs) being checked (eu-

[122] **COM(2017) 344 final**: Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRISTCN system) and amending Regulation (EU) No 1077/2011

LISA: ECRIS-TCN). They can then use the existing ECRIS system to address requests for conviction information only to the identified Member States.

3.3.1.8 Customs Information System (CIS)

Council Regulation 515/97 [123] sets up a Customs Information System (CIS), a common computer network managed by the customs administrations of the Member States and the Commission. It is a central database which can be accessed via terminals, in order to handle breaches of Community customs or agricultural legislation (Articles 24, 27). Data and information are disseminated quickly, allowing the system to exchange data on goods moving between EU and non-EU countries. The following summary points out the most important key aspects of the CIS, indicating the corresponding regulation articles (EU: CIS system (Summary)):

The conditions on the use of information technology within customs are strictly defined. As such, the data entered into the CIS shall only be related to [Article 24]:

- goods;
- means of transport;
- businesses;
- people;
- trends in fraud;
- available competencies;
- goods detained, seized or confiscated;
- cash detained, seized or confiscated.

Access to the data in the CIS

Only the authorities designated by the Member States and the Commission have direct access to the data contained in the CIS. These authorities are designated after a list has been sent to the Commission, which also details specific conditions regarding each authority's access to the data [Article 29].

International or regional organisations can access the CIS by special dispensation [Article 29]. In exceptional circumstances, certain data can be sent to other national authorities or to third countries [Article 30].

Data protection

The CIS contains data only, including that of a personal character[124], necessary to achieve the system's objective and which are provided by measures such as sighting, surveillance, specific checks and operational analysis[125] [Articles 25, 27].

---

[123] **Council Regulation (EC) No 515/97** of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs or agricultural matters

[124] Personal data (EU: CIS system (Summary)): *"any information regarding a physical person, identified or identifiable (this means it could be identified either directly or indirectly, in particular by an identification number or by elements specific to his physical, physiological, psychological, economic, cultural or social identity)."*

[125] Operational analysis (EU: CIS system (Summary)): *"the process of analysis of operations which constitute, or appear to constitute, breaches during many phases such as the collection of information, evaluation of the reliability of the information, the linking of information, as well as the formulation of*

The personal details which can be entered into the CIS are detailed in a limited list [see details below]. They are only entered if there are real indications that the person concerned has breached, is breaching or will breach customs or agricultural legislation. Any person has the right to access the data concerning them to check that they are accurate and what is being made of them. This information could be used in legal proceedings [Article 45].

The data in the CIS is confidential and may only be reproduced for technical reasons such as in cases justified by the information search [Article 45]. On the authorisation of the authority that entered them, personal data can be transmitted to systems of risk management used for national customs controls or to operational analysis systems used at Community level.

Customs Files Identification Database

The Customs Files Identification Database (FIDE)[126] is a database which has been added to the CIS to facilitate investigations carried out by the Commission and the national competent authorities. It brings together files relating to persons and businesses that have been suspected of or found guilty of offences.

The personal data to be included in the CIS (excluding for the categories trends in fraud and available competencies) should be no more than name and surname; date and place of birth; nationality; sex; particular physical characteristics; reason for inclusion of data; suggested action; warning code (if armed, violent or escaping); registration number of mean of transport. Furthermore, *"personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and data concerning the health or sex life of an individual shall not be included"* in all the cases (Article 25).

3.3.1.9 Europol Information System (EIS)

Council Decision 2009/371/JHA[127] established the Europol Information System (EIS), which is Europol's (see 3.3.2.2) central criminal information database that is available in all EU Member States[128]. It contains information on persons that are suspected of having committed or having taken part in criminal offences and on persons who are thought to believe that they will commit criminal offences (Articles 10-13). In particular, information includes names, date and place of birth, nationality, sex, place of residence, profession and whereabouts of the person, social security numbers, driving licenses, identity documents, and other characteristics (where necessary). Europol and the Member States can use the EIS to store and query the data on a case by case basis (there might be limitations).

recommendations aimed at identifying persons or businesses implicated and/or to detect other offences."

[126] For more information on The Customs Files Identification Database (FIDE) see: https://ec.europa.eu/anti-fraud/sites/antifraud/files/docs/body/98_fide.pdf

[127] **Council Decision 2009/936/JHA** of 30 November 2009 adopting the implementing rules for Europol analysis work files

[128] For more information see: https://www.europol.europa.eu/activities-services/services-support/information-exchange/europol-information-system

3.3.1.10 Interpol Criminal Information System (ICIS)

INTERPOL is a network of police forces from 190 countries all over the world that helps these countries to work together to solve cross-border crimes via alert messages ('notices') (INTERPOL: Databases). INTERPOL possesses a number of databases that cover all types of evidence (e.g. individuals, forensic data, travel and official documents, stolen property, and firearms trafficking). The Interpol Criminal Information System (ICIS) contains information collected by police organisations (e.g. fugitives, suspected criminals, persons linked to or of interest in an ongoing criminal investigation, persons and entities subject to UN Security Council Sanctions, potential threats, missing persons and dead bodies).

3.3.2 Operational cooperation[129]

This chapter introduces European Agencies that are relevant for border security and management.

3.3.2.1 European Border and Coast Guard (Frontex)

Regulation (EU) 2016/1624[130] sets up a European Border and Coast Guard to ensure European Integrated Border Management (IBM) at external borders of the EU as well as of the Schengen associate countries (Iceland, Norway and Switzerland), addressing *"migratory challenges and potential future threats at those borders"* (Article 1). The key points of the regulation are summarized below, indicating the respective regulation articles (EU: European Border and Coast Guard (Summary)).

The European Border and Coast Guard consists of the European Border and Coast Guard Agency ('the Agency'), created on the basis of the existing EU borders agency (commonly known as Frontex[131],[132]), and the EU countries' and Schengen associate countries' authorities responsible for border management. It also extends and strengthens Frontex's mandate [Article 3].

Main tasks of the European Border and Coast Guard

The main task of the European Border and Coast Guard is to work towards a **European integrated border management (IBM)** as a shared responsibility of the Agency and the national authorities responsible for border management. The main actions of the Agency are to [Article 8]:

- contribute to the **effective functioning of border control** at the relevant external borders, including actions to facilitate legal border crossings and the detection of cross-border crime, such as migrant smuggling or human trafficking;
- provide technical and operational assistance to the participating countries through **joint operations** and **rapid border interventions**;

[129] For more information see: https://ec.europa.eu/home-affairs/what-we-do/agencies

[130] **Regulation (EU) 2016/1624** of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC

[131] Established in: **Council Regulation (EC) No 2007/2004** establishing a European Agency for the Management of Operational Cooperation at the External Borders

[132] For more information about the agency see: https://frontex.europa.eu/

- provide technical and operational assistance in the support of **search and rescue operations for persons in distress at sea**, which may arise during border surveillance operations at sea;
- provide an analysis of the risks for **internal security** as well as of the threats that may affect the functioning or **security of the EU's external borders**;
- **cooperate with non-EU countries and non-Schengen associate countries**, focusing on neighbouring countries and countries of origin and/or transit for irregular immigration;
- carry out a vulnerability assessment including the assessment of the capacity and readiness of the participating countries to face threats and challenges at the external borders;
- organise, coordinate and conduct **return operations** and interventions.

Monitoring of migration flows and risk analysis

The Agency contributes to ensuring that **EU standards to protect and enforce border management** are implemented at all external borders. EU countries' and Schengen associate countries' external borders will constantly be monitored by means of **risk analysis** and **mandatory vulnerability assessments** to identify and address weak spots [Recital 20, Article 11].

EU border and coast guards

A rapid reaction pool of at least **1 500 border and coast guards** and a technical equipment pool are to be ready to react to any kind of pressure of illegal migration at the external borders [Recital 29, Articles 14, 20]. Where necessary, the deployment of European Border and Coast Guard teams from the reaction pool will be immediately supplemented by additional border guards from EU countries.

Processing of personal data

The Agency is permitted to process personal data only for the purpose of risk analysis, [identifying / tracking vessels, administrative tasks,] organising operational activities including joint operations, rapid border interventions, return operations and return interventions, and transmission to the competent national authorities or EU agencies, such as EASO, Europol and Eurojust [Articles 46, 47]. The Agency will manage the personal data of persons suspected of involvement in criminal activities, such as migrant smuggling, human trafficking and terrorism [Article 47].

European Border and Coast Guard: There are 11 main components of the IBM (Article 4):

- border control[133]
- search and rescue operations for persons in distress at sea[134]
- risk analysis for internal security and external borders
- cooperation between Member States (supported and coordinated by the Agency)
- inter-agency cooperation among the national authorities[135]
- cooperation with third countries[136]

[133] incl. measures to facilitate legitimate border crossings, measures related to the prevention and detection of cross-border crime (e.g. migrant smuggling, trafficking in human beings and terrorism), and measures related to the referral of persons who are in need of, or apply for international protection

[134] In accordance with **Regulation (EU) No 656/2014** of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union

[135] inclusive the regular exchange of information through existing information exchange tools, such as the European Border Surveillance System ('Eurosur', see 3.3.2.1.1);

[136] focusing in particular on neighbouring countries and on those third countries which have been identified through risk analysis as being countries of origin and/or transit for illegal immigration

- technical and operational measures within the Schengen area
- return of third-country nationals who are the subject of return decisions issued by a Member State
- use of state-of-the-art technology (large-scale information systems)
- a quality control mechanism (Schengen evaluation mechanism[137])
- solidarity mechanisms (Union funding instruments)

European Border and Coast Guard Agency: The European Border and Coast Guard Agency replaces the name for the European Agency for the Management of Operational Cooperation at External Borders (commonly known as Frontex[138]) (EU: European Border and Coast Guard (Summary)). The Agency's tasks are: monitor migratory flows (also Articles 9-11) and the management of external borders through liaison officers (Articles 12, 55); carry out risk analysis (also Articles 9-11) and vulnerability assessment (Article 13) of external borders; assist Member States by organising joint operations or by launching rapid border interventions (also Articles 15-17); provide technical and operational assistance to Member States and third countries; set up and deploy European Border and Coast Guard teams and technical equipment (also Articles 14, 20-26, 38-43); help in return operations and interventions (also Article 27-33); cooperate with Europol and Eurojust and others (also Articles 52-55); assist Member States with training of border guards (also Articles 36); participate in research regarding external borders (also Article 37); develop and operate information systems that allow information exchanges (also Article 44); and provide assistance in developing and operating Eurosur (see 3.3.2.1.1) (Article 8).

General provisions: Fundamental rights have to be protected by the European Border and Coast Guard. Particular attention has to be paid to children's rights (Article 34). The transfer of personal data from the Agency towards Member States or third countries is prohibited (Article 45). Data processing has to be limited to the necessary purposes for the tasks (Article 46). The Agency can only process personal data regarding suspected persons of crime, persons who cross borders illegally, and license plate numbers, vehicle identification numbers and phone numbers collected during joint operations, pilot projects and rapid border interventions and by migration management support teams (Article 47). Personal data has to be deleted once it has been transmitted to EASO, Europol or Eurojust – in any event, the storage period must not exceed 90 days after the collection of the data. The processing of personal data in the context of return operations and interventions has to be limited to the purposes and deleted as soon as the purpose is completed but no later than 30 days after the end of the operation or intervention (Article 48). The Agency can transfer such data. The agency can process personal data in the context of Eurosur (see 3.3.2.1.1). The Agency is a body of the Union and hence has legal personality (Article 56).

[137] As well as possible national mechanisms in order to ensure the implementation of Union legislation for border management

[138] Established in: **Council Regulation (EC) No 2007/2004** establishing a European Agency for the Management of Operational Cooperation at the External Borders

3.3.2.1.1 Eurosur

Regulation (EU) No 1052/2013 [139] established the European Border Surveillance system (Eurosur) (EU: European border surveillance system (Eurosur) (Summary)). Frontex cooperates with EU Member States via this multipurpose system to improve situational awareness and increase reaction capability at external borders with the aim to prevent cross-border crime and irregular migration. Hence, Eurosur allows Member States to rapidly exchange information.

3.3.2.1.2 Copernicus

Frontex also provides geospatial information collected from satellites via Copernicus[140] for border surveillance (EC: Security Service). Regulation (EU) No 377/2014 [141] established Copernicus, which is a programme that allows increasing situational awareness in Europe by providing satellite data about security (also includes atmosphere, marine, and land monitoring as well as climate change, and emergency management). The service for security improves crisis prevention and helps with border and maritime surveillance.

3.3.2.2 Other agencies

- **Europol:** Europol[142] is the EU's law enforcement agency that supports the Members in fighting terrorism, cybercrime and other forms of crime[143,144].
- **Cepol:** Cepol[145] is the EU's agency for law enforcement training that is dedicated to develop, implement and coordinate the training of law enforcement officials[146].
- **eu-LISA:** eu-LISA[147] is EU's large-scale IT system that operates Eurodac, SIS II, VIS and will operate ETIAS and EES (eu-LISA – managing IT systems in the field of border and migration controls (Summary)).

---

[139] **Regulation (EU) No 1052/2013** of the European Parliament and of the Council of 22 October 2013 establishing the European border surveillance system (Eurosur)

[140] For more information see: https://www.copernicus.eu/en

[141] **Regulation (EU) No 377/2014** of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010 Text with EEA relevance

[142] For more information see: https://www.europol.europa.eu/

[143] **Council Decision** of 6 April 2009 establishing the European Police Office (Europol)

[144] **Regulation (EU) 2016/794** of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

[145] For more information see: https://www.cepol.europa.eu/

[146] **Regulation (EU) 2015/2219** of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA

[147] For more information see: https://www.eulisa.europa.eu/

- **EMCDDA:** EMCDDA[148] provides the EU an overview of the drug situation in Europe[149].
- **Eurojust:** Eurojust[150] supports cooperation to combat terrorism and serious organised crime that affect more than one EU Member State[151].

3.4 European agenda on security

The EU face several new and complex security threats which highlight the need for closer cooperation between Member States at all levels (EC: European Agenda on Security). For this reason, security has been made a key priority within the EU (EC: Security Union – A Europe that protects). The European agenda on security defines how the Union can help Member States to ensure security, prioritising terrorism, organised crime and cybercrime across borders. It aims at strengthening tools that are already in place and at continuously improving information exchanges and operational cooperation (EC: Strengthening the EU's external borders).

Thirty legislative initiatives have been presented since the Juncker Commission (EC: Security Union – A Europe that protects; EP: The Juncker Commission's ten priorities). Of these, eight have been adopted and 22 are still on the table and need to be adopted. For example, concerning the sharing of information regarding external borders, the following proposals have been on the table since 2016/2017:

- Amendment to European Criminal Records Information System (ECRIS)
- Upgrade of European Criminal Records Information System (ECRIS-TCN system)
- Revision of Eurodac system
- Reinforced Schengen Information System
- Stronger mandate of the eu-LISA Agency
- Interoperability between EU information systems for security, border and migration

Concerning the protection of borders, the following proposals have been on the table since 2017/2018:

- Revision of the rules for temporary reintroduction of border control at internal borders
- Reinforced European Border and Coast Guard

Four initiatives have already been adopted by the European Parliament and the Council: European Border and Coast Guard Agency, Systematic checks against relevant databases, Entry/Exit System (EES), and ETIAS.

3.5 Pilot cases

The following sections discuss legal and regulatory aspects pertaining to the TRESSPASS pilot cases based on inputs provided by consortium partners. The information presented does not

[148] For more information see: http://www.emcdda.europa.eu/

[149] **Regulation (EC) No 1920/2006** of the European Parliament and of the Council of 12 December 2006 on the European Monitoring Centre for Drugs and Drug Addiction

[150] For more information see: http://www.eurojust.europa.eu/Pages/home.aspx

[151] **Regulation (EU) 2018/1727** of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA

constitute a detailed review of all national laws pertaining to the pilot cases and will have to be evaluated in detail during the preparation of the pilots to realise them within the given legal boundaries. For every participating Member State, a general legal overview is given, yet when more details regarding the pilots are clear, a specific legal overview for each pilot should be made.

3.5.1 The Netherlands

The Netherlands share land borders with Germany in the east and Belgium to the south. Northwest the country is surrounded by the North Sea. Additionally, three Caribbean island territories Bonaire, Sint Eustatius, and Saba belong to the Netherlands' administrative structure as municipalities and Sint Maarten, Curaçao and Aruba as autonomous countries within the Kingdom of the Netherlands. Thus, the country also shares maritime borders with France and the United Kingdom (Nations online: Netherlands).

The pilot case within the TRESSPASS project is the Amsterdam Airport Schiphol. It is one of the biggest airports in Europe and transferred more than 63 million passengers in 2016 (Schiphol: Amsterdam Airport Schiphol Airport Facts). About 40% have crossed the border, about 38% were in transfer and about 22% travelled intra-Schengen.

3.5.1.1 Border control

Border control in the Netherlands is performed by the Royal Netherlands Marechaussee (RNLM) [152], by order of the Ministry of Justice and Security. The RNLM is a military police force. Its tasks involve, for example, combatting cross-border crime and terrorism, drug trafficking, identity fraud as well as people smuggling[153].

The RNLM performs travel document checks at airports, seaports, along the coast, on roads and in trains in order to combat, for example, illegal immigration. With Mobile Security Monitoring (Mobiel Toezicht Veiligheid/MTV), people travelling from another Schengen country to the Netherlands either via the Belgian or the German border are being monitored. RNLM uses the @migoboras camera system as a tool for mobile checks.

RNLM participates in Frontex, the European border control agency (3.3.2.1) [154] and thus contributes to the control of Europe's external borders in other EU member states. Migration control dogs are used in order to find concealed persons in trucks, cars, busses as well as ships and cargo etc.

At Schiphol Airport, RNLM receives Advance Passenger Information (API) data for all incoming flights from outside the EU. These data are automatically compared to watchlists and profiles, hits become alerts and are directed to the operations. Then, a follow up takes place in the

[152] For more information see: https://english.defensie.nl/topics/border-controls and https://english.defensie.nl/organisation/marechaussee/tasks-of-the-royal-netherlands-marechaussee

[153] Tasks of the RNLM are regulated in Article 4 of the **Police Act 2012**: https://wetten.overheid.nl/BWBR0031788/2018-09-19#Hoofdstuk2 and in Article 5 of the **Safety (BES Islands) Act 2012**: https://wetten.overheid.nl/BWBR0028586/2018-08-01#Hoofdstuk2

[154] For more information see: https://frontex.europa.eu/

operation, for example by means of a Dedicated Gate Control, if the risk assessment is judged as high. All border crossing points at the airport have e-gates as well as manual control booths, and the airport is monitored by surveillance cameras.

With regard to current and future challenges, Schiphol Airport and RNLM have taken initiative to further streamline the passenger flow process and developed the "seamless flow-concept", where the passenger is identified with a biometric token, by which he can move through all airport processes. However, this means that certain information should be available before a passenger arrives at the airport. The idea is to classify passengers on the basis of information received before arrival at the border crossing point, into three categories: "no or acceptable risk" (green), "unknown risk" (orange) and "known risk" (red). Furthermore, a passengers' behaviour at the airport and updated information on the passenger should be incorporated into the final risk assessment as well.

3.5.1.2 Immigration

On the basis of article 4 of the Police Act, the RNLM carries out multiple tasks derived from the Dutch Aliens Act, such as border control.

Access to the Netherlands: As an EU country, the Netherlands apply the Schengen Borders Code (3.2.1). However, in cases other than those regulated by the Schengen Borders Code, entry to the Netherlands is denied for individuals not fulfilling certain requirements, e.g. no valid travel document, posing a threat to national security, no sufficient means to provide for themselves etc. (Article 3). The carrier bringing an individual to a Dutch border may be required to take a copy of the alien's border-crossing document or collect passenger data and hand it over to officials in charge of border control (Article 4). If an alien is denied entry into the Netherlands, he / she has to leave the country (with the means of transport used to enter, if a vessel or aircraft) (Article 5). Aliens who cannot return or are waiting for an application to be processed, are to be staying in a room designated by an officer in charge (Article 6).

Establishing an alien's identity: Officials in charge of border surveillance are competent to retain persons to establish their identity and residence status, and are authorized to investigate the clothing and body of the person held, as well as to search his belongings (Article 50). If reasonable suspicion arises that persons are transported by means of transport with regard to which the officers in charge of border control have a supervisory task, the means of transport (such as vehicles, vessels, aircrafts etc.) can be examined (Article 51). Travel and identity documents can be taken into custody, however are returned to the alien if he wishes to leave the Netherlands and does so (Article 52).

Biometrics, data provision and processing: A facial image and ten fingerprints may be collected from foreigners other than Community nationals[155] (EU nationals) and compared to facial images and fingerprints in the foreigners administration database ("vreemdelingenadministratie") (Article 106a). The foreigners administration entails and

[155] Community nationals (as defined in Aliens Act 2000): nationals of the Member States of the European Union and their family members who are entitled to enter and reside in a Member State; nationals of a State party to the Agreement on the European Economic Area of 2 May 1992 who have the same rights than EU citizens and their family members who are entitled to enter and reside in a Member State; citizens of the Swiss Confederation and family members who are entitled to enter and reside in a Member State

processes a) facial images and fingerprints, b) other personal and referral data of identified and registered foreign nationals and c) other data, including personal data that are important for the implementation of the Aliens Act 2000 and the Kingdom Act on Dutch citizenship (Article 107). The data has to be destroyed seven years after entry into force of the Act of 11 December 2013 amending the Aliens Act 2000 (expansion of biometric features) (Article 115).

3.5.1.3 Information exchange

Besides the GDPR (3.1.2) which is applicable in the Netherlands, the Dutch laws Wpg (Police Data Act)[156] and Wiv (Intelligence and Security Services Act)[157] are of interest as well regarding the topic of information exchange. The Wpg is applicable when personal data is being processed with regard to all the tasks noted in Article 4 of the Police Act, except the tasks being carried out under the Aliens Act. These are specified as follows (ICLG: Data Protection 2018 – Netherlands):

> *"The Police Data Act (Wet politiegegevens) (…) regulates the processing of personal data carried out by the National Police, the special investigative bodies, the Royal Netherlands Marechaussee and the National Department of Criminal Investigation. It also applies to the tasks that the police carry out for judiciary purposes (…))."*
>
> *"[T]he intelligence and security act (Wet op de inlichtingen – en veiligheidsdiensten) (…) extends the powers of the Dutch general safety and intelligence agency and of the military intelligence and safety agency (…)."*

The Wpg (Police Data Act) states that police data are only to be processed for the purposes set out by the act (Article 3). They have to be lawfully obtained, and processed only if adequate, relevant and not excessive, and their origin and method of acquisition have to be stated. Data can only be processed for certain specific purposes (Articles 8, 9, 10, etc.).

Special categories of personal data, such as data on a person's religion / belief, race, political opinion, trade union membership, health or sexual life, are only processed in addition to other police data and if it is inevitable for the purpose of the processing (Article 5).

The provision of police data to entities other than the police and the RNLM is regulated in Articles 16 to 24. Data may be provided to, for example, members of the public prosecution service, mayors, the Chief of Police, the Board of Procurators General, the Minister of Security and Justice or the Minister of Defense[158] (Article 16). International bodies, criminal courts, authorities responsible for carrying out police tasks in Europe, as well as third countries may be provided with data for the purposes of prevention, control, investigation and prosecution of serious crime (Articles 15a and 17a). However, an adequate level of protection for data processing must be ensured by the receiving parties. Furthermore, data may be shared with third parties structurally or incidentally for the purposes of prevention and detection of criminal offences; maintaining public order; providing assistance and supervising compliance with regulations (Articles 18 and 19).

---

[156] Police Data Act. For more information see: https://www.ns.nl/en/privacy/law-on-policedata.html

[157] Law on intelligence and security services 2017. For more information see: https://pilpnjcm.nl/en/dossiers/bill-intelligence-security-services-act-wiv/

[158] the Chief of Police, the Board of Procurators General, the Minister of Security and Justice or the Minister of Defense

Within the framework of information-led or risk-based border management, information exchange thus would take place between border police organisations and intelligence services, such as the General Intelligence and Security Service. However, the specific legal obligations and restrictions of the respective laws have to be taken into account.

3.5.2 Poland

Poland has joined the European Union in 2004, and is a member of the Schengen area since December 2007 (EU: Poland). The country shares land borders with Russia (Kaliningrad), Lithuania, Belarus, Ukraine, Slovakia, Czechia, and Germany. In the north, the country is bordered by the Baltic Sea. Of these countries, Lithuania, Slovakia, Czechia and Germany are members of the European Union and the Schengen area as well, meaning that the land borders with Poland are no longer in use. Border control is thus carried out on the borders with Russia (Kaliningrad), Belarus and Ukraine.

At the external land border crossing point, the vast majority of passengers and goods arrive by railway, as pedestrians or in vehicles (cargo, buses, cars). Statistics show a steady increase in the number of travellers crossing the Polish border, while the nationalities of travellers differ. The majority of travellers are Ukrainian, Russian or Belarusian citizens, which are all third country nationals in respect of the Schengen Agreement and require visas in order to travel into the EU. However, the group of frequent travellers constitutes about 80% of all border crossings.

Challenges for the land border risk-based screening in the case of Poland are the high volumes of traffic, as well as cross-border smuggling (alcohol, drugs, etc.), which is particularly difficult to detect due to constantly changing patterns and means of hiding the illicit goods. Document forgeries are another challenge; this applies to freight transport and truck drivers' attempts to forge certificates allowing them to transport hazardous materials, as well as a growing tendency to forge passport stamps, on the basis of which border officers are able to establish how long an individual stayed in the territory of the EU/Schengen zone. A bottleneck is the customs control, which is conducted separately after the passport control. Hence, potential threats posed by car, truck or train passengers travelling with stolen or false ID and vehicle documents have to be identified and mitigated, in order to enhance security on land border crossings itself and neighbouring areas. Furthermore, interoperability between Border Guards should be promoted. Yet, data privacy and protection have to be preserved, taking into account the growing importance of legal, ethical and social aspects.

3.5.2.1 Border control[159]

Crossing the Polish state border is only permissible at designated border crossings. Border control is carried out by uniformed officers of the Border Guard Service (Polish *Straż Graniczna*, SG). The Border Guard is in charge of preventing illegal border crossings and crimes, counteracting cross border smuggling of explosives, arms, radioactive materials, dangerous chemicals, security controls of passengers and luggage, postal deliveries etc., maintenance of public law and order around border crossing points, securing major public

[159] For more information see: http://www.migrant.info.pl/Border_crossing_procedures.html and http://antyterroryzm.gov.pl/eng/anti-terrorism/institutions-and-servi/the-border-guard/658,The-Border-Guard.html

events and critical infrastructure, protecting transportation routes, monitoring centers of foreign nationals and their criminal activities, gathering and analysing information on potential terrorist threats as well as cooperating in this regard with the International Security Agency, the Foreign Intelligence Agency, the Police, etc. (Antyterroryzm.gov.pl: The Border Guard). It consists of nearly 4.000 civil workers and almost 15.000 officers who protect one of the longest EU external borders.

A vast majority of travellers passing the Polish borders do so under the local border traffic[160] regime[161] (3.2.2.2.2). This is to facilitate crossing borders for citizens of neighbouring countries living in a frontier area (Migrant info.pl: Local Border Traffic). The local border traffic regime allows for residents of border areas[162] to regularly cross a common state border without a visa, in order to stay in the border area of the second state, for social, cultural or family reasons, as well as for justified economic reasons. Currently, the following two agreements on local border traffic are in force between Poland and (Migrant info.pl: Local Border Traffic):

- *"Ukraine: the border area includes the zone up to 30 km from the shared border,*
- *Kaliningrad region: the local border traffic regime applies to all of the inhabitants on the Russian side of the Kaliningrad region, and on the Polish side to the residents of large parts of Pomerania and Warmia-Mazury voivodships."*

Border area residents, Ukrainian and Russian citizens, receive a so-called permit for crossing the border to Poland within the local border traffic regime. They are allowed to remain in the designated border areas at one time for a period of up to 60 days from the date of entry (Ukrainian citizens) and 30 days (Russian citizens), but the total period of stay cannot exceed 90 days during six months calculated from the date of the first entry. In the respective time frame, permit holders can cross the border as many times as they want (Migrant info.pl: Local Border Traffic).

3.5.2.2 Immigration

As Poland is an EU country, the Schengen Borders Code applies (see 3.2.1). Furthermore, the Polish Act on foreigners[163] regulates border crossing in Poland[164] with regards to foreigners. It

[160] Definition of «local border traffic» in the Polish Act on Foreigners (see below): *"the entry of foreigners into the territory of the Republic of Poland, to whom Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention (OJ UE L 405 of 30.12.2006, p. 1, as amended) applies, and their stay in that territory"*.

[161] See also **Regulation (EC) No 1931/2006** of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention

[162] Border area residents: individuals with documented permanent residence in the border area for a period of not less than 3 years, as well as their spouses and adult and minor children.

[163] Act of 12 December 2013 on foreigners: http://www.asylumlawdatabase.eu/en/content/en-act-12-december-2013-foreigners-poland

[164] A list of border crossing with details regarding the kind of permitted movements through these border crossings and opening hours can be found here: Official Gazette of the Government of the

"lays down the principles and conditions governing entry into, transit through, residence on and departure from the territory of the Republic of Poland as they apply to foreigners, as well as the procedure and the authorities competent in these matters" (Article 1). The Act on foreigners does not apply to members of staff of diplomatic missions and consular posts of foreign states and other persons treated equally and nationals of the EU and EFTA Member States, and the Swiss Confederation as well as their family members (Article 2).

Access to Poland: a foreigner (any person who does not have Polish citizenship) entering Poland should be in possession of a valid travel document; a valid visa or similar document allowing him/her to enter and stay in Poland; a permit to enter or stay in another country, if such a permit is required for transit (Article 23). Foreigners are obliged to justify the purpose and conditions of the stay and be in possession of a document certifying that he/she has health insurance and sufficient financial means to cover the costs of the stay and return or transit to another country[165] (Article 25). Entry to Poland is denied when no valid travel document is available; if the permitted period of stay has been used up; if no sufficient documentation is available on the purpose and conditions of the stay; if he/she does not have sufficient financial means of subsistence regarding the length and purpose of the stay; if personal data of the foreigner appear in the register of foreigners whose stay is undesirable (e.g. SIS); when the foreigners stay could pose a threat to public health or national security (Article 28). This does not apply to foreigners who hold a Schengen visa or have applied for refugee status.

Local border traffic permit: border area residents receive a local border traffic permit if a) they are in possession of a valid travel document, b) they produce documents that prove their status as border residents and prove legitimate reasons to frequently cross the external land border, c) no alert has been issued in the SIS for refusing them entry and d) they are not considered a threat to public health or internal security, and no alert has been issued in a Member States' database (Article 37; Article 9 of Regulation (EC) No 1931/2006[166]). Member States have to keep a register of the local border traffic permits issues or denied and – upon request – provide information on permits entered to other Member States (Article 12 of Regulation (EC) No 1931/2006). For the application, the foreigner has to provide various personal information as well as fingerprints (Article 44).

Data collection of foreigners: Article 13 states the kind of data and information concerning a foreigner that may be processed in registers kept under the Act on foreigners (summarized):

> *name(s) and surname(s); sex; parents name; date, place and country of birth; height in centimetres, colour of the eyes, distinctive features; fingerprints; citizenship, nationality; marital status; education, occupation; national identification number, number of the travel document; identification of the entity ensuring the performance of work; place of residence or stay; phone number, email address; information on criminal records etc.; identification number in the Universal Electronic System for Registration of the Population (PESEL); image of the face;*

Republic of Poland of 2015, item 636 – URL (the document is in Polish): http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20150000636

[165] Exceptions from this requirement are stated in Article 25, Paragraph 3.

[166] **Regulation (EC) No 1931/2006** of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention

information about residing in the territory of another EU Member State for at least 18 months on the basis of a residence permit issued by that state with an annotation ("EU Blue Card"); data of a host.

Regulation OJ 1990 "USTA AWA" [167] about the Border Guard specifies tasks and duties of the Polish Border Guard. Concerning the collection and procession of personal data, border guards may collect and use the following kind of data (Article 10a):

"fingerprints, photographs and personal data for detection and identification purposes, including revealing ethnic origin, religious affiliation and data on health status, people suspected of committing offenses prosecuted against public prosecution, (…) without the consent and knowledge of the data subject".

The data, except for data revealing ethnic origin or religious affiliation[168] has to be kept for a period necessary for the Border Guard to perform statutory tasks and have to be verified at least every 10 years. The Border Guard has direct access to view information on wanted persons[169], and supplementary information provided by the Police on request (Article 10aa), and can further obtain data which does not constitute content such as telecommunications, postal items etc.[170] (Article 10b).

3.5.3 Greece

Greece is, as the Netherlands and Poland, both an EU country and in the Schengen area. It borders in the northwest with Albania, in the north with the Republic of North Macedonia and Bulgaria and to the northeast with Turkey. The rest of the country, with its many islands, is surrounded by the Aegean Sea (east), the Cretan and Mediterranean Sea (south) and the Ionian Sea (west).

In this project, Greece and specifically the Cruise Port of Piraeus serves as the maritime border crossing point, revolving around passengers travelling by cruise ships. Piraeus Port is the largest passenger port in Europe, the biggest and most important in Greece, and besides the handling of cruise and coastal (ferry) passengers, it also hosts cargo handling, ship repair activities, and domestic transfer to the islands as well as environmental and logistics operations (Piraeus Port Authority S.A.: Annual Financial Report 2017; Greek Law Digest: Greek Port Regulations). In 2017, more than one million cruise ship passengers visited Piraeus Port, and more than 15.5 million coastal passengers.

---

[167] Polish legislation, obtained by end-user Poland: **OJ 1990 No. 78 item 462**, "USTA AWA" of October 12, 1990 about the Border Guard

[168] Particular rules apply regarding the storage of personal data revealing the ethnic origin or religious affiliation of persons suspected or convicted of committing offenses prosecuted from public prosecution (Article 10a(4, 5))

[169] as referred to in Art. 20 Para. 2a Point 5 of the Act of 6 April 1990 on the Police (Journal of Laws of 2017, item 2067)

[170] For further details see Article 10b of **OJ 1990 No. 78 item 462**, "USTA AWA" of October 12, 1990 about the Border Guard

Cruise travelling is a relatively new form of transportation and tourism, especially in the Mediterranean. Two types of passengers exist: home and transit passengers, depending on whether they exit the ship permanently to the destination country or they exit the ship for a period of time to visit the country and then board the ship again to continue their cruise. The cruise lines conduct their own security checks on board, e.g. with X-ray machines and magnetic doors. Transit passengers hold a special ship boarding card ID, provided by the cruise company. Ship boarding cards are given to embarked passengers during checks in process at the terminals or on board depending on cruise line handling. All cruise terminals support checking procedures with suitable infrastructure and software technology. Disembarking passengers keep their own boarding card (or not) depending on the cruise line. Non-Schengen passengers go through a control in the first Greek or first EU port, then Schengen applies for the rest of the visiting ports. Dedicated cruise terminals exist for non-Schengen passengers to be served.

Challenging for the Greek maritime use case are the large flows of disembarking passengers. In Piraeus Port at passport checks there could be delays only in the rare case of a system failure. However, as resources and time are restricted, it is not feasible to perform all border and customs controls uniformly on all cruise passengers. Thus, these controls often happen based on an on-the-fly risk analysis approach, following an alert. All cruise terminals in the Port of Piraeus are equipped with X-ray machines for passenger belongings / luggage control and all passenger belongings / luggage are controlled with them before embarkation. Transit passengers are also controlled before embarkation. In every terminal there are also special booths for the passport control handled by the Hellenic Police. On cruise premises the ISPS Code is applied.

One of the objectives within this project is to introduce a Maritime PNR interoperable with the Airlines PNR, in order to provide a common operating platform based on a risk-based screening among all competent authorities. Furthermore, fast border crossing should be introduced, with the TRESSPASS on-the-move identification and verification technology with the logic of a non-disruptive no-gate border crossing while still preserving the data privacy of the passengers.

3.5.3.1 Border control

Border control in Greece is under the responsibility of the Hellenic Police[171]. However, the Hellenic Coast Guard (HCG)[172] plays a key role as well. Especially on the coastal borders they support the Hellenic Police, applying police duties in Greek ports which are characterized as BCPs. The main tasks of the Hellenic Coast Guard are:

- general police duties at the sea and at the port facilities
- marine environment protection
- border surveillance
- fishery control
- maritime security/safety

[171] The role of the Hellenic Police, specifically of the Branch of Aliens and Borders Protection Division, is stipulated in **Law 4249/2014 (Article 18)**

[172] The role of the Hellenic Coast Guard is stipulated in **Law 3922/2011 (Article 2)**

› search and rescue operation

As Greece is located on the crossroad between Europe, Asia and Africa, HCG is specialised in dealing with illegal activities which occur at BCPs, in particular at the ports of Piraeus, Patras and Igoumenitsa.

3.5.3.2 Immigration

The current law on the status of aliens is Law 4251/2014[173] (as amended by Law 4232/2015) dealing with entry, residence and social integration of third-countries nationals and stateless persons (Migration and Social Integration Code) (Greek Law Digest: Foreign Citizens – Immigrants Introduction). It is not applicable for EU citizens, officials of diplomatic as well as consular authorities and beneficiaries of international protection according to the provisions of the 1951 Geneva Convention (Article 2).

Access to Greece: Entry into and exit from Greece is only allowed at controlled border crossing points; under specific conditions however, temporary passing points may be installed. Checks at border crossing points are conducted by local police authorities (Article 3). Third-country nationals entering Greek territory have to hold a passport or another recognized travel document, incl. a visa (Article 6). Entry can be refused if the third-country national poses a threat to public order and security; does not have a travel document that ensures the return to the country of origin or to a third country; does not hold the required visa or residence permit for the purpose of the trip and does not have sufficient resources for sustaining him/herself (Article 4).

Collection of personal data: Law 4251/2014 does not specify which kind of personal data is collected before or upon crossing the Greek border. In specific cases, personal data such as name, date of birth and passport number are collected (e.g. when hiring third-country nationals for employment, Article 14). Furthermore, personal data of third-country nationals who reside in Greece are recorded and processed, however the legislation does not specify which kind of data (Article 133). Regulation (EC) No 810/2009 (Visa Code) stipulates in Articles 13 and 14 which personal data are required before crossing the Greek borders.

3.5.3.3 Customs[174]

End-user IAPR (Greek Customs) provided a legislation overview on the respective Regulations currently in force. The Union Customs Code (Regulation (EU) No 952/2013) specifies in Article 46 risk management and customs controls. Customs authorities can carry out any customs controls that they consider necessary, in particular examine goods, verifying the given declaration, and inspecting means of transport, luggage and other goods persons carry etc. These controls should be based on risk analysis *"using electronic data-processing techniques"*, and be carried out within a common risk management framework. For intra-union flights and sea crossings, customs controls are to be carried out *"only where the customs legislation provides for such controls or formalities"* (Article 49). This applies without prejudice to either *"a) security and safety checks or b) checks linked to prohibitions or restrictions"* (Article 49). In

[173] **Law 4251/2014** Government Gazette 80 / A / 01.04.2014. Immigration and Social Integration Code and other provisions

[174] Greek customs legislation, obtained from IAPR

Greece, the National Customs Code applies (Law 2960/2001[175]). Passengers arriving from a third country are obliged to present their baggage to the Customs Authority of entry when crossing the border, in order to be examined (Article 50).

Controls of goods: Regulation (EU) 2015/2447[176] treats the controls of goods. In Articles 37 to 42 it is stated that airports carry out cabin and hold baggage checks in cases of transit flights (Article 37), transit flights in business and tourist aircraft (Article 38), inbound transfer flights (Article 39), outbound transfer flights (Article 40), transfers to a tourist or business aircraft (Article 41), and transfers between airports on the territory of the same Member State (Article 42). Furthermore, measures to prevent illegal transfer are provided in Article 43. For baggage transported by sea, Article 46 provides for points where customs controls and formalities are carried out on pleasure crafts. Article 47 provides for ports where baggage controls and formalities applicable to the baggage of persons using a maritime service provided by the same vessel and comprising successive legs departing from, calling at or terminating in a non-Union port are carried out.

Controls of cash: Inspections for cash in Greece are based on Regulation (EC) 1889/2005[177] on the control of cash coming into or exiting the Community, and according to which a person entering or exiting the Community and carrying cash of a value equal to or greater than 10'000 euros must declare this amount to the competent authorities of the Member States. According to Article 147(8) of Law 2960/2001[178] failure to declare cash is subject to a fine amounting to 25% of the cash found. If there is a link between the cash and illegal activities, the case is transmitted to the competent prosecution authority, if not, the amount remaining after deducting the fine is returned to the person that was carrying the cash.

3.5.3.4 Port Security

Within the TRESSPASS project, PPA is an end-user, and thus provided a translation of Law 3622/2007[179], which is to define responsibilities and plan and coordinate national actions in order to ensure the implementation of Regulation (EC) 725/2004 [180] and the Directive 2005/65/EC[181] (3.2.3.3) on enhancing the security of ships, port facilities and ports. The scope of the law includes various types of ships engaged on international voyages, such as

[175] **Law 2960/2001**, Government Gazette 265 A. National Customs Code

[176] **Commission Implementing Regulation (EU) 2015/2447** of 24 November 2015 laying down detailed rules for implementing of certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code.

[177] **Regulation (EC) No 1889/2005** of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community

[178] **Law 2960/2001**, Government Gazette 265 A. National Customs Code

[179] **Law 3622/2007** – Government Gazette 281 / A ' / 20.12.2007. Enhancing the security of ships, port facilities and ports and other provisions.

[180] **Regulation (EC) No 725/2004** of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (Text with EEA relevance)

[181] **Directive 2005/65/EC** of the European Parliament and of the Council of 26 October 2005 on enhancing port security (Text with EEA relevance)

passenger ships, cargo ships and mobile offshore drilling units, companies of ships, as well as port facilities (Article 3).

The Ministry of Shipping and Island Policy (former Ministry of Mercantile Marine, the Aegean and Island Policy) coordinates, supervises, and monitors compliance with the procedures and the implementation of security measures, while the Port Safety Authority drafts and implements port security plans (Article 4(1), (2)). In addition, the Ministry appoints a Port Security Authority and a Port Security Officer (Article 4(2)).

Ship operators have to make sure to carry out a safety assessment of their shops and port facilities, and implement the safety plans complying with the provisions of the ISPS Code (Article 5(1)). It is also possible that port operators assign security controls (incl. checks on persons, baggage and cargo etc.) to private security companies (with a lawful permit) (Article 5(3)).

4 SUMMARY AND CONCLUSIONS

As described in TRESSPASS Deliverable D9.6, *"the introduction of risk-based border management is a modification of* how *the purposes of border checks are to be attained, i.e. it is a modification of the ways in which the two main functions of border checks* [access and egress control function and revelatory function] *are meant to be applied."* This chapter summarises the legal and regulatory framework, further illustrating legal boundaries to the implementation of risk-based border management approaches through a discussion of the guiding key research questions. A summary of chapter 3 is presented, however, please note that indirect citations were omitted and refer back to chapter 3 for them. Finally, possibilities for refining the risk-based border control concept of TRESSPASS according to current legal standards are discussed.

4.1 Summary of legal and regulatory framework

4.1.1 Privacy and data protection

Data protection is primarily regulated in three legislative documents:

- Regulation (EU) 2018/1725[182]: Processing of personal data by the Union institutions, bodies, offices and agencies and of the free movement of such data;
- Regulation (EU) 2016/679 (GDPR) applies to the processing of personal data and the free movement of such data; and
- Directive (EU) 2016/680 applies to the processing of personal data by police and criminal justice authorities.

The GDPR's main principles are the following (GDPR, Article 5):

- **(a) Lawfulness, fairness and transparency:** "*Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*". Hence, valid legal grounds have to be identified for the use of personal data and one has to be open and honest with data subjects about the use of their data.
- **(b) Purpose limitation:** "*Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*". Hence, it is necessary to define a purpose for which personal data will be processed before the collection of data.
- **(c) Data minimisation:** "*Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". Hence, the minimum amount of personal data needed to fulfil the stated purpose must be identified and no more than that processed.
- **(d) Accuracy:** "*Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*". Hence, personal data must always be kept up-to-date and erased or corrected as soon as it becomes incorrect **(e) Storage limitation:** "*Personal data shall be kept in a form*

[182] **Regulation (EU) 2018/1725** of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC

which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes". Hence, personal data must only be stored for the minimum amount of time needed for the stated purpose.

- **(f) Integrity and confidentiality:** "*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*". Hence, appropriate safeguards have to be in place to protect personal data.

At least one of the following six specific grounds has to apply in order for the processing of personal data to be lawful (GDPR, Article 6):

- **(a) Consent:** The data subject has given his/her consent to the processing, which can, however, be withdrawn at any time. Consent is needed by the holder of parental responsibility of children younger than 16 years (GDPR, Articles 7, 8).
- **(b) Contract:** The processing is necessary for a contract with an individual.
- **(c) Legal obligation:** The processing is necessary for compliance with legal obligations.
- **(d) Vital interests:** The processing is necessary to protect the life of the data subject or another person.
- **(e) Public task:** The processing is necessary to carry out a public task or function.
- **(f) Legitimate interest:** The processing is necessary based on legitimate interests.

The processing of special categories of personal data (e.g. race or biometric data) is prohibited (GDPR, Article 9) if the data subjects have not given their explicit consent (GDPR, Article 10).

The individual's rights are the following (GDPR, Articles 12-23):

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restriction of processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making

The transfer of personal data within the European Economic Area (EEA) is allowed. However, the transfer outside it can only occur based on an adequacy decision by the EC (Article 45) or if appropriate safeguards in the receiving country or territory are in place (Article 47). If neither is present, the transfer can only take place if the data subject has given explicit consent, or the transfer is necessary for the performance or conclusion of a contract, significant reasons of public interest, the establishment or defence of legal claims, protection of lives, or the transfer is made from a register (Article 49). The application of data protection rules is monitored and ensured by the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), the Data Protection Authorities (DPAs), and Data Protection Officers (DPO). The EDPS is an independent EU body with the task to monitor that the data protection rules of the regulation are applied fully by EU institutions and bodies.

4.1.2 Border control and management

Regulation (EU) 2016/399, also called the Schengen Borders Code, states the rules applicable to persons crossing the Schengen area's internal and external borders.

Internal borders: Any person can freely cross internal Schengen borders, but police checks (not related to border checks) can still be carried out. A temporary reintroduction of border control can take place for foreseeable events that need increased security, cases requiring immediate action due to a threat or cases where exceptional circumstances put the overall functioning of the Schengen area at risk. However, this should be a last resort and last as shortly as possible.

It has been proposed recently by the EC to update the rules on temporarily reintroducing internal border control, mainly by prolonging the time limits of temporary reintroduction[183]. The EC has also proposed to add a new article laying down specific procedures for serious threats to public policy or internal security lasting longer than one year.

External borders: To cross external borders, travellers need an adequate travel document and need to undergo checks by border guards. Additionally, their identity can be checked against national and European databases such as the VIS or SIS. Schengen Member States are authorized to exchange information (according to the Schengen Borders Code), which in general should result in more secure borders and less cross-border crime. The IBM (laid out in Regulation (EU) 2016/1624[184]) was established to reach this goal, by addressing migratory challenges and potential future threats as regards migrant smuggling, human trafficking and terrorism. It is put in practice by the European Border and Coast Guard (Frontex).

Regulation (EC) No 810/2009[185], also called Visa Code, regulates short stays in the Schengen area: Nationals of non-EU countries need to be in possession of a uniform Schengen visa, which allows them to remain in the area for a maximum of 90 days in any 180-day period. Hence, if a visa has been issued, the person can travel to all 26 Member countries of the Schengen area. As the procedure of application for the visa is lengthy and can discourage people from travelling to Europe but also due to security concerns and migratory challenges, it was decided that the common visa rules should be updated to respond to the mentioned challenges. These updates include, amongst others, the possibility for travellers to benefit from easier and

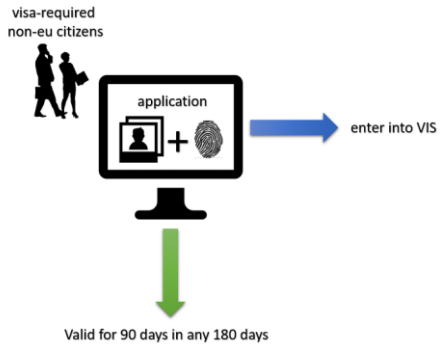

FIGURE 2: SCHEMATIC OVERVIEW OF VISA CODE

[183] For more information see: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20170927_factsheet_updated_schengen_rules_en.pdf

[184] **Regulation (EU) 2016/1624** of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC

[185] **Regulation (EC) No 810/2009** of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code)

faster procedures through electronic application forms as well as easier travelling for frequent visitors.

As regards legal immigration, certain categories of immigrants have the possibility to enter the EU on the basis of various directives, such as family reunification, long-term residency, the EU Blue Card, single permit, seasonal work, intra-corporate transfer, or for studies or research.

Upon crossing an external border, not only travellers but also goods are subject to checks by the border guards. In the domain of aviation security, Regulation (EC) No 300/2008 (and Directive 2005/65/EC as complement) applies, for all civil airports in the EU and air carriers providing goods via these airports. Maritime transport security is regulated in Regulation (EC) No 725/2004, introducing measures for improving the security of international / domestic shipping and port facilities, and implementing the security measures of the IMO. For all types of border crossings (airport, ports, and land borders), the Union Customs Code laid down by Regulation (EU) 952/2013 provides general rules and procedures for goods imported into or exported from the EU. Customs checks are carried out on the basis of established common risk criteria, meaning that not all consignments and goods crossing an EU border are inspected, but those which are considered to pose a risk to the security of the EU and its citizens. Thus, e.g. priority control areas are defined, where more dense controls are carried out over a predetermined period of time.

4.1.3 Information systems

In the following, the most important EU information systems are summarized based on the following questions:

- Who does the system apply to?
- Which are the participating countries (as of May 2018)?
- What data does the system collect?
- How is the data stored?
- Who has access to the system?
- Is a data transfer allowed and if so with whom?

4.1.3.1 Schengen Information System II (SIS II)

The SIS II is an information system that stores and generates alerts, thereby giving information on categories of wanted and missing persons as well as objects.

Application: The SIS II applies to EU and non-EU nationals.

Participating countries: 26 EU Member States participate, as well as the four Schengen associated countries (Switzerland, Norway, Iceland, and Liechtenstein). Special conditions exist for Bulgaria, Romania, and the United Kingdom. It is currently not yet operational in Cyprus and Ireland.

Data collected: The SIS II contains the following information on persons for whom an alert has been issued:

- Identity of person or object: surname(s), forename(s), name(s) at birth, aliases, specific physical characteristics, place and date of birth, sex, nationality(ies)
- Photographs and fingerprints
- Reason for alert and links between alerts plus authority issuing alert
- Whether person is armed, violent or has escaped

- Alerts on persons wanted for arrest or sought to assist with a judicial procedure
- Alerts on persons or vehicles, boats, aircraft and containers for checks in order to prosecute criminal offences
- Alerts on objects sought for seizure

After the issuance of an alert, the Member State that entered the data has to review the need to keep the data within three years. Copies of data can only be created for technical purposes and must be retained no more than 48 hours. Processing of sensitive data is not allowed.

Data storage: Alerts can be retained for five and a maximum of 10 years depending on the alert.

Access rights:
- Visa authorities
- Border guards: enter/consult alerts
- Migration authorities: enter/consult alerts
- Asylum authorities
- Police authorities
- Customs authorities
- Judicial (law enforcement) authorities
- Vehicle authorities: access alerts on stolen vehicles, number plates and vehicle registration documents
- Boat, aircraft and firearms registration authorities
- Under certain conditions: Europol, Eurojust and the European Border and Coast Guard Agency (Frontex)

In all cases, users can only access the system for the performance of their tasks.

Data transfer: The transfer of personal data to third parties is generally prohibited.

Other: The SIS II has been consulted about 5 billion times in 2017, which makes it the most widely used information system.

4.1.3.2 Visa Information System (VIS)

The VIS is an information system that gives information relating to applications for short-stay visas either to visit or to transit through the Schengen area.

Application: The VIS applies to visa-required non-EU nationals.

Participating countries: 22 EU Member States participate, as well as the four Schengen associated countries (Switzerland, Norway, Iceland, and Liechtenstein).

Data collected:
- Fingerprints and facial images
- Information on the visa application
- Decisions concerning the visa application

Access rights:
- Visa authorities: examine visa applications, enter/amend/delete data
- Migration authorities: consult data (check validity of visa and identity of traveller)
- Asylum authorities: consult data (determine country responsible for examining an asylum application)
- Border guards: consult data (check identity of traveller and validity of visa)

- Law enforcement authorities and Europol: consult data (prevent, detect, and investigate terrorist and other serious criminal offences on case-by-case basis)
- Carriers, police authorities, and Frontex (under certain conditions)

Visa, asylum, and migration authorities and border guards have limited access to the extent of the performance of their task. Border guards can search the VIS with the number of the visa sticker and fingerprints. If they have a match, they can consult further data on the application file. When a person is suspected to no longer fulfil the conditions for stay and fingerprints yield no results in the database, they can also search by name, sex, date/place of birth and information from the application. Law enforcement authorities and Europol can search the VIS only with certain limitations.

Data storage: Data is stored in the VIS for five years after the expiry date of the issued visa or the last date a decision has been taken relating to the visa.

Data transfer: Data in the VIS is not allowed to be communicated to third countries or international organisations,

- unless it is necessary to attest a TCN's identity (in individual cases and when data protection standards are met only) or
- in urgent cases for the purpose of the prevention and detection of serious crime (when data protection standards are met only).

Other: In 2018, a revision of the VIS was proposed in order to ensure interoperability with other EU information systems, and to include long-stay visas and residence permits.

4.1.3.3 European Travel Information and Authorisation System (ETIAS)

The ETIAS is an information system with scheduled operation in 2021 that aims to improve border management, prevent irregular migration, reinforce the fight against crime/terrorism, and save travellers time by carrying out pre-travel screening.

Application: The ETIAS will apply to visa-exempt non-EU citizens/nationals.

Participating countries: 25 EU Member States participate, as well as the four Schengen associated countries (Switzerland, Norway, Iceland, and Liechtenstein). Denmark is currently yet to decide.

Data collected: The following information is collected:

- Personal data: surname (family name), first name(s) (given name(s)), surname at birth, first name(s) of parents, other names (alias(es), artistic name(s), usual name(s)), date/place/country of birth, sex, current nationality, other nationalities, type/number/country of issuance of travel document, date/expiry of issuance, home address/city of residence; email address, phone numbers, education, current occupation, and fingerprints
- Travel document (passport or equivalent)
- First intended stay in Member State
- Background questions: Information relating to previous criminal records, presence in conflict zones, orders to leave the territory of a Member State / third country, return decisions issued

The processing must be non-discriminative (not based on sex, race, colour, ethnic/social origin, genetic features, language, religion/belief, political or other opinions, national minorities, property, birth, disability, age or sexual orientation). Minors only have to give

surname and first name(s), home/email address, phone number and parental authority. The ETIAS system will automatically compare the collected data against SIS, EES, VIS, Eurodac, Europol and Interpol SLTD (Stolen and Lost Travel Document) and TDAWN (Travel Documents Associated with Notices).

Data storage: Data and the applications are only allowed to be stored for the validity of the travel document or five years from the last decision concerning the application. It can be stored an additional three years with the explicit consent of the data subject for the purpose of facilitating a new application.

Access rights:

- Border guards: consult data (check whether traveller has valid authorisation, whether it will expire within the next 90 days, whether there were false hits)
- Carriers
- Migration authorities
- Other national authorities, Europol and the European Border and Coast Guard Agency (Frontex) (under certain conditions)

Data transfer: Generally, data is not allowed to be transferred to a third country, international organisation or any private party (except to Europol and Interpol in certain circumstances). However, in case of exceptional urgency or for the prevention, detection or investigation in criminal and terrorist offences, a transfer to third countries is allowed.

Other: The ETIAS will be valid for three years. The valid travel authorisation will have to be shown to carriers prior to boarding (air, land or sea) in order to be accepted to travel. At the border crossing point, the valid ETIAS authorisation plus the EES will allow the travellers to enter the Schengen area.

4.1.3.4 Entry/Exit System (EES)

The EES is an information system with scheduled operation in 2020/2021 that will provide data of non-EU nationals and note their entry/exit records in order to identify over-stayers. Additionally, it will replace the current system of manually stamping passports.

Application: The EES will apply to all non-EU nationals (both visa-exempt and visa-required) for short stay visits only.

Participating countries: 21 EU Member States participate, as well as the four Schengen associated countries (Switzerland, Norway, Iceland, and Liechtenstein). Denmark is currently yet to decide.

Data collected:

- Date, time/place of entry and exit
- Data on identity: surname (family name), first name(s), date of birth, nationality(ies), sex,
- Biometric data: facial image (taken live), fingerprints
- Data on travel documents: type/number/expiry date of travel document

Access rights:

- Visa authorities: examine visa applications
- Immigration authorities: verify identity of traveller
- Border guards: enter data each time traveller crosses external border, check to verify identity of travellers

- Other national authorities, law enforcement authorities and Europol (for the prevention, detection or investigation of terrorist or other serious criminal offences)

The access will be limited to the pursued purpose and has to be necessary and appropriate. Border/immigration authorities will be able to access the EES with fingerprint data only or in combination with a facial image. Where necessary, data from the EES can be kept in national files (in individual cases).

Data storage: The data can be stored for three years for travellers who respect the short stay rules, and five years for those who exceed their short stay period.

Data transfer: The data is generally not allowed to be transferred to third countries, international organisations or private entities. However, if it serves the purpose of return or where there is an exceptional case of urgency and the transfer is necessary for the prevention, detection or investigation of terrorist or other criminal offences, data can be transferred on an individual basis.

4.1.3.5 Passenger Name Record (PNR)

The PNR system is an information system for data stored in airlines' reservation systems.

Application: PNR applies to passengers on international flights entering/departing the EU as well as intra-EU flights.

Participating countries: 27 Member States participate. Denmark is currently not participating.

Data collected:
- Passenger's name
- Travel dates/itinerary
- Ticket information (seat number)
- Contact details
- Means of payment used
- Baggage information

Data is only allowed to be processed for the prevention, detection, investigation and prosecution of terrorist and serious criminal offences and for a pre-arrival assessment of passengers against predetermined risk criteria (if it is non-discriminative).

Data storage: Data can be stored for five years from the time of the transfer to the EU country in which the flight is landing/departing. After six months, this data must be depersonalised to mask out name, address/contact information, and payment information. Disclosure of the full PNR data after this period is permitted if it is reasonably believed to be necessary at the request of Europol and it has been approved by national authorities under national law.

Access rights: PNR data can only be accessed to prevent, detect, and investigate terrorist and other serious criminal offences.

Data transfer: PNR data can be exchanged with Member State authorities or with Europol only for law-enforcement purposes. PNR data can be transferred to a non-EU country under certain specific conditions only.

4.1.3.6 European Dactyloscopy (Eurodac)

Eurodac is an information system regarding asylum applicants and third-country nationals.

Application: Eurodac applies to non-EU nationals applying for asylum in the EU.

Participating countries: 28 EU Member States participate, as well as the four Schengen associated countries (Switzerland, Norway, Iceland, and Liechtenstein).

Data collected: Fingerprint data

Access rights:
- Border guards
- Asylum and police authorities
- Europol and the European Border and Coast Guard Agency (Frontex) (under certain conditions)

Access is only allowed to prevent, detect or investigate serious criminal offences.

Data storage: Fingerprint data has to be erased once asylum applicants, non-EU nationals or stateless persons obtain EU citizenship.

Data transfer: Data is not allowed to be shared with non-EU countries.

Other: In 2016, a revision of Eurodac was proposed in order to include facial images in the database that help identifying irregularly staying non-EU nationals.

4.1.3.7 European Criminal Records Information System (ECRIS)

ECRIS is an information system that allows exchanging criminal records between EU Member States.

Application: The ECRIS applies to all persons convicted in the EU.

Participating countries: 28 EU Member States participate.

Data collected:
- Nationality(ies) of persons
- Criminal history of persons

The information can be exchanged for the purpose of criminal proceedings or other purposes (e.g. pre-employment screening).

Access rights: Judges, prosecutors, and other relevant authorities have access.

Other: In 2016/2017, improvements were proposed to create the ECRIS - Third Country National (ECRIS-TCN) System that will also allow the exchange of information on criminal records of non-EU nationals (operational in 2020/2021).

4.1.4 Operational cooperation

The European Border and Coast Guard Agency (Frontex) is the main agency[186] responsible for managing security at EU borders and thus ensuring the integrated border management (IBM), which consists of managing migratory challenges and potential future threats at external borders. Frontex provides border and coast guards tasked with detecting cross-border crime (e.g. migrant smuggling or human trafficking) with technical and operational assistance (e.g. joint operations and rapid border interventions) and risk analysis (e.g. of risks for internal security). Frontex can process personal data for the purpose of risk analysis, rapid border and

[186] Other agencies include Europol, Cepol, eu-LISA, EMCDDA, and Eurojust.

return interventions, and joint operations. They can also transfer data to competent national authorities or EU agencies (e.g. Europol and Eurojust).

4.2 Discussion of guiding key research questions

In the following, the guiding key research questions are discussed on the basis of the regulations and directives presented above. As regards the collection and processing of personal data in general, the principal regulation is the GDPR, which is also cited in the following. Where applicable, articles of Regulation (EU) 2018/1725 are noted as well.

4.2.1 What kind of traveller/passenger data is allowed to be processed?

Important for the answer to this question is the definition of personal data and its processing. According to the GDPR, personal data is (Article 4; Article 3 of Regulation (EU) 2018/1725):

> *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".*

Hence, an individual is identified or identifiable if you can distinguish them from other individuals. This means that pseudonymised data is still personal data, whereas truly anonymised data is not. For the special category of criminal conviction and offence data, special rules apply (Articles 9, 10). According to the GDPR (Article 9; Article 10 in Regulation (EU) 2018/1725):

> *"processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited".*

According to the GDPR, processing means (Article 4; Article 3 in Regulation (EU) 2018/1725):

> *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".*

The following principles apply to the processing of data (Article 5; Article 4, Recital 20 in Regulation (EU) 2018/1725):

- **(a) Lawfulness, fairness, and transparency:** Valid legal grounds for the use of personal data have to be identified, it must be used in a fair (non-detrimental) way, and one must be open and honest with data subjects about the use of their data.
- **(b) Purpose limitation:** It is necessary to define a purpose for which data will be processed before they are collected.
- **(c) Data minimisation:** The minimum amount of personal data needed to fulfil a stated purpose must be identified and no more than that processed.
- **(d) Accuracy:** Data must be kept up-to-date and corrected or erased if it becomes incorrect.
- **(e) Storage limitation:** Data must be stored no longer than necessary for a stated purpose.
- **(f) Integrity and confidentiality:** Appropriate safeguards have to be in place to protect personal data.

Moreover, processing can only be lawful in case (Article 6; Article 5 in Regulation (EU) 2018/1725):

- (a) the data subject has given consent[187];
- (b) processing is necessary for the performance of a contract;
- (c) processing is necessary for compliance with a legal obligation;
- (d) processing is necessary to protect the vital interests of the data subject;
- (e) processing is necessary for a task carried out in the public interest;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party.

The information systems below either currently do or will store traveller/passenger data as listed.

Data in VIS:

- Fingerprints and facial images
- Information on the visa application
- Decisions concerning the visa application

Data in SIS:

- Surname(s), forename(s), name(s) at birth, aliases, specific physical characteristics, place and date of birth, sex, nationality(ies)
- Photographs and fingerprints
- Reason for alert and links between alerts, authority issuing alert
- Whether person is armed, violent or has escaped
- Alerts on persons wanted for arrest or sought to assist with a judicial procedure
- Alerts on persons or vehicles, boats, aircraft and containers for checks in order to prosecute criminal offences
- Alerts on objects sought for seizure

Data in ETIAS:

- Surname (family name), first name(s) (given name(s)), surname at birth, first name(s) of parents, other names (alias(es), artistic name(s), usual name(s)), date/place/country of birth, sex, current nationality, other nationalities, type/number/country of issuance of travel document, date/expiry of issuance, home address/city of residence; email address, phone numbers, education, current occupation, and fingerprints
- Travel document (passport or equivalent)
- First intended stay in Member State
- Background questions: Information relating to previous criminal records, presence in conflict zones, orders to leave the territory of a Member State / third country, return decisions issued

Data in EES:

- Date, time/place of entry and exit
- Data on identity: surname (family name), first name(s), date of birth, nationality(ies), sex
- Facial image (taken live), fingerprints
- Data on travel documents: type/number/expiry date of travel document

[187] Children above the age of 16 can give their consent themselves (Member States can also provide a lower age by law if it is not below 13), if they are younger, consent needs to be given from the person who holds parental responsibility (Article 8).

Data in PNR:
- Passenger's name
- Travel dates/itinerary
- Ticket information (seat number)
- Contact details
- Means of payment used
- Baggage information

Data in Eurodac:
- Fingerprint data

Data in ECRIS:
- Nationality(ies) of persons
- Criminal history of persons

Information systems in the EU collect and store different kinds of personal data based on specific legal grounds and purposes for the processing. Crucial to note is that if personal data is processed, data subjects have to be informed about what data is collected about them and why. Additionally, the processing is only lawful if the subject has given his or her consent or if specific other reasons necessitate the processing. The more sensitive the personal data, the less can be legally done with it. Children have more protection under the GDPR.

In the definitions of genetic and biometric data in both the GDPR and Directive (EU) 2016/680, facial images are explicitly mentioned as biometric data. Thus, as discussed in the above section 3.1.2, the processing of such data is in general not allowed, however, exceptions (with corresponding processing method and duration considerations) apply if the data subject has given consent, if it is necessary to protect lives, if the data was made public by the data subject (as can be the case with posts on social media sites[188]), or if it is necessary for the public interest.

4.2.2 Is it legal to store passenger data over a certain period of time, within the EU for example? If so, how long can passenger data be stored?

According to the GDPR, personal data must be "*kept in a form which identifies the subject no longer than necessary*" (Article 5; Article 4 in Regulation (EU) 2018/1725). After this retention period, data has to be erased. If keeping it longer is desired, it must be anonymised to a form which no longer permits the identification of data subjects. Only archiving purposes in the public interest, scientific and historical research purposes or statistical purposes can be indefinite data storage grounds.

Storage duration in VIS:
- Data is stored in the VIS for five years after the expiry date of the issued visa or the last date a decision has been taken relating to the visa.

Storage duration in SIS:
- Alerts can be retained five and a maximum of 10 years depending on the alert.

Storage duration in ETIAS:

[188] See MEDIA4SEC (2016) Ethics and Legal Issues Inventory (http://media4sec.eu/downloads/d1-3.pdf) for an overview of considerations in that domain

- Data and the applications are only allowed to be stored for the validity of the travel document or five years from the last decision concerning the application. It can be stored an additional three years with the explicit consent of the data subject for the purpose of facilitating a new application.

Storage duration in EES:

- The data is stored for three years for travellers who respect the short stay rules and five years for those who exceed their short stay period.

Storage duration in PNR:

- Data must be stored for five years from the time of the transfer to the EU country in which the flight is landing/departing. After six months, this data must be depersonalised to mask out name, address/contact information, and all payment information. Disclosure of the full PNR data after this period is permitted if it is reasonably believed to be necessary at the request of Europol and it has been approved by national authorities under national law.

Storage duration in Eurodac:

- Fingerprint data has to be erased once asylum applicants, non-EU nationals or stateless persons obtain EU citizenship.

In accordance with the GDPR, data storage periods must be defined and justified before the collection of personal data. The abovementioned information systems show that a period of some years can be a rough guideline.

4.2.3 What possibilities exist for countries to share passenger data?[189]

Transfer[190] of data within the EEA is allowed. The GDPR restricts the transfer or personal data to third countries or international organisations, no matter the size or frequency of the transfers. If the data is anonymised (so that it is not possible to identify individuals), it is no longer personal data, meaning that it can be transferred outside the EEA.

Transfers of personal data outside the EEA can be made:

- on the basis of an adequacy decision (Article 45; Article 47 in Regulation (EU) 2018/1725) or
- if they are subject to appropriate safeguards (Articles 46-48; Article 48 in Regulation (EU) 2018/1725) or
- if they fulfil an exception (Articles 49; Article 50 in Regulation (EU) 2018/1725).

According to the GDPR (Article 45; Article 47 in Regulation (EU) 2018/1725):

> *"a transfer of personal data to a third country or an international organisation may take place where the Commission has decided[191] that the third country, a territory or one or more specified*

[189] For more information see: https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

[190] Note that transfer is not the same as transit. An example: personal data is transferred via a server in a non-EU country from Member Country A to Member Country B. Then the transfer is only to Member Country B.

[191] Addition in Article 47 of Regulation (EU) 2018/1725: "(…) pursuant to Article 45(3) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680 (…)"

sectors within that third country, or the international organisation in question ensures an adequate level of protection[192]. Such a transfer shall not require any specific authorisation."

So far, adequacy decisions have been made about the following countries and territories: Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay. The Commission has made partial findings of adequacy about Canada, and the USA.

According to the GDPR (Article 46; Article 48 in Regulation (EU) 2018/1725):

"in the absence of a decision pursuant to Article 45(3)[193], a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available."

Appropriate safeguards can be provided from a supervisory authority by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules [where the processor is not a Union institution or body (Article 48 of Regulation (EU) 2018/1725)];
- standard data protection clauses adopted by the Commission;
- standard data protection clauses adopted by a supervisory authority [by the European Data Protection Supervisor (Article 48 in Regulation (EU) 2018/1725)] and approved by the Commission
- an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights;
- an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

According to the GDPR, binding corporate rules means (Article 4):

"personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity"

The GDPR also allows for exceptions when there is no adequacy decision or appropriate safeguards that are in place (Article 49; Article 50 in Regulation (EU) 2018/1725):

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;

[192] Addition in Article 47 of Regulation (EU) 2018/1725: "(…) and where the personal data are transferred solely to allow tasks within the competence of the controller to be carried out."

[193] Addition in Article 48 of Regulation (EU) 2018/1725: "(…) of Regulation (EU) 2016/679 or to Article 36(3) of Directive (EU) 2016/680 (…)".

(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Data sharing from VIS:

- Data in the VIS is not allowed to be communicated to third countries or international organisations
    - unless it is necessary to attest a TCN's identity (in individual cases and when data protection standards are met only) or
    - in urgent cases for the purpose of the prevention and detection of serious crime (when data protection standards are met only).

Data sharing from SIS:

- The transfer of data to third countries is prohibited.

Data sharing from ETIAS:

- Generally, data is not allowed to be transferred to a third country, international organisation or any private party, except to Europol and Interpol in certain circumstances. However, in case of exceptional urgency or for the prevention, detection or investigation in criminal and terrorist offences, it is allowed to be transferred to third countries.

Data sharing from EES:

- The data is generally not allowed to be transferred to third countries, international organisations or private entities. However, if it serves the purpose of return or where there is an exceptional case of urgency and the transfer is necessary for the prevention, detection or investigation of terrorist or other criminal offences, data can be transferred on an individual basis.

Data sharing from PNR:

- PNR data can be exchanged with Member State authorities or with Europol only for law-enforcement purposes. PNR data can be transferred to a non-EU country under certain specific conditions only. The EU has signed bilateral passenger name record (PNR) agreements with the United States and Australia.

Data sharing from EURODAC:

- Data is not allowed to be shared with non-EU countries.

Within the EU, personal data sharing is possible under conditions listed above. However, if personal data is transferred to a location outside the EU, there has to be an adequacy decision or appropriate safeguards in place. There are some exceptions in the GDPR and the existing information systems mentioned above.

Data from third countries should be obtained in accordance with national regulations of the respective third countries, and possibly through established international databases such as ICIS.

4.2.4 *What possibilities exist to receive passenger data from individuals approaching land borders?*

Passenger data from individuals approaching land borders can be received if they have previously given their data for travel to the EU. Visa-required travellers have to apply for a visa prior to entering the EU.

Visa-exempt travellers arriving on foot or by car, bus or train, have given no such a priori information. In this case, border guards have to make their decision of entry or refusal without prior knowledge about a person – especially if the person arrives by land, because the only source of information is the travel document. However, if a traveller arrives by air, carriers have to share all passenger data – advance passenger information (API) – ahead of the arrival. Additionally, airlines have to share passenger name record (PNR) data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious crime. Authorised authorities can then process the data for a pre-arrival risk-assessment of the passengers.

The European Travel and Information System (ETIAS) with scheduled operation in 2021 will allow pre-screening of visa-exempt travellers arriving at EU borders. Similarly to the visa application, the ETIAS application has to be completed online before travelling. The valid travel authorisation will need to be shown to carriers prior to boarding (air, land or sea). The ETIAS system will also automatically compare the collected data against SIS II, EES, VIS, Eurodac, Europol, and Interpol SLTD (Stolen and Lost Travel Document) and TDAWN (Travel Documents Associated with Notices) databases.

4.2.5 *What are the current obligations and rights of border and customs authorities in the EU regarding checks of travellers and goods?*

The Schengen Borders Code (SBC) governs the rules for any person that crosses the Schengen area's external borders as well as how they have to be controlled by border guards. The following describe obligations of border guards rooted in the SBC:

- Border surveillance (Article 13): Border guards have to carry out border surveillance to prevent unauthorised border crossings.
- Conducting of checks (Article 7): Border guards have to respect human dignity. They are not allowed to discriminate persons based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation.
- Checks on persons (Article 8): Both persons and their means of transport as well as objects in the possession of persons are subject to checks. Every person has to undergo a minimum check to establish his/her identity. This can be done by using technical devices and by consulting relevant databases where appropriate – specially to ensure that individuals do not represent a serious threat to security.

In more detail, on entry and exit, third-country nationals are subject to checks such as follows (Article 8):

- (a) thorough checks on entry shall comprise verification of the conditions governing entry and, where applicable, of documents authorising residence and the pursuit of a professional activity. This shall include a detailed examination covering the following aspects:
  - (i) verification that the third-country national is in possession of a document which is valid for crossing the border and which has not expired, and that the document is accompanied, where applicable, by the requisite visa or residence permit;
  - (ii) thorough scrutiny of the travel document for signs of falsification or counterfeiting;

- (iii) examination of the entry and exit stamps on the travel document of the third-country national concerned, in order to verify, by comparing the dates of entry and exit, that the person has not already exceeded the maximum duration of authorised stay in the territory of the Member States;
- (iv) verification regarding the point of departure and the destination of the third-country national concerned and the purpose of the intended stay, checking, if necessary, the corresponding supporting documents;
- (v) verification that the third-country national concerned has sufficient means of subsistence for the duration and purpose of the intended stay, for his or her return to the country of origin or transit to a third country into which he or she is certain to be admitted, or that he or she is in a position to acquire such means lawfully;
- (vi) verification that the third-country national concerned, his or her means of transport and the objects he or she is transporting are not likely to jeopardise the public policy, internal security, public health or international relations of any of the Member States. Such verification shall include direct consultation of the data and alerts on persons and, where necessary, objects included in the SIS and in national data files and the action to be performed, if any, as a result of an alert;

› (b) if the third country national holds a visa, the thorough checks on entry shall also comprise verification of the identity of the holder of the visa and of the authenticity of the visa, by consulting the Visa Information System (VIS) in accordance with Article 18 of Regulation (EC) No 767/2008;

› (c) by way of derogation, the VIS may be consulted using the number of the visa sticker in all cases and, on a random basis, the number of the visa sticker in combination with the verification of fingerprints where:

- traffic of such intensity arises that the waiting time at the border crossing point becomes excessive;
- all resources have already been exhausted as regards staff, facilities and organisation; and
- on the basis of an assessment there is no risk related to internal security and illegal immigration.

However, in all cases where there is doubt as to the identity of the holder of the visa and/or the authenticity of the visa, the VIS shall be consulted systematically using the number of the visa sticker in combination with the verification of fingerprints.

This derogation may be applied only at the border crossing point concerned for as long as the conditions referred to in points (i), (ii) and (iii) are met;

› (d) the decision to consult the VIS in accordance with point (c) shall be taken by the border guard in command at the border crossing point or at a higher level. The Member State concerned shall immediately notify the other Member States and the Commission of any such decision;

› (e) each Member State shall transmit once a year a report on the application of point (c) to the European Parliament and the Commission, which shall include the number of third-country nationals who were checked in the VIS using the number of the visa sticker only and the length of the waiting time referred to in point (c)(i);

› (f) points (c) and (d) shall apply for a maximum period of three years, beginning three years after the VIS has started operations. The Commission shall, before the end of the second year of application of points (c) and (d), transmit to the European Parliament and to the Council an evaluation of their implementation. On the basis of that evaluation, the European Parliament or the Council may invite the Commission to propose appropriate amendments to this Regulation;

› (g) thorough checks on exit shall comprise:

- verification that the third-country national is in possession of a document valid for crossing the border;
- verification of the travel document for signs of falsification or counterfeiting;
- whenever possible, verification that the third-country national is not considered to be a threat to public policy, internal security or the international relations of any of the Member States;

- (h) in addition to the checks referred to in point (g) thorough checks on exit may also comprise:
  - verification that the person is in possession of a valid visa, if required pursuant to Regulation (EC) No 539/2001, except where he or she holds a valid residence permit; such verification may comprise consultation of the VIS in accordance with Article 18 of Regulation (EC) No 767/2008;
  - verification that the person did not exceed the maximum duration of authorised stay in the territory of the Member States;
  - consultation of alerts on persons and objects included in the SIS and reports in national data files;
  - for the purpose of identification of any person who may not fulfil, or who may no longer fulfil, the conditions for entry, stay or residence on the territory of the Member States, the VIS may be consulted in accordance with Article 20 of Regulation (EC) No 767/2008.

Border guards have to perform checks on people and their goods and consult relevant databases in order to grant or refuse border crossings in accordance with the SBC. They are allowed to check travel documents against (some) EU information systems. They have to respect travellers' fundamental rights in doing so.

The following documents have to be checked for persons that cross EU external borders:

- For EU citizens: a passport or identity card
- For non-EU citizens: visa (for >60 countries) (future: ETIAS)

Additionally, when travelling by road, a valid driving license and vehicle's registration certificate are needed.

Regarding checks on goods, customs authorities are allowed to carry out customs checks they consider necessary, which should primarily be based on risk analysis, using electronic data-processing techniques. Controls by customs authorities are performed within a common risk management framework, based on information exchange with other customs authorities regarding specific risks and results of risk analyses. Customs authorities can verify the information given in a customs declaration, and examine the accounts of the declarant etc. As regards intra-Union flights and sea crossings, customs controls are carried out for the purpose of security and safety checks, and checks linked to prohibitions or restrictions.

4.2.6 What are likely future changes to the obligations and rights of border and customs authorities in the EU regarding checks of travellers and goods?

When comparing 2018 with 2017, border guards have already gained more access to EU information systems: Whilst border guards were able to access the SIS, VIS, and EES in 2017, in 2018 they were allowed to access Eurodac additionally[194]. A goal of the EU is to *increase interoperability* between existing information systems and technologies in order to make better use of them.

ETIAS, which will be operational in 2020, is a first step towards systematically checking people and their goods *prior to their arrival* at the actual border. While it is only planned for visa-exempt countries, it might eventually be introduced for every person crossing the Schengen

[194] For more information see: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170629_eu_information_system_-_update_june_2017_en.pdf and https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180516_eu-information-systems-security-borders_en.pdf

border. Furthermore, a new system is being tested and might be integrated with already existing information systems: the Intelligent Portable Border Control System[195] (iBorderCtrl), which is an intelligent control system for testing third-country nationals that reach EU external borders. To do so, the system scans faces (38 facial micro-gestures) of travellers during interrogation by border guards and flags suspicious reactions. iBorderCtrl was developed within the scope of the Horizon 2020 programme, is currently under lab testing, and piloting is planned for August 2019.

All such changes will have to comply with current data protection regulations. However, it is imaginable that perceptions on the trade-offs between safety and security and privacy might shift, leading to regulatory changes.

4.3 Possible refinements of the TRESSPASS concept

The TRESSPASS concept involves the use of an information exchange network (TIEN) to enable efficient and reliable, risk-based passenger checks through:

- The application of biometric technologies
- The use of sensing technologies (passport/ID readers, CCTV systems, body/cargo scanners)
- The design and development of a risk-based management system and relevant models to assess identity (of traveller), possession (of assets that can/cannot be used to generate a threat), capability (specific skills of people with which they can/cannot impose threat) and intent (from which the presence or absence of a threat can be derived)
- Links to legacy systems and external databases such as VIS/SIS/PNR through the TRESSPASS node

An international alert system that offers the capability to exchange and receive information to operational entities with links from the TIEN to legacy systems and external databases such as VIS, SIS II and PNR through the TRESSPASS node is envisaged. Currently however, information is not allowed to be exchanged outside the EEA if there are no adequacy decisions or appropriate safeguards in place. Even within the EEA, not all countries are connected to all existing information sharing systems and these systems are in turn not all interconnected with each other. Moreover, different authorities have different access to data. As part of increasing interoperability on the EU level, it is planned to establish the European Search Portal (ESP), through which all information systems could be searched simultaneously. However, no legislative instruments have been adopted yet and before TIEN can leverage access through the ESP, legislative changes at the EU level will have to occur. Possible changes in law regarding PNR (pending decision of the EU Court of Justice) will also have to be taken into account. Access to any existing databases will require authorisation by legal departments of the appropriate agencies and a clear and transparent definition of access and data processing rules within the information flow of the TIEN will most likely be a prerequisite.

The different ways of obtaining information about travellers (and staff) envisaged within the TRESSPASS concept will have to be discussed appropriately and explicitly within the framework of current data protection principles. In order for the TRESSPASS concept to be fully compliant with current legal requirements regarding data protection and exchange, the processing of personal information within the pilots – likely from volunteers – will have to be

[195] For more information see: https://www.iborderctrl.eu/

justified appropriately. It will have to be transparent what data is processed about individuals by whom, how, and why. Pilots of the TRESSPASS concept must either be run independently of regular border checks or seek specifications within the current regulations.

The risk-based border checks envisaged within the TRESSPASS concept are a departure from current rule-based checks. In the domain of aviation security, Regulation (EC) No 300/2008 has allowed Member States to *"derogate from the common basic standards"* and *"adopt alternative security measures that provide an adequate level of protection on the basis of a local risk assessment"* (Article 4). Article 6 further states:

> 1. Member States may apply more stringent measures than the common basic standards referred to in Article 4. In doing so, they shall act on the basis of a risk assessment and in compliance with Community law. Those measures shall be relevant, objective, non-discriminatory and proportional to the risk that is being addressed.
> 2. Member States shall inform the Commission of such measures as soon as possible after their application. Upon reception of such information, the Commission shall transmit this information to the other Member States.
> 3. Member States are not required to inform the Commission where the measures concerned are limited to a given flight on a specific date.

A revision of border control regulations inspired by Regulation (EC) No 300/2008 and the common risk management framework and information exchange between customs authorities regarding specific risks and results of risk analyses (Regulation (EU) 952/2013) could provide room for replacing current mandatory border checks by risk-based screening of travellers. The creation of a matrix of **a)** specific legal bases per type of border check along with **b)** proposed changes to them, **c)** their expected benefits, **d)** the residual risk, and **e)** their cost in ethical terms would likely enhance the TRESSPASS concept.

REFERENCES

Non-legislative documents

Airlines International Representation in Europe (AIRE): EU Smart Borders Package Entry-Exit System / ETIAS / API, available at: http://aire.aero/eu-smart-borders-package-entry-exit-system-etias-api/ [accessed 25 February 2019]

Antyterroryzm.gov.pl: The Border Guard, available at: http://antyterroryzm.gov.pl/eng/anti-terrorism/institutions-and-servi/the-border-guard/658,The-Border-Guard.html [accessed 17 December 2018]

EU policies – Delivering for citizens: Protection of EU external borders, available at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/630316/EPRS_BRI(2018)630316_EN.pdf [accessed 28 January 2019]

EU: EU law, available at: https://europa.eu/european-union/law_en [accessed 28 September 2018]

Eu-LISA: ECRIS-TCN, available at: https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn [accessed 27 September 2018]

EUR-Lex: Access to the Official Journal, available at: https://eur-lex.europa.eu/oj/direct-access.html [accessed 28 September 2018]

EUR-Lex: EFTA documents, available at: https://eur-lex.europa.eu/collection/eu-law/efta.html [accessed 28 September 2018]

EUR-Lex: International agreements and the EU's external competences, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aai0034 [accessed 28 September 2018]

EUR-Lex: Legal acts, available at: https://eur-lex.europa.eu/collection/eu-law/legislation/recent.html [accessed 28 September 2018]

EUR-Lex: National transposition, available at: https://eur-lex.europa.eu/collection/n-law/mne.html [accessed 28 September 2018]

EUR-Lex: Preparatory documents, available at: https://eur-lex.europa.eu/collection/eu-law/pre-acts.html [accessed 28 September 2018]

EUR-Lex: Summaries of EU Legislation, available at: https://eur-lex.europa.eu/browse/summaries.html [accessed 28 September 2018]

EUR-Lex: Treaties currently in force, available at: https://eur-lex.europa.eu/collection/eu-law/treaties/treaties-force.html [accessed 28 September 2018]

European Commission: A stronger, more efficient and secure EU Visa Policy, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-migration/20180314_eu-visa-policy_en.pdf [accessed 27 September 2018]

European Commission: advance passenger information (API), available at: https://ec.europa.eu/home-affairs/content/advance-passenger-information-api_en [accessed 25 February 2019]

European Commission: Aviation Security, available at: https://ec.europa.eu/transport/modes/air/security_en [accessed 20 September 2018]

European Commission: Closing security information gaps: new EU rules on Passenger Name Record (PNR) data, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180524_security-union-new-eu-rules-pnr_en.pdf [accessed 20 September 2018]

European Commission: Customs and tax allowances for travellers, available at: https://ec.europa.eu/taxation_customs/individuals/travelling/entering-eu_en [accessed 16 October 2018]

European Commission: Customs Risk Management, available at: https://ec.europa.eu/taxation_customs/general-information-customs/customs-risk-management_en [accessed 21 February 2019]

European Commission: Customs Risk Management Framework (CRMF), available at: https://ec.europa.eu/taxation_customs/customs-risk-management-framework-crmf_en [accessed 21 February 2019]

European Commission: Data protection in the EU, available at: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [accessed 10 September 2018]

European Commission: ETIAS – The European Travel Information and Authorisation System, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20180425_etias_en.pdf [accessed 6 November 2018]

European Commission: EU information management instruments, available at: http://europa.eu/rapid/press-release_MEMO-10-349_en.htm?locale=en [accessed 25 February 2019]

European Commission: EU legislation on Maritime Security, available at: https://ec.europa.eu/transport/sites/transport/files/modes/maritime/security/doc/legislation_maritime_security.pdf [accessed 6 November 2018]

European Commission: European Agenda on Security, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security_en [accessed 28 September 2018]

European Commission: European Criminal Records Information System (ECRIS), available at: https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/tools-judicial-cooperation/european-criminal-records-information-system-ecris_en [accessed 11 September 2018]

European Commission: European integrated border management, available at: https://ec.europa.eu/home-affairs/content/european-integrated-border-management_en [accessed 20 September 2018]

European Commission: Information exchange, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange_en [accessed 30 January 2019]

European Commission: Legal migration and Integration, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/legal-migration_en [accessed 15 October 2018]

European Commission: Legal Migration Fitness Check - REFIT initiative, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/legal-migration/fitness-check_en [accessed 29 September 2018]

European Commission: Maritime – What do we want to achieve?, available at: https://ec.europa.eu/transport/modes/maritime_en [accessed 15 September 2018]

European Commission: Maritime Transport Strategy, available at: https://ec.europa.eu/transport/themes/strategies/2018_maritime_transport_strategy_en [accessed 15 September 2018]

European Commission: Operational cooperation, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/operational-cooperation_en [accessed 30 January 2019]

European Commission: Passenger Name Record (PNR), available at: https://ec.europa.eu/home-affairs/what-we-do/policies/police-cooperation/information-exchange/pnr_en [accessed 18 September 2018]

European Commission: Protection of personal data, available at: https://ec.europa.eu/info/aid-development-cooperation-fundamental-rights/your-rights-eu/know-your-rights/freedoms/protection-personal-data_en [accessed 10 September 2018]

European Commission: Questions and Answers: Schengen Information System (SIS II), available at: http://europa.eu/rapid/press-release_MEMO-13-309_en.htm [accessed 28 September 2018]

European Commission: Schengen Area, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen_en [accessed 10 September 2018]

European Commission: Schengen Information System, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system [accessed 28 September 2018]

European Commission: Securing Europe's external borders – A European Border and Coast Guard, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/fact-sheets/docs/20170125_a_european_border_and_coast_guard_en.pdf [accessed 28 September 2018]

European Commission: Security Service, available at: https://www.copernicus.eu/sites/default/files/documents/Copernicus_Security_October2017.pdf [accessed 28 January 2018]

European Commission: Security Union – A Europe that protects, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181010_agenda-on-security-factsheet-progress-report_en.pdf [accessed 27 September 2018]

European Commission: Strengthening the EU's external borders, available at: https://www.consilium.europa.eu/en/policies/strengthening-external-borders/# [accessed 28 September 2018]

European Commission: Systematic checks at external borders, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/fact-sheets/docs/systematic_checks_at_external_borders_en.pdf [accessed 15 February 2019]

European Commission: Temporary Reintroduction of Border Control, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen/reintroduction-border-control_en [accessed 13 September 2018]

European Commission: The measures: Customs Risk Management Framework (CRMF), available at: https://ec.europa.eu/taxation_customs/general-information-customs/customs-risk-management/measures-customs-risk-management-framework-crmf_en [accessed 21 February 2019]

European Commission: The Schengen Information System, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181119_update-factsheet-sis_en.pdf [accessed 28 September 2018]

European Commission: Visa Information System (VIS), available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system_en [accessed 17 October 2018]

European Commission: Visa policy, available at: https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/visa-policy_en [accessed 10 September 2018]

European Commission: Why is risk management crucial?, available at: https://ec.europa.eu/taxation_customs/general-information-customs/customs-risk-management/why-is-risk-management-crucial_en [accessed 21 February 2019]

European Council: Improving security through information sharing: Council agrees negotiating mandate on interoperability, available at: https://www.consilium.europa.eu/en/press/press-releases/2018/06/14/improving-security-through-information-sharing-council-agrees-negotiating-mandate-on-interoperability/

European Parliament: The Juncker Commission's ten priorities, available at: http://www.europarl.europa.eu/EPRS/EPRS-Study-625176-Juncker-Commission-priorities-autumn-2018-FINAL.pdf [accessed 28 September 2018]

European Union: Poland, available at: https://europa.eu/european-union/about-eu/countries/member-countries/poland_en [accessed 17 December 2018]

European Union: Regulations, Directives and other acts, available at: https://europa.eu/european-union/eu-law/legal-acts_en [accessed 14 February 2019]

European Union: What can you take with you?, available at: https://europa.eu/youreurope/citizens/travel/carry/index_en.htm [accessed 20 September 2018]

Greek Law Digest: Foreign Citizens – Immigrants Introduction, available at: http://www.greeklawdigest.gr/topics/foreign-citizens-immigrants/item/255-foreign-citizens-immigrants-introduction [accessed 22 September 2018]

Greek Law Digest: Greek Port Regulations, available at: http://www.greeklawdigest.gr/topics/transportation/item/239-greek-port-regulations [accessed 22 September 2018]

ICLG International Comparative Legal Guides: Data Protection 2018 – Netherlands, available at: https://iclg.com/practice-areas/data-protection-laws-and-regulations/netherlands [accessed 31 January 2019]

ICO Information Commissioner's Office: Lawful basis for processing, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ [accessed 10 September 2018]

IMO International Maritime Organization: Introduction to IMO, available at: http://www.imo.org/en/About/Pages/Default.aspx [accessed 15 September 2018]

IMO International Maritime Organization: SOLAS XI-2 and the ISPS Code, available at: http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas-xi-2%20isps%20code.aspx [accessed 15 September 2018]

INTERPOL: Databases, available at: https://www.interpol.int/INTERPOL-expertise/Databases [accessed 28 January 2018]

Lambert, P. (2017). Understanding the New European Data Protection Rules. Auerbach Publications. Available at: https://books.google.ch/books?id=QL42DwAAQBAJ&lpg=PT428&dq=EU%20%20data%20protection%20exceptions&pg=PT428#v=onepage&q&f=false [accessed 10 January 2019]

Liberati A, Altman DG, Tetzlaff J, Mulrow C, Gøtzsche PC, et al. (2009). The PRISMA Statement for Reporting Systematic Reviews and Meta-Analyses of Studies That Evaluate Health Care Interventions: Explanation and Elaboration. PLOS Medicine 6(7): e1000100. Available at: https://doi.org/10.1371/journal.pmed.1000100 [accessed 20 September 2018]

Migrant info.pl: Local Border Traffic, available at: http://www.migrant.info.pl/Local_border_traffic.html [accessed 17 December 2018]

Moher D, Liberati A, Tetzlaff J, Altmann DG, and the PRISMA Group. Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. Ann Intern Med. 2009;151:264–269. doi: 10.7326/0003-4819-151-4-200908180-00135. Available at: https://ac.els-cdn.com/S1743919110000403/1-s2.0-S1743919110000403-main.pdf?_tid=1796848f-4b69-41d4-ab64-318db438159b&acdnat=1545049428_20444b5116bad42a0f299b4ee7ead324 [accessed 20 September 2018]

Nations online: Netherlands, available at: https://www.nationsonline.org/oneworld/netherlands.htm [accessed 15 December 2018]

Piraeus Port Authority S.A.: Annual Financial Report 2017, available at: http://www.olp.gr/en/investor-information/annual-reports [accessed 22 September 2018]

Schengen Visa Info: ETIAS – European Travel Information and Authorisation System, available at: https://www.schengenvisainfo.com/etias/ [accessed 3 October 2018]

Schengen Visa Info: Schengen Visa Types & Validity, available at: https://www.schengenvisainfo.com/schengen-visa-types/ [accessed 20 September 2018]

Schiphol: Amsterdam Airport Schiphol Airport Facts, available at: https://www.schiphol.nl/en/route-development/page/amsterdam-airport-schiphol-airport-facts/ [accessed 15 December 2018]

TRESSPASS (2018): Technical Framework, available at: https://www.tresspass.eu/Technical-Framework [accessed 28 January 2019]

TRESSPASS (2018): Deliverable D9.6: Typology of ethical, legal and societal issues of risk based screening concepts

U.S. Customs and Border Protection: Advance Passenger Information System Fact Sheet, available at: https://www.cbp.gov/document/fact-sheets/advance-passenger-information-system-fact-sheet [accessed 25 February 2019]

Legislative documents (https://eur-lex.europa.eu/homepage.html) and legislation summaries (https://eur-lex.europa.eu/browse/summaries.html)

Summary of 2002/946/JHA: Council framework Decision: Penal framework for preventing the facilitation of illegal immigration, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0045&from=EN [accessed 24 September 2018]

Agreement between the European Community and the Government of Canada on the processing of Advance Passenger Information and Passenger Name Record data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22006A0321(01)&from=EN [accessed 20 September 2018]

Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22012A0714(01)&from=EN [accessed 20 September 2018]

Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22012A0811(01)&from=EN [accessed 20 September 2018]

COM(2009) 8 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Strategic goals and recommendations for the EU's maritime transport policy until 2018,

available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0008&from=EN [accessed 20 September 2018]

Summary of COM(2009) 8 final: European maritime transport policy until 2018, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:tr0015&from=EN [accessed 20 September 2018]

COM(2011) 898 final: Communication from the Commission to the European Parliament and the Council. European vision for Passengers: Communication on Passenger Rights in all transport modes, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0898&from=EN

COM(2015) 285 final: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - EU Action Plan against migrant smuggling (2015 - 2020), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0285&from=EN [accessed 24 September 2018]

COM(2016) 205 final: Communication from the Commission to the European Parliament, the Council - Stronger and Smarter Information Systems for Borders and Security, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0205&from=EN [accessed 29 January 2019]

COM(2017) 344 final: Proposal for a Regulation of the European Parliament and of the Council establishing a centralised system for the identification of Member States holding conviction information on third country nationals and stateless persons (TCN) to supplement and support the European Criminal Records Information System (ECRISTCN system) and amending Regulation (EU) No 1077/2011, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017PC0344&qid=1547202003390&from=EN [accessed 20 September 2018]

COM(2018) 549 final: Report from the Commission to the Council and the European Parliament – Second Progess Report on the implementation of the EU Strategy and Action Plan for customs risk management, available at: https://ec.europa.eu/taxation_customs/sites/taxation/files/crm_second_progress_report.pdf [accessed 21 February 2019]

Summary of Commission Implementing Decision (EU) 2016/1250: Protecting EU citizens' privacy in data transfers to the US, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4298958&from=EN [accessed 10 September 2018]

Summary of Council Decision 2007/533/JHA: Second generation Schengen Information System (SIS II) – former 3rd pillar decision, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14569&from=EN [accessed 10 September 2018]

Summary of Council Decision 2008/617/JHA: Cooperation between special intervention units, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0003&from=EN [accessed 20 September 2018]

Summary of Council Decision 2008/633/JHA: Rules for access to the EU's Visa Information System (VIS), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14512&from=EN [accessed 10 September 2018]

Summary of Council Decision 2009/371/JHA: EU agency for law enforcement cooperation — Europol, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0025&from=EN [accessed 20 September 2018]

Summary of Council Directive 2002/90/EC: Defining the facilitation of illegal immigration, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0044&from=EN [accessed 30 October 2018]

Summary of Council Directive 2003/86/EC: Family reunification, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33118&qid=1543570618600&from=EN [accessed 10 September 2018]

Summary of Council Directive 2003/109/EC: Non-EU nationals – rules for long-term residence, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l23034&from=EN [accessed 20 September 2018]

Summary of Council Directive 2004/82/EC: Obligation of air carriers to communicate passenger data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14582&from=EN [accessed 10 September 2018]

Summary of Council Directive 2007/74/EC: Value-added tax and excise duties — exemptions for travellers from outside the EU, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l31045&from=EN [accessed 15 October 2018]

Summary of Council Directive 2009/50/EC: EU Blue Card – entry and residence of highly qualified workers, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14573&qid=1543570866894&from=EN [accessed 10 September 2018]

Summary of Council Framework Decision 2009/315/JHA: Exchange of information on criminal records between EU countries, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0023&from=EN [accessed 10 September 2018]

Summary of Council Regulation (EC) No 515/97: CIS system, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l11037&from=EN [accessed 27 September 2018]

Summary of Council Regulation (EC) No 2007/2004: European Agency for the Management of External Borders — Frontex, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l33216&from=EN [accessed 20 September 2018]

Summary of Council Regulation (EC) No 377/2004: Immigration liaison officers' network, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14511&from=EN [accessed 20 September 2018]

Summary of Council Regulation (EC) No 539/2001: Visa requirements for non-EU nationals, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0031&from=EN [accessed 20 September 2018]

Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0065&from=GA [accessed 17 September 2018]

Summary of Directive 2005/65/EC: Port infrastructure: enhancing port security, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24162&from=EN [accessed 17 September 2018]

Directive 2011/51/EU of the European Parliament and of the Council of 11 May 2011 amending Council Directive 2003/109/EC to extend its scope to beneficiaries of international protection (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0051&qid=1543570828283&from=EN [accessed 20 September 2018]

Directive 2011/98/EU of the European Parliament and of the Council of 13 December 2011 on a single application procedure for a single permit for third-country nationals to reside and work in the territory of a Member State and on a common set of rights for third-country workers legally residing in a Member State, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0098&qid=1543570911859&from=EN [accessed 20 September 2018]

Summary of Directive 2011/98/EU: Non-EU workers – easier residence and work formalities, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14574&qid=1543570911859&from=EN [accessed 10 September 2018]

Directive 2014/36/EU of the European Parliament and of the Council of 26 February 2014 on the conditions of entry and stay of third-country nationals for the purpose of employment as seasonal workers, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0036&qid=1543570952249&from=EN [accessed 20 September 2018]

Summary of Directive 2014/36/EU: Employment as seasonal workers, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:23010602_1&qid=1543570952249&from=EN [accessed 10 September 2018]

Directive 2014/66/EU of the European Parliament and of the Council of 15 May 2014 on the conditions of entry and residence of third-country nationals in the framework of an intra-corporate transfer, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0066&qid=1543570991252&from=EN [accessed 20 September 2018]

Summary of Directive 2014/66/EU: Posting of staff from outside the EU, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:240204_1&qid=1543570991252&from=EN [accessed 10 September 2018]

Directive (EU) 2016/680 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 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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN [accessed 20 September 2018]

Summary of Directive (EU) 2016/680: Protecting personal data when being used by police and criminal justice authorities (from 2018), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_3&qid=1540907376326&from=EN [accessed 10 September 2018]

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0681&qid=1541001284561&from=EN [accessed 20 September 2018]

Summary of Directive (EU) 2016/681: Use of passenger records to prevent terrorism and serious crime, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:2307_4&from=EN [accessed 10 September 2018]

Directive (EU) 2016/801 of the European Parliament and of the Council of 11 May 2016 on the conditions of entry and residence of third-country nationals for the purposes of research, studies, training, voluntary service, pupil exchange schemes or educational projects and au pairing (recast), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0801&qid=1543571025649&from=EN [accessed 20 September 2018]

Summary of Directive (EU) 2016/801: Residence for non-EU nationals involved in research training, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4298974&qid=1543571025649&from=EN [accessed 10 September 2018]

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1727&qid=1548767104576&from=EN [accessed 10 January 2019]

Summary of Council Regulation (EC) No 1186/2009: EU customs relief system, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l11002&from=EN [accessed 22 September 2018]

Regulation (EU) No 181/2011 of the European Parliament and of the Council of 16 February 2011 concerning the rights of passengers in bus and coach transport and amending Regulation (EC) No 2006/2004 (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R0181&from=EN [accessed 30 January 2019]

Summary of Regulation (EU) No 181/2011: Bus and coach passengers' rights, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:tr0050&from=EN [accessed 30 January 2019]

Regulation (EC) No 261/2004 of the European Parliament and of the Council of 11 February 2004 establishing common rules on compensation and assistance to passengers in the event of denied boarding and of cancellation or long delay of flights, and repealing Regulation (EEC) No 295/91 (Text with EEA relevance) - Commission Statement, available at: https://eur-lex.europa.eu/resource.html?uri=cellar:439cd3a7-fd3c-4da7-8bf4-b0f60600c1d6.0004.02/DOC_1&format=PDF [accessed 30 January 2019]

Summary of Regulation (EC) No 261/2004: EU air passenger rights in case of denied boarding, a delayed flight or a cancelled flight, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24173&from=EN [accessed 30 January 2019]

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of aviation security and repealing Regulation (EC) No 2320/2002 (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0300&qid=1544178524742&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 300/2008: Civil aviation security: EU-wide rules, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:tr0028&from=EN [accessed 20 September 2018]

Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010 Text with EEA relevance, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0377&qid=1547198528711&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) No 377/2014: Copernicus Programme (2014-2020): observing and monitoring the planet, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:27020204_1&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) No 377/2014: European satellite monitoring programme (Copernicus): climate aspects, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:2001_12&from=EN [accessed 20 September 2018]

Regulation (EU) No 576/2013 of the European Parliament and of the Council of 12 June 2013 on the non-commercial movement of pet animals and repealing Regulation (EC) No 998/2003 (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0576&from=EN [accessed 15 October 2018]

Summary of Regulation (EU) No 576/2013: Non-commercial movements of pet animals, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:300203_2&from=EN [accessed 15 October 2018]

Regulation (EU) No 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending

Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0603&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) No 603/2013: Eurodac: European system for the comparison of fingerprints of asylum applicants, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:230105_1&from=EN [accessed 10 September 2018]

Regulation (EU) No 656/2014 of the European Parliament and of the Council of 15 May 2014 establishing rules for the surveillance of the external sea borders in the context of operational cooperation coordinated by the European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0656&qid=1547467958613&from=EN [accessed 20 January 2019]

Summary of Regulation (EU) No 656/2014: Controlling the EU external maritime borders and saving immigrants' lives in operations at sea, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:2301_3&from=EN [accessed 20 January 2019]

Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (Text with EEA relevance), available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:129:0006:0091:en:PDF [accessed 15 September 2018]

Summary of Regulation (EC) No 725/2004: Security for ships and port facilities, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24099&from=GA [accessed 15 September 2018]

Regulation (EC) No 764/2008 of the European Parliament and of the Council of 9 July 2008 laying down procedures relating to the application of certain national technical rules to products lawfully marketed in another Member State and repealing Decision No 3052/95/EC (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0764&qid=1540979983287&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 764/2008: National technical regulations and free movement of goods, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:mi0006&from=EN [accessed 20 September 2018]

Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008R0767&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 767/2008: VIS Regulation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14517&from=EN [accessed 10 September 2018]

Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas (Visa Code), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1538999164510&uri=CELEX:32009R0810 [accessed 20 September 2018]

Summary of Regulation (EC) No 810/2009: Visa Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:jl0028&from=EN [accessed 10 September 2018]

Regulation (EU) No 952/2013 of the European Parliament and of the Council of 9 October 2013 laying down the Union Customs Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0952&from=EN [accessed 15 October 2018]

Summary of Regulation (EU) No 952/2013: EU Customs Code update, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:12_2&from=EN [accessed 15 October 2018]

Regulation (EU) No 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1052&qid=1539083677865&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) No 1052/2013: European border surveillance system (Eurosur), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:230103_1&from=EN [accessed 10 September 2018]

Regulation (EU) No 1077/2011 of the European Parliament and of the Council 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, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011R1077&from=EN [accessed 21 September 2018]

Summary of Regulation (EU) No 1077/2011: Eu-LISA: managing IT systems in the field of border and migration controls, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:2301_4&from=EN [accessed 10 September 2018]

Regulation (EU) No 1177/2010 of the European Parliament and of the Council of 24 November 2010 concerning the rights of passengers when travelling by sea and inland waterway and amending Regulation (EC) No 2006/2004 (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010R1177&from=EN [accessed 30 January 2019]

Summary of Regulation (EU) No 1177/2010: Rights of passengers travelling by sea and inland waterways, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:tr0049&from=EN [accessed 30 January 2019]

Regulation (EU) No 1294/2013 of the European Parliament and of the Council of 11 December 2013 establishing an action programme for customs in the European Union for the period 2014-2020 (Customs 2020) and repealing Decision No 624/2007/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R1294&from=en [accessed 22 February 2019]

Summary of Regulation (EU) No 1294/2013: Action programme for customs in the European Union for the period 2014-20 (Customs 2020), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:12_1&from=EN [accessed 22 February 2019]

Regulation (EC) No 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007R1371&from=EN [accessed 30 January 2019]

Summary of Regulation (EC) No 1371/2007: Rail passenger Rights, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24003&from=EN [accessed 30 January 2019]

Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 1889/2005: Money laundering: prevention through customs cooperation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l25069&from=EN [accessed 20 September 2018]

Regulation (EC) No 1920/2006 of the European Parliament and of the Council of 12 December 2006 on the European Monitoring Centre for Drugs and Drug Addiction (recast), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1545048777411&uri=CELEX:32006R1920 [accessed 20 September 2018]

Summary of Regulation (EC) No 1920/2006: European Monitoring Centre for Drugs and Drug Addiction, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:c11518&from=EN [accessed 20 September 2018]

Regulation (EC) No 1931/2006 of the European Parliament and of the Council of 20 December 2006 laying down rules on local border traffic at the external land borders of the Member States and amending the provisions of the Schengen Convention, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1931&qid=1539087953866&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 1931/2006: Local border traffic at external land borders, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14506&from=EN [accessed 10 September 2018]

Regulation (EC) No 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1986&qid=1541422261427&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 1986/2006: Access of vehicle registration services to SIS II, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14545&from=EN [accessed 20 September 2018]

Regulation (EC) No 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006R1987&from=EN [accessed 20 September 2018]

Summary of Regulation (EC) No 1987/2006: Second generation Schengen Information System (SIS II) – former 1st pillar regulation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14544&from=EN [accessed 10 September 2018]

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2219&qid=1540980133068&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) 2015/2219: European Union Agency for Law Enforcement Training (CEPOL), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4314913&from=EN [accessed 20 September 2018]

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code) (codification), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0399&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) 2016/399: Rules on crossing EU borders, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:230101_1&from=EN [accessed 10 September 2018]

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) (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) 2016/679: Protection of personal data (from 2018), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:310401_2&qid=1540907376326&from=EN [accessed 10 September 2018]

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0794&from=en [accessed 20 September 2018]

Summary of Regulation (EU) 2016/794: European Union Agency for Law Enforcement Cooperation (Europol), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:23040102_1&from=EN [accessed 20 September 2018]

Regulation (EU) 2016/1624 of the European Parliament and of the Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1624&qid=1539084338300&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) 2016/1624: European Border and Coast Guard (Regulation (EU) 2016/1624), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:230103_3&from=EN [accessed 10 September 2018]

Regulation (EU) 2017/2225 of the European Parliament and of the Council of 30 November 2017 amending Regulation (EU) 2016/399 as regards the use of the Entry/Exit System, available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation_proposal_entryexit_system_en.pdf [accessed 20 September 2018]

Summary of Regulation (EU) 2017/2225: Smart borders: EU Entry/Exit System, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4326388&from=EN [accessed 10 September 2018]

Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes, and amending the Convention implementing the Schengen Agreement and Regulations (EC) No 767/2008 and (EU) No 1077/2011, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R2226&qid=1541001165422&from=EN [accessed 20 September 2018]

Summary of Regulation (EU) 2017/2226: Smart borders: EU Entry/Exit System, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:4326388&from=EN [accessed 10 September 2018]

Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1240&qid=1539261643150&from=EN [accessed 20 September 2018]

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725&qid=1550136325856&from=EN [accessed 14 February 2019]

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT [accessed 20 September 2018]

SWD(2018) 380 final: Commission Staff Working Document, Accompanying the document: Report from the Commission to the Council and the European Parliament – Second Progress Report on the implementation of the EU Strategy and Action Plan for Customs Risk Management, available at: https://ec.europa.eu/taxation_customs/sites/taxation/files/crm_second_progress_report_staff_working_document.pdf [accessed 21 February 2019]

Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31997R0515&from=EN [accessed 27 September 2018]

2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0518&from=EN [accessed 20 September 2018]

Council Regulation (EC) No 539/2001 of 15 March 2001 listing the third countries whose nationals must be in possession of visas when crossing the external borders and those whose nationals are exempt from that requirement, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02001R0539-20170611&from=EN [accessed 20 September 2018]

2002/2/EC: Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=en [accessed 20 September 2018]

Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1998&from=EN [accessed 15 December 2018]

2002/946/JHA: Council framework Decision of 28 November 2002 on the strengthening of the penal framework to prevent the facilitation of unauthorised entry, transit and residence,

available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002F0946&from=EN [accessed 24 September 2018]

Council Directive 2002/90/EC of 28 November 2002 defining the facilitation of unauthorised entry, transit and residence, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0090&from=EN [accessed 30 October 2018]

2003/490/EC: Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0490&from=EN [accessed 20 September 2018]

Council Directive 2003/86/EC of 22 September 2003 on the right to family reunification, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0086&qid=1543570618600&from=EN [accessed 20 September 2018]

2003/821/EC: Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey (Text with EEA relevance) (notified under document number C(2003) 4309), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003D0821&from=EN [accessed 20 September 2018]

Council Directive 2003/109/EC of 25 November 2003 concerning the status of third-country nationals who are long-term residents, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003L0109&from=en [accessed 20 September 2018]

Council Regulation (EC) No 377/2004 of 19 February 2004 on the creation of an immigration liaison officers network, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R0377&qid=1540980243190&from=EN [accessed 20 September 2018]

2004/411/EC: Commission Decision of 28 April 2004 on the adequate protection of personal data in the Isle of Man, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004D0411&from=EN [accessed 20 September 2018]

Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004L0082&qid=1545047588503&from=EN [accessed 20 September 2018]

Council Regulation (EC) No 2007/2004 of 26 October 2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32004R2007&qid=1545048493366&from=EN [accessed 20 September 2018]

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007D0533&from=EN [accessed 20 September 2018]

Council Directive 2007/74/EC of 20 December 2007 on the exemption from value added tax and excise duty of goods imported by persons travelling from third countries, available at:

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32007L0074&from=EN [accessed 15 October 2018]

2008/333/EC: Commission Decision of 4 March 2008 adopting the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document number C(2008) 774), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0333&qid=1541001408460&from=EN [accessed 20 September 2018]

2008/393/EC: Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey (notified under document number C(2008) 1746) (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0393&from=EN [accessed 20 September 2018]

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0633&qid=1541001466347&from=EN [accessed 20 September 2018]

Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service (https://eur-lex.europa.eu/resource.html?uri=cellar:d48aa827-83bb-4210-b9e7-4e4066d3ce4a.0006.01/DOC_1&format=PDF and https://eur-lex.europa.eu/resource.html?uri=cellar:d48aa827-83bb-4210-b9e7-4e4066d3ce4a.0006.01/DOC_2&format=PDF [accessed 20 September 2018]

Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0617&from=EN [accessed 20 September 2018]

Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009F0315&qid=1545048214510&from=EN [accessed 20 September 2018]

Commission Regulation (EC) No 206/2009 of 5 March 2009 on the introduction into the Community of personal consignments of products of animal origin and amending Regulation (EC) No 136/2004 (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R0206&from=EN [accessed 23 September 2018]

Council Decision 2009/316/JHA of 6 April 2009 on the establishment of the European Criminal Records Information System (ECRIS) in application of Article 11 of Framework Decision 2009/315/JHA, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0316&qid=1545048114948&from=EN [accessed 20 September 2018]

Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0371&qid=1544867507279&from=EN [accessed 20 September 2018]

Council Directive 2009/50/EC of 25 May 2009 on the conditions of entry and residence of third-country nationals for the purposes of highly qualified employment, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0050&qid=1543570866894&from=EN [accessed 20 September 2018]

Council Regulation (EC) No 1186/2009 of 16 November 2009 setting up a Community system of reliefs from customs duty, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009R1186&from=EN [accessed 22 September 2018]

Council Decision 2009/936/JHA of 30 November 2009 adopting the implementing rules for Europol analysis work files, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009D0936&qid=1548767656214&from=EN [accessed 20 September 2018]

2010/146/: Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data (notified under document C(2010) 1130) (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0146&from=en [accessed 20 September 2018]

2010/625/EU: Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra (notified under document C(2010) 7084) (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0625&from=EN [accessed 20 September 2018]

2011/61/EU: Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data (notified under document C(2011) 332) Text with EEA relevance, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011D0061&from=EN [accessed 20 September 2018]

2012/484/EU: Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data (notified under document C(2012) 5704) Text with EEA relevance, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012D0484&from=EN [accessed 20 September 2018]

2013/65/EU: Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557) Text with EEA relevance, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0065&from=EN [accessed 20 September 2018]

Commission Regulation (EU) No 245/2013 of 19 March 2013 amending Regulation (EC) No 272/2009 as regards the screening of liquids, aerosols and gels at EU airports (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0245&from=EN [accessed 15 December 2018]

Commission Delegated Regulation (EU) 2015/2446 of 28 July 2015 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2446&from=EN [accessed 15 October 2018]

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN [accessed 20 September 2018]

Commission Implementing Decision (EU) 2016/578 of 11 April 2016 establishing the Work Programme relating to the development and deployment of the electronic systems provided for in the Union Customs Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0578&from=EN [accessed 22 February 2019]

Commission Delegated Regulation (EU) 2018/1063 of 16 May 2018 amending and correcting Delegated Regulation (EU) 2015/2446 supplementing Regulation (EU) No 952/2013 of the European Parliament and of the Council as regards detailed rules concerning certain provisions of the Union Customs Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1063&from=EN [accessed 15 October 2018]

Commission Implementing Regulation (EU) 2015/2447 of 24 November 2015 laying down detailed rules for implementing certain provisions of Regulation (EU) No 952/2013 of the European Parliament and of the Council laying down the Union Customs Code, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R2447&from=EN [accessed 15 October 2018]

Pilot cases legislative documents

Netherlands Aliens Act 2000, available at: http://hrlibrary.umn.edu/research/Netherlands/Alien%20Act%202000.pdf [accessed 2 October 2018]

Government Gazette of the Hellenic Republic 265 / A: Law 2960/2001 - National Customs Code (translated by consortium partners)

Government Gazette of the Hellenic Republic 281/ A / 20.12.2007: Law 3622/2007 Enhancing the security of ships, port facilities and ports and other provisions (translated by consortium partners)

Government Gazette of the Hellenic Republic 80 / A / 01.04.2014: Law 4251/2014 - Immigration and Social Integration Code and other provisions, available at: http://www.ypes.gr/UserFiles/24e0c302-6021-4a6b-b7e4-8259e281e5f3/metanast-N4251-2014.pdf [accessed 22 September 2018]

Greek Customs: Legislation overview (translated by consortium partners)

OJ 1990 No. 78 item 462, "USTA AWA" of October 12, 1990 (translated by consortium partners)

Republic of Poland: Act of 12 December 2013 on foreigners (Item 1650), available at: http://www.asylumlawdatabase.eu/sites/www.asylumlawdatabase.eu/files/aldfiles/EN%20-%20Poland%20act_on_foreigners_en_0.pdf [accessed 13 September 2018]

Wet op de inlichtingen – en veiligheidsdiensten (Wiv), Intelligence and Security Services Act, available at: https://wetten.overheid.nl/BWBR0039896/2018-05-01#Hoofdstuk1 [accessed 31 January 2019] (translated by consortium partners)

Wet politiegegevens (Wpg), Police Data Act, available at: https://wetten.overheid.nl/BWBR0022463/2018-05-01 [accessed 31 January 2019] (translated by consortium partners)

LIST OF FIGURES

LIST OF TABLES

ANNEX: PRISMA METHOD

Database searches[196]

TABLE 4: DATABASE SEARCHES CONDUCTED IN EUR-LEX: GENERIC SEARCH STRING

	Search ID	Search Query	Number of Results
Generic Search String	20180905 (2)	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("requirements" OR "framework" OR "challenges" OR "solutions") In title and text, Search language: English	33 Results
	20180905 (3)	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND ("requirements" OR "framework" OR "challenges" OR "solutions") In title and text, Search language: English	101 Results
	20180905 (5)	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border security" OR "border crossing" OR "border checkpoint") AND ("requirements" OR "framework" OR "challenges" OR "solutions") In title and text, Search language: English	47 Results
	20180905 (6)	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("BCP" OR "passport control") AND ("requirements" OR "framework" OR "challenges" OR "solutions") In title and text, Search language: English	40 Results
	20180905 (7)	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("requirements" OR "framework" OR "challenges" OR "solutions") In title and text, Search language: English	1 Result

TABLE 5: DATABASE SEARCHES CONDUCTED IN EUR-LEX: CHECKS AT BCPS

	Search ID	Search Query	Number of Results
Checks at BCPs	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("obligation" OR "right" OR "coast" OR "port" OR "airport" OR "land" OR "passenger" OR "traveller" OR "individual" OR "goods" OR "luggage" OR "belongings" OR "risk assessment" OR "screening") In title and text, Search language: English	No Results
	20180905_B1	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results	1 Result

[196] https://eur-lex.europa.eu/advanced-search-form.html

		containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("obligation" OR "right" OR "coast") In title and text, Search language: English	
	20180905_B1_1	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("port" OR "airport" OR "land") In title and text, Search language: English	1 Result
	20180905_B1_2	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("passenger" OR "traveller" OR "individual") In title and text, Search language: English	1 Result
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("goods" OR "luggage" OR "belongings") In title and text, Search language: English	No Results
	20180905_B1_3	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("risk assessment" OR "screening") In title and text, Search language: English	1 Result
	20180905_B2	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("obligation" OR "right" OR "coast") In title and text, Search language: English	29 Results
	20180905_B3	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND ("obligation" OR "right" OR "coast") In title and text, Search language: English	67 Results
	20180905_B4	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border security" OR "border crossing" OR "border checkpoint") AND ("obligation" OR "right" OR "coast") In title and text, Search language: English	42 Results
	20180905_B5	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("BCP" OR "passport control") AND ("obligation" OR "right" OR "coast") In title and text, Search language: English	23 Results
	20180905_B6	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("port" OR "airport" OR "land") In title and text, Search language: English	20 Results

20180905_B 7	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND (“port” OR “airport” OR “land”) In title and text, Search language: English	56 Results
20180905_B 8	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND (“port” OR “airport” OR “land”) In title and text, Search language: English	42 Results
20180905_B 9	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“BCP” OR “passport control”) AND (“port” OR “airport” OR “land”) In title and text, Search language: English	24 Results
20180905_B 10	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND (“passenger” OR “traveller” OR “individual”) In title and text, Search language: English	32 Results
20180905_B 11	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND (“passenger” OR “traveller” OR “individual”) In title and text, Search language: English	103 Results
20180905_B 12	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND (“passenger” OR “traveller” OR “individual”) In title and text, Search language: English	67 Results
20180905_B 13	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“BCP” OR “passport control”) AND (“passenger” OR “traveller” OR “individual”) In title and text, Search language: English	48 Results
20180905_B 14	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND (“goods” OR “luggage” OR “belongings”) In title and text, Search language: English	2 Results
20180905_B 15	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND (“goods” OR “luggage” OR “belongings”) In title and text, Search language: English	8 Results
20180905_B 16	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND (“goods” OR “luggage” OR “belongings”) In title and text, Search language: English	9 Results
20180905_B 17	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“BCP” OR “passport control”) AND (“goods” OR “luggage” OR “belongings”) In title and text, Search language: English	1 Result
20180905_B 18	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs")	29 Results

		AND (“risk assessment” OR “screening”) In title and text, Search language: English	
	20180905_B19	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND (“risk assessment” OR “screening”) In title and text, Search language: English	92 Results
	20180905_B20	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND (“risk assessment” OR “screening”) In title and text, Search language: English	52 Results
	20180905_B21	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: (“BCP” OR “passport control”) AND (“risk assessment” OR “screening”) In title and text, Search language: English	43 Results

TABLE 6: DATABASE SEARCHES CONDUCTED IN EUR-LEX: MULTI-AGENCY COOPERATION

Search ID		Search Query	Number of Results
Multi-agency cooperation	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR “border security” OR “border crossing” OR “border checkpoint” OR “BCP” OR “passport control”) AND ("Multi-agency cooperation" OR "International cooperation" OR "third-countries cooperation" OR "neighbouring countries cooperation" OR "cross-border information sharing" OR “data protection” OR “GDPR” OR “privacy” OR “fundamental rights”) In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR “border security” OR “border crossing” OR “border checkpoint” OR “BCP” OR “passport control”) AND ("Multi-agency cooperation" OR "International cooperation" OR "third-countries cooperation") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR “border security” OR “border crossing” OR “border checkpoint” OR “BCP” OR “passport control”) AND ("neighbouring countries cooperation" OR "cross-border information sharing" OR “data protection”) In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR “border security” OR “border crossing” OR “border checkpoint” OR “BCP” OR “passport control”) AND (“GDPR” OR “privacy” OR “fundamental rights”) In title and text, Search language: English	No Results
	20180905_C1	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results	1 Result

	containing: ("border authorities" OR "border guard" OR "customs") AND ("Multi-agency cooperation" OR "International cooperation" OR "third-countries cooperation") In title and text, Search language: English	
20180905_C2	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND ("Multi-agency cooperation" OR "International cooperation" OR "third-countries cooperation") In title and text, Search language: English	1 Result
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("border security" OR "border crossing" OR "border checkpoint") AND ("Multi-agency cooperation" OR "International cooperation" OR "third-countries cooperation") In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 05/09/2018, Results containing: ("BCP" OR "passport control") AND ("Multi-agency cooperation" OR "International cooperation" OR "third-countries cooperation") In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 10/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("neighbouring countries cooperation" OR "cross-border information sharing" OR "data protection") In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 10/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND ("neighbouring countries cooperation" OR "cross-border information sharing" OR "data protection") In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 10/09/2018, Results containing: ("border security" OR "border crossing" OR "border checkpoint") AND ("neighbouring countries cooperation" OR "cross-border information sharing" OR "data protection") In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 10/09/2018, Results containing: ("BCP" OR "passport control") AND ("neighbouring countries cooperation" OR "cross-border information sharing" OR "data protection") In title and text, Search language: English	No Results
20180911_C3	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("GDPR" OR "privacy" OR "fundamental rights") In title and text, Search language: English	4 Results
20180911_C4	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND ("GDPR" OR "privacy" OR "fundamental rights") In title and text, Search language: English	3 Results
	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border security" OR "border crossing" OR "border	No Results

		checkpoint") AND ("GDPR" OR "privacy" OR "fundamental rights") In title and text, Search language: English	
	20180911_C5	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("BCP" OR "passport control") AND ("GDPR" OR "privacy" OR "fundamental rights") In title and text, Search language: English	3 Results

TABLE 7: DATABASE SEARCHES CONDUCTED IN EUR-LEX: INTERACTION WITH TRAVELLERS

Search ID		Search Query	Number of Results
Interaction with travellers	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("travellers trust" OR "travellers rights" OR "data protection" OR "privacy rights" OR "data collection" OR "personal data" OR "passenger rights" OR "GDPR" or "privacy" OR "fundamental rights") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("travellers trust" OR "travellers rights" OR "data protection") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("privacy rights" OR "data collection" OR "personal data") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("passenger rights" OR "gdpr") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs" OR "border police" OR "border management" OR "border control" OR "border security" OR "border crossing" OR "border checkpoint" OR "BCP" OR "passport control") AND ("privacy" OR "fundamental rights") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("travellers trust" OR "travellers rights" OR "data protection") In title and text, Search language: English	No Results
	-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results	No Results

	containing: ("border police" OR "border management" OR "border control") AND ("travellers trust" OR "travellers rights" OR "data protection") In title and text, Search language: English	
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND ("travellers trust" OR "travellers rights" OR "data protection") In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“BCP” OR “passport control”) AND ("travellers trust" OR "travellers rights" OR "data protection") In title and text, Search language: English	No Results
20180911_D1	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND ("privacy rights" OR “data collection” OR “personal data") In title and text, Search language: English	2 Results
20180911_D2	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND ("privacy rights" OR “data collection” OR “personal data") In title and text, Search language: English	3 Results
20180911_D3	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND ("privacy rights" OR “data collection” OR “personal data") In title and text, Search language: English	3 Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“BCP” OR “passport control”) AND ("privacy rights" OR “data collection” OR “personal data") In title and text, Search language: English	No Results
20180911_D4	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND (“passenger rights” OR “GDPR”) In title and text, Search language: English	2 Results
20180911_D5	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND (“passenger rights” OR “GDPR”) In title and text, Search language: English	1 Result
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND (“passenger rights” OR “GDPR”) In title and text, Search language: English	No Results
-	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“BCP” OR “passport control”) AND (“passenger rights” OR “GDPR”) In title and text, Search language: English	No Results
20180911_D6	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border authorities" OR "border guard" OR "customs") AND (“privacy” OR “fundamental rights”) In title and text, Search language: English	25 Results

	20180911_D7	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: ("border police" OR "border management" OR "border control") AND (“privacy” OR “fundamental rights”) In title and text, Search language: English	40 Results
	20180911_D8	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“border security” OR “border crossing” OR “border checkpoint”) AND (“privacy” OR “fundamental rights”) In title and text, Search language: English	30 Results
	20180911_D9	Domain: All, Subdomain: All documents, Date: All dates, From: 01/01/2007, To: 11/09/2018, Results containing: (“BCP” OR “passport control”) AND (“privacy” OR “fundamental rights”) In title and text, Search language: English	22 Results