PERSONA Deliverable D1.3: PERSONA benchmark for the assessment process

Casiraghi, Simone; Kloza, Dariusz; Konstantinou, Ioulia; Calvi, Alessandra; Burgess, James Peter

Publication date:
2020

Document Version:
Final published version

Privacy, Ethical, Regulatory and SOcial
No-gate crossing point solutions Acceptance

D1.3: PERSONA benchmark for the assessment process

WP1: Requirements for Privacy, Ethical, Regulatory and Social No-Gate crossing point technology Acceptance
Lead beneficiary: VUB

Delivery date: May 2020
Dissemination level: Public

Project title: PERSONA - Privacy, Ethical, Regulatory and SOcial No-gate crossing point solutions Acceptance
Duration: 1 September 2018 - 28 February 2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787123.

Document information

Document status	
Document lead	Simone Casiraghi, Dariusz Kloza, Ioulia Konstantinou, Alessandra Calvi, James Peter Burgess (VUB)
Internal reviewer	BRZ: Carl-Markus Piswanger, Christian Libert SMOI: Vesna Jancic CEL: Antonio Carnevale
Type	Report
Work Package	WP1: Requirements for Privacy, Ethical, Regulatory and Social No-Gate crossing point technology Acceptance
Task(s)	T1.4: Definition of PERSONA requirements
Deliverable number and title	D1.3: PERSONA benchmark for the assessment process
Due date	M12, August 2019
Delivery date	06 May 2020 (re-submission)
Distribution	PERSONA consortium, European Commission

Document history	
Versions	*v0.1 VUB, 04/07/2019, definition of table of content* *v0.2 VUB, 05/07/2019, further work on table of content* *v0.3 VUB, 19/07/2019, first draft of chapters 1 and4* *v0.4 VUB, CEL 25/07/2019, refinement of chapter 4 and draft of chapter 3* *v0.5 PRIO, SPA 30/07/2019, contributions to chapter 1 and 2* *v1.1 VUB, 12/08/2019s, complete draft of chapters 5, 6, 7* *v1.3 VUB, 22/08/2019, first full draft of the document for internal review* *v1.4 BRZ, 23/07/2019, general comments* *v1.5 SMOI, 27/08/2019, general comments* *v2 VUB, 29/08/2019, consolidated version for the consortium* *v2.1 VUB, 30/08/2019, final proofreading and editing* *v2.5 VUB, 31/08/2019, final version* *v2.6 VUB 06/05/2020, change level of confidentiality*
Contributions	SPA: Philip Ensgtröm; section 2.1.1 and general comments.
	PRIO: Kristoffer Lidén; chapter 2 general contributions, review of chapter 4.
	CEL: Antonio Carnevale, Maria Pia Verzillo; chapter 3 and revision of chapter 4.

Project partners

Logo	Partner	Country	Short
	Vrije Universiteit Brussel	Belgium	VUB
	Institutt for Fredsforskning Stiftelse	Norway	PRIO
	Cyberethics Lab Srls	Italy	CEL
	Atos Spain Sa	Spain	ATOS
	Inov Inesc Inovacao – Instituto de Novas Tecnologias	Portugal	INOV
	Queen Mary University of London	UK	QMUL
	Polismyndigheten Swedish Police Authority	Sweden	SPA
	Bundesrechenzentrum Gmbh	Austria	BRZ
	Ministarstvo Unutrasnjih Poslova Republike Srbije	Serbia	SMOI
	Ministry of Public Security	Israel	MOPS-INP
	RISE Research Institutes of Sweden	Sweden	RISE

Project website

http://www.persona-project.eu

List of abbreviations

AFIS	Automated Fingerprint Identification Systems
AFSJ	Area of Freedom, Security and Justice
API	Advanced Passenger Information
CBS	Critical Border Studies
CIR	Common Identity Repository
CIS	Custom Information System
DoA	Description of the Action
DPIA	Data Protection Impact Assessment
DPIA	Data Protection Impact Assessment
Dxy	Deliverable
ECRIS-TCN	European Criminal Records Information System
EDPS	European Data Protection Supervisor
EES	Entry Exit System
ELSA	Ethical, Legal and Social Aspects
ESP	European Search Portal
ETIAS	European Travel Information and Authorisation System
EUDPR	Data Protection Regulation for European Institutions
EURODAC	European Asylum Dactyloscopy Database
EUROSUR	European Border Surveillance System
FMR	False Matching Rate
FNIR	False Negative Identification Rate
FNMR	False Non-Matching Rate
FPIR	False Positive Identification Rate
FTER	Failure to Enrol Rate
GDPR	General Data Protection Regulation
GDPR	General Data Protection Regulation
LEA	Law Enforcement Authority
LED	Law Enforcement Directive
LR	Legal Requirement
MID	Multiple Identity Detector
PNR	Passenger Name Records
RRI	Responsible Research and Innovation

SBC	Schengen Borders Code
SCT	Social Cognitive Theory
SIS	Schengen Information System
SLTD	Stolen and Lost Travel Documents
TAM	Technology Acceptance Model
TCN	Third Country National
TDAWN	Travel Documents Associated with Notices
TRA	Theory of Reasoned Action
UAV	Unmanned Air Vehicles
UTAUT	Unified Theory of Acceptance and Use of Technology
VIS	Visa Information System
WP	Work Package

Executive summary

Building on the outcomes from deliverables D1.1 and D1.2, this deliverable constitutes a report on the identification and elaboration upon the relevant ethical, legal and other regulatory and social acceptance requirements. The aim is to establish a "benchmark" against which the impacts of the selected no-gate crossing point solutions will be assessed. The requirements listed in the benchmark will guide the development of the tailored-down impact assessment method (D3.1 and 3.2, first and final version, respectively), as well as the assessor to carry out such method. The two deliverables (D1.3 and D3.1/D3.2), therefore, should be read in conjunction.

If necessary, updates to the current benchmark (especially regarding the current regulatory framework for border management) will be included as an annex in the next version of the impact assessment method (D3.2, due M24).

The components of the benchmark will focus on the requirements applicable in the European Union, concerning: (1) the technical requirements of (some) of the latest border crossing technologies; (2) individual perception of emerging technologies and border security; (3) European ethical principles tailored to the field of border technologies; (4) relevant EU law, the Council of Europe's frameworks, and selected national frameworks, notably of those EU Member States where the field assessments will be used.

The original title of the deliverable (*PERSONA requirements, risks and mitigation measures*) has been changed to *PERSONA PERSONA benchmark for the assessment process* to match the task description (T1.4). Risks and mitigation measures will be dealt separately in D1.4 (due in M30).

Table of contents

1 Introduction

1.1 General intro

Effective border management through border-less crossing technologies has to satisfy two sets of criteria. On the one hand, it has to deliver on technical requirements (functional, non-functional and security requirements) of the initiative (including efficiency); on the other hand, it has to address the evolving ethical and legal requirements, and public acceptance of them. The goal of the assessment process to be developed within the PERSONA project is to assess a given border management solution against both sets of criteria in an integrated manner, and to reconciliate the seemingly competing goals. In order to identify the requirements (technical, social, ethical, legal) against which a given borderless crossing technologies will be assessed, the present deliverable will elaborate a 'benchmark' which will guide the development of the impact assessment method in D3.1 and D3.2.

This report reflects the law as it stood on 31 August 2019.

1.2 Key concepts in impact assessment

1.2.1 Impact assessment

An impact assessment (IA), in general terms, is a "tool used for the analysis of possible consequences of an initiative on a relevant societal concern or concerns, if this initiative can present dangers to these concerns, with a view to support the informed decision-making whether to deploy this initiative and under what conditions, ultimately constituting a means to protect these concerns".[1]

Different types of impact assessment have grown out of new threats to individuals and emerging societal concerns. Three among the most established types of impact assessments are particularly relevant for PERSONA, i.e. Data Protection Impact Assessment (DPIA), Privacy Impact Assessment (PIA) and ethical impact assessment (eIA).

Below reproduced are definitions for each IA type to clarify their characteristics and the differences among them:

- **Data Protection Impact Assessment:** A Data Protection Impact Assessment […] method aims to identify the main risks of a project with respect to the rights of data subjects concerning their personal data. It is a systematic process to elicit threats to the privacy of individuals, identify the procedures and practices in place to mitigate these threats, and document how the risks were addressed in order to minimise harm to data subjects.[2]
- **Privacy Impact Assessment:** Privacy impact assessment is a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal. An alternative definition might be that a privacy impact assessment is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated.[3]

[1] (Kloza et al., 2017).
[2] (Alnemr et al., 2016) p. 60.
[3] (Stewart, 1996) p. 61.

- **Ethical Impact Assessment:** […] ethical impact assessment […] could [be] used by those developing new technologies, services, project, policies or programmes as a way to ensure that their ethical implications are adequately examined by stakeholders before possible deployment and so that mitigating measures can be taken as necessary [4]

1.2.2 Benchmark

The term '**benchmark'**, in English, usually refers to three meanings: a "standard by which something is evaluated or measured"; "surveyor's mark made on some stationary object and shown on a map; used as a reference point" or a "computer program that is executed to assess the performance of the runtime environment".[5] In this deliverable, we adopt the first meaning.

Our choice is in line with how other disciplines use the term 'benchmarking'. In business, 'benchmarking' refers to the process of comparing your results to peers in your industry, e.g. compare your best practices to those of a company you want to be like, or compare performance measures.[6]

Similarly, in the context of impact assessment, we call benchmark 'a standard or reference by which an impact is assessed'. A benchmark in this case could have to do with environment (biophysical or human), ethics, privacy, personal data or public health.

A proposed (envisaged) '**initiative'** – be it a product, service or a piece of legislation (small scale) or policy, programme (large scale) – is the object of assessment process and it is evaluated against a benchmark, or benchmarks. In some instances, an initiative is assessed at a macro-level, e.g. entire approach to a given concern. A method, given the nature of the initiative, defines the benchmark, either precisely or (deliberately) vaguely, requiring a single or multiple components of the benchmark in a single process of assessment. Alternatively, multiple initiatives can be assessed against a single benchmark.

For the purpose of PERSONA, four domains of the benchmark have been identified, divided into two groups:

1) Technical requirements. Including the systems' functional, non-functional and security requirements, as listed in D1.2. These requirements will be discussed in Chapter 2;
2) Constraints on the technical requirements, including:
    2.1. Social acceptability, which will be discussed in Chapter 3;
    2.2. Ethics principles, which will be dealt with in Chapter 4;
    2.3. Legal and otherwise regulatory requirements regarding:
        2.3.1. Human rights (especially privacy and data protection), analysed in Chapter 5 and
        2.3.2. Border management, which will be discussed in Chapter 6.

This distinction is of course artificial; as many of the requirements overlap with one another. In particular, security requirements will be part of technical requirements (in the sense of cybersecurity or computer security, cf. Section 2.1.2.3), of social acceptance (in the sense of 'human security' perception, cf. Section 3.5) and the legal requirements on border management (technical and security requirements related to the database, cf. Section 5.6).

[4] (Wright, 2011), p. 223.
[5] Oxford Dictionary of English.
[6] Cf. Online Business Dictionary at: http://www.businessdictionary.com/definition/benchmarking.html

1.2.3 Framework and method for impact assessment

The architecture of an impact assessment, besides the benchmark, consists of a framework and a method. These are supplemented by e.g. guidelines, templates or questionnaires.

A *framework* constitutes an "essential supporting structure"[7] or organisational arrangement for something, which, in this context, concerns the policy for impact assessment, and defines and describes the structure, principles and rules thereof.

In turn, a *method*, which is a "particular procedure for accomplishing or approaching something",[8] concerns the practice of impact assessment and defines the consecutive and/or iterative steps to be undertaken to perform such a process in accordance with the framework. An integrated impact assessment method is a method which combines different types of assessment (e.g. privacy, societal, data protection, environmental) in a single process, with a view of improving efficiency and adaptiveness.

The idea of considering and integrating ethical, legal and social concerns in PERSONA is in line with the ELSA and Responsible Research and Innovation (RRI) approach purported by the EU via the "Science with and for Society" Horizon 2020 objective.[9]

1.3 Structure of the deliverable

This deliverable is divided in two main parts. The first part is dedicated to technical requirements of border management and relative technologies. The second part will list constraints on the technical requirements of part 1. Such constraints will range from social acceptance to ethical principles and legal requirements (including human rights and border management legal statutes). In particular:

- Chapter 3 is about social acceptance requirements;
- Chapter 4 is about ethics requirements;
- Chapter 5 is about fundamental rights related legal requirements;
- Chapter 6 is about border management related requirements.

At the end of each chapter, a table summarizes and provides and ID for each requirement. Finally, to complete the picture of the legal requirements, an overview of the legal frameworks concerning border management and privacy and data protection in Israel and Serbia will be provided as an annex.

The multiple components of the benchmark prepare the ground for the impact assessment method that will be included in D3.1 and D3.2 (respectively, first and final version of the PERSONA impact assessment method).

[7] Oxford Dictionary of English.
[8] Oxford Dictionary of English.
[9] Cf. European Commission's portal at: https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society

Part I: Technical requirements

2 Technical requirements of contemporary practices of border management

2.1 Requirements defined by end-users

2.1.1 Summary

The purpose of a border control is to facilitate border authorities to enforce defined rules and regulations regarding the movement of people. The border authorities need to verify that the traveller satisfies the Schengen Borders Code in order to be admitted into the country. An “Entry Exit System” (EES) will be introduced in the European Union (EU) countries soon, where third country nationals will be registered. At entry fingerprints and facial images will be verified and alpha numeric information will be stored in a common EES-database. EES/EU member state will be required to identify and capture biometric data for every third country national entering or exiting the Schengen area. Due to logistics and asylum issues, a “pre-registration” called ETIAS (European Travel Information and Authorization System), similar to the United States’ ESTA (Electronic System for Travel Authorization) system will be introduced.

There are two main aspects of the border control, the actual identity of the traveller and the passport information of the traveller and finally to verify that these two identities match. The most trivial check is to compare the picture in the passport with the traveller, a speedy and non-secure check.

The passport needs to be verified in multiple ways to ensure against forgery or fraud, and the passport information must be compared against watchlists to make sure that the traveller is indeed authorized to enter.

Once the authenticity of the passport is established, the last step is to verify that the traveller is in fact the real beholder of the passport. Simply comparing the facial image is not enough, multimodal biometrics with several different techniques are required. Examples of techniques that can be used are, fingerprints, automatic facial recognition, iris or gait analysis. Having at disposal several different techniques to establish a traveller's identity enables the border control to adopt the level of intrusiveness of the techniques depending on the level of uncertainty.

By achieving a good identification several severe threats such as terrorism, human smuggling and trafficking, illegal migration, drug trafficking and other criminal activities can be limited. At the same time, the number of travelers and the number of checks needed is constantly increasing which also adds requirements on efficiency. A solution with a higher throughput will have a clear advantage over a slower one.

2.1.2 Technical requirements

In order to achieve such goals, end users are constrained by the technical requirements of the technologies they use. For a detailed review of the technical requirements considered within the PERSONA project, please refer to the list in D1.2. In D1.2 technical requirements are divided into:

- *Functional requirements*: they define the function of the systems involved; in this case the multiple systems that will be assessed in the PERSONA project;
- *Non-functional requirements*: requirements that set criteria which can be used to determine the operation of a system, rather than behaviour that is specific (functional);
- *Security requirements*: requirements defined for reasons of cybersecurity or computer security. This regards the protection of hardware, software, data, procedures of the system and also people interacting with it.

For the scope of this deliverable, it is impossible to list all possible technical requirements of borderless crossing technologies solutions, as the spectrum of these technologies is very wide. Therefore, the list of technical requirements below refers to the list of technologies considered in PERSONA, and merely reproduces the requirements already outlined in D1.2.

2.1.2.1 Functional requirements (FR)

Id	*Description*
FR1	Passport and fingerprints reader: The system will detect if the passenger tries to enter the e-Gate from the wrong direction
FR2	Passport and fingerprints reader: The document reader component will recognize the biographical data page of the normalized European biometric passport
FR3	Passport and fingerprints reader: The document reader component will recognize the type of travel document such as ePassport, e-national card, or others
FR4	Passport and fingerprints reader: The document reader component will read all the information available from the travel document
FR5	Passport and fingerprints reader: The document reader component will recognize if the biographic page of the document is impossible to be read
FR6	Passport and fingerprints reader: The document reader component will detect if the chip of the electronic travel document is not working
FR7	Passport and fingerprints reader: The system will recognize the physical or digital token
FR8	Passport and fingerprints reader: The system will read the information from the physical or digital token
FR9	Passport and fingerprints reader: The system will recognize the key characteristics of the visa such as number, issuing country, start date and validity date
FR10	Passport and fingerprints reader: The system will read the passenger's biographic information from the documents presented
FR11	Passport and fingerprints reader: The system will search for the legal terms and conditions under which a passenger is allowed to access to the country
FR12	Passport and fingerprints reader: The system will capture and process live biometric data to ensure compliance with the International Civil Aviation Organization (ICAO) biometric data
FR13	Passport and fingerprints reader: In case of detection of spoofing attempt, the system will not capture biometric data
FR14	Passport and fingerprints reader: The system will compare the biometric data being captured against the biometric data stored in the chip of the passenger's document that has been read

Id	*Description*
FR15	Passport and fingerprints reader: The system will provide a smart-phone solution to manage e-Gates
FR16	Passport and fingerprints reader: The system will only process one passenger at the same time in the e-Gate
FR17	Passport and fingerprints reader: The system will not allow the next passenger to start the registration process until the current passenger exits the e-Gate
FR18	Passport and fingerprints reader: In case that the passport chip includes the fingerprint of the owner, the system will ask the passenger to scan their correspondent fingerprint, in order to make a comparation
FR19	Passport and fingerprints reader: e-Gates will be ready to accept all EU ID cards that include a chip
FR20	Passport and fingerprints reader: The system will read the ePassport in all allowed positions
FR21	Passport and fingerprints reader: Information will be sent for 2nd line checks when errors appear during the verification process
FR22	Passport and fingerprints reader: The document reader component will use mechanical mechanisms to ensure the correct position of the travel document, and that it is not removed before the reading process is finished
FR23	Passport and fingerprints reader: The system will provide a final total score for the biometric recognition
FR24	Risk Support system: Cost/Benefit Assessment (CBA) will be used for evaluation; total expected costs will be compared with the total expected benefits in order to choose the best option from the pure economical point of view. This evaluation is quantitative
FR25	Risk Support system: The Qualitative Criteria Assessment (QCA) aims to integrate different non-tangible decision parameters into the evaluation process. Qualitative criteria are defined as “criteria of relevance for taking a decision which cannot be quantified by a certain physical or logical dimension in the same way that costs or quantities can be quantified”. Thus, this includes intangible criteria that are subjective
FR26	Risk Support system: There will be two methods implemented for QCA analysis. The first one is based on the use of utility functions and is called Utility Function Based Analysis (UFBA). The second method has been created by a modification of Thomas Saaty’s Analytic Hierarchy Process (AHP); it is called Modified AHP (MAHP)
FR27	Risk Support system: Financial costs analysis will be based on a defined combination of three elements: an asset, a threat and an alternative. Different kinds of financial costs for the alternative’s security measures will be identified; investment costs, operational costs and possible future benefits
FR28	Risk Support system: Alternatives for financial costs analysis; one predefined set of up to five alternatives will be assigned for making the cost-benefit assessment (CBA). Each security measure under each alternative will have investment cost, operational cost and future benefits
FR29	Risk Support system: Cost and Benefit Workdown Structure; a cost and benefit work-down structure will be defined for the cost-benefit assessment (CBA). It will be possible to tailor this structure if deemed necessary

Id	*Description*
FR30	Risk Support system: Aggregated costs. The different cost elements for all alternative's security measures will be aggregated to obtain a calculation of total cost during the considered lifetime
FR31	Risk Support system: Qualitative criteria database. There will be a database with a hierarchical structure of qualitative intangible (subjective) criteria from the political, social, personal and other perspectives describing potential positive or negative consequences of the security measures
FR32	Risk Support system: Qualitative criteria analysis (QCA-MAHP) will be based on a combination of an asset, a threat and a security measure alternative. A relative weight addressing its importance will be assigned to each category
FR33	Risk Support system: Alternatives for qualitative criteria analysis; one set of up to five alternatives will be assigned to the defined criteria. Under each criterion every alternative will be assigned a specific weight that will be pondered
FR34	Risk Support system: Aggregated values for alternatives; using the relative weights of the criteria and the alternatives, up to five, that has been chosen, a specific value will be calculated for each alternative's security measures
FR35	Risk Support system: Qualitative criteria analysis (QCA-MAHP) will be based on a combination of an asset, a threat and a security measure alternative. It will be possible to compare each category with all the others using a matrix. Additionally, each selected criterion for the selected category will be compared with each other using a matrix
FR36	Risk Support system: Aggregated Results (AGR); the aggregated result module will gather the results of the functional blocks: CBA and QCA (including both UFBA and MAHP analysis) and will deliver a summary report. The module will compare and rank the assessment results of the different security measures alternatives considered according to the given categories and criteria (for QCA) and the cost and benefit work-down structure (for CBA)
FR37	Risk Support system: Aggregated Results (AGR); the aggregated result module will gather the results of all functional blocks: CBA and QCA (including both UFBA and MAHP) and will deliver summary reports. The results will be: For each alternative of each security measure: graphics, figures and report of each assessment. For all security measures together: graphics and a report
FR38	Classification of objects: The system will be able to detect and track people and different objects (like bags and backpacks) using video footage in real time. This Classification of objects: detection will be possible using any COTS camera
FR39	Classification of objects: The system will provide the position of the objects detected if the camera used is able to send position metadata in Key-Length-Value (KLV) format
FR40	Detection of anomalous behaviour: The system will be able to detect anomalous behaviours using real time video footage. This detection will be possible using any COTS camera
FR41	Detection of anomalous behaviour: Detection will consist in the detection of human pose. System will be able to determine the position and movement of any number of people using a fixed camera.

Id	*Description*
FR42	Detection of anomalous behaviour: Camera will need to be calibrated to estimate position of people in the 3D space.
FR43	Heartrate remote detection: The system will be able to detect the heartbeat of people remotely using real time video footage. This detection will be possible using any COTS camera or even a webcam
FR44	Heartrate remote detection: The system will need people to be in front of the camera with the head and especially the forehead visible
FR45	Heartrate remote detection: The system will work at a maximum distance of half a meter
FR46	Heartrate remote detection: The system will be able to re-identify people and store and retrieve their heartrate to detect anomalies. Identification will be anonymous
FR47	Heartrate remote detection: The system will work with only one person at the same time
FR48	Multimodal detection: Multimodal detection system will use different biometrics parameters like face, gait and voice. The system will use all the biometrics or combination available
FR49	Multimodal detection: Multimodal detection system will implement an anti-spoofing module to avoid identification forgery attempts
FR50	Soft Biometrics: Detection system will extract anthropometric measurements and attributes to help with categorisation or recognition of people based on body geometry.
FR51	Face detection and recognition: System will be able to detect face of the person and recognise person's identity based on facial features and data extracted from passport and internal database system
FR52	People detection and tracking: System will be able to detect and track people in the video footage in order to provide important clues for anomalous behaviour detection or person search
FR53	Foreground and Background subtraction: System will extract all moving objects from the video footage for further video processing and object/person tracking
FR54	System will extract summary of events in the video using panoramic view in case of moving camera
FR55	System will detect and track distinctive region or pattern of interest in the video for identification of tracking of person or object of interest
FR56	System will be able to extract foreground information in the video footage from the background.
FR57	The system must verify if the user if is real passenger (if it is "alive")
FR58	Situational and operational context awareness REQUIRES that reported data are always provided with a timestamp and whenever applicable with information regarding the location of the reported data.
FR59	Spatial context MUST be expressed in a way to assure the visualization of the information location as a geo-marker over a map-based layout.
FR60	Extracted markers MUST be utilised to classify the nature and the importance of the detected event.
FR61	Sentiment analysis: system will use video in real time combined with voice recognition as input
FR62	Sentiment analysis: system will provide analysis of sentiment in real time

2.1.2.2 Non-functional requirements (NF)

Id	*Description*
NF1	Passport and fingerprints reader: The threshold for document capture and reading will be configurable
NF2	Passport and fingerprints reader: Design will enforce that only one passenger can use the e-Gate at a time
NF3	Passport and fingerprints reader: The information being transmitted to the passengers will show sequential steps for the passenger to follow (e.g., insert the document, look at the camera, remove the document, pass, etc.)
NF4	Passport and fingerprints reader: The system will avoid passenger to stop in the doors, eliminating the necessity of being (re)identified. The authorization to cross the border will be made while the passenger walks through the identification control
NF5	Passport and fingerprints reader: Expected throughput of the system will be significantly improved (less than 10s for 95%)
NF6	Passport and fingerprints reader: System will have a device in the identification kiosk to collect the fingerprints and compare then with the ones that are on the data bases (previously collected in the consulates or equivalent)
NF7	Passport and fingerprints reader: The system will attract the attention of the passenger towards the biometric capture process
NF8	Passport and fingerprints reader: The system will guide the passengers during all biometric capture process
NF9	Passport and fingerprints reader: The system physical layout will ensure adequate illumination of the face and, at the same time, will avoid creating shadows
NF10	Passport and fingerprints reader: The illumination system will not disturb the passenger; blinding the passenger, etc.
NF11	Passport and fingerprints reader: The passenger will fill in a form to collect their personal data that will be used to perform the analysis
NF12	Passport and fingerprints reader: Terminology in the Graphical User Interface will be familiar and understandable to the application user
NF13	Passport and fingerprints reader: The layout conventions for how information is read shall be followed. Western countries display the layout from left-to-right and top-to-bottom
NF14	Risk Support system: Aggregated Results (AGR); the aggregated result module will gather the results of the combined assessments made for the different security measures alternatives considered during the analysis
NF15	Risk Support system: Colour rules for the interface; the interface will use colours that are far enough apart and that are clearly distinguishable in the display.
NF16	Risk Support system: Control of the application; users of the system must have full control of the application. The user interface will always clearly indicate the status of the system
NF17	Risk Support system: Feedback to the user; after any important user action, the system will provide clear and informative feedback with the results of the action
NF18	Risk Support system: Notification area will be available for displaying control, warning and error information messages whenever deemed necessary

Id	*Description*
NF19	Risk Support system: Efficiency; the application will enable the users to carry out their tasks efficiently. The application will not display redundant information unless it is deemed needed for specific safety, clarity or task performance reasons
NF20	Risk Support system: User errors notification will be clear and informative
NF21	Risk Support system: Visual elements (including graphics, icons, buttons and labels) will be organized following standard usability rules
NF22	Risk Support system: Forms will be used to provide the user with the possibility to enter data which is logically associated with a certain user task. Mandatory fields will be properly indicated in the forms
NF23	Risk Support system: The application default language will be in English.
NF24	Risk Support system: It will be possible to storage and retrieve the assessments even if partial
NF25	Risk Support system: CBA configuration. Assessment parameters and cost-benefits subcategories will be configurable in the cost and benefit breakdown structure
NF26	Risk Support system: QCA configuration. Assessment parameters and qualitative criteria (categories and their subcategories) will be configurable
NF27	Risk Support system: Aggregated results will be obtainable from any number of the assessments without any mandatory order of analysis or a minimum number of assessments performed
NF28	Detection of anomalous behaviour: Footage gathered for abnormal behaviour and classification modules will respect legal privacy aspects
NF29	Heartrate remote detection: Footage gathered for heartrate detection module including re-identification will respect legal privacy aspects
NF30	Multimodal detection: Footage gathered for the classification module will respect legal privacy aspects
NF31	Soft biometrics: The parameters for anthropometric measurements and attributes will be configurable
NF32	Soft biometrics: Footage gathered for soft biometrics will respect legal privacy aspects
NF33	Foreground and background subtraction: System will be able to operate in real-time speed
NF34	Foreground and background subtraction: Footage gathered for foreground and background subtraction will respect legal privacy aspects
NF35	People detection and tracking: Footage gathered for people detection and tracking will respect legal privacy aspects
NF36	Face detection and recognition: System will provide accuracy of the recognition in order to assist in decision making
NF37	Face detection and recognition: Footage gathered for face detection and recognition will respect legal privacy aspects
NF38	Distinctive region or pattern of interest: System will allow user to input specific pattern of interest by user.
NF39	Distinctive region or pattern of interest: Footage gathered for distinctive region or pattern of interest will respect legal privacy aspects
NF40	Video summarisation: System will enable user to choose between classical vs panoramic view of the video summary

Id	*Description*
NF41	Video summarisation: Footage gathered for video summarisation will respect legal privacy aspects
NF42	All: The system will contribute for differentiation of passenger groups without discrimination.
NF43	All: System will detect or contribute to verify passenger identification, detect and prevent dangerous goods from being transported by passengers or baggage.
NF44	All: The system should contribute to better passenger experience
NF45	All: The system should contribute to “one stop security”
NF46	All: The system should contribute to cost efficiency (better allocation of staff)
NF47	All: The system should contribute to enhanced capability (reduce time for completion of measures)
NF48	All: The system should improve the high security level (increase knowledge about passengers)
NF49	The system will consider the dangerous goods listed in the IATA Dangerous Goods Regulations (DGR) (identify in Annex A and Annex B).
NF50	System will have a device an e-gate to identify the user and verify if the user is a passenger.
NF51	The system will monitor critical areas, through CCTV and video cameras, in order to analyse the passenger behaviour.
NF52	The system will support soft biometrics using anthropometric measurements
NF53	The system will support identification based on face detection and recognition
NF54	The system will support people detection and tracking.
NF55	To enhance the detection of moving objects, the system will support video manipulation (namely Robust foreground and background subtraction).
NF56	The system will support Panoramic video summarisation.
NF57	The system will support multimedia processing distinctive region or pattern of interest detection and tracking are supported.
NF58	The system will support Multifactorial biometric identification based on the use of video cameras (e.g. face, gait…)
NF59	The system will support remote heartrate detection using video cameras
NF60	The system object classification (e.g. people, bags,…) based in video cameras
NF61	The system will support abnormal behaviour detection (pre define situations) using video cameras.
NF62	The system will support Real Simple Syndication (RSS) for risk management of possible measures (web based)
NF63	The system will support people tracking (using cameras)
NF64	The system will support hyper-spectral image analysis
NF65	The system will support monitoring of body temperature
NF66	The system will support a Body/Tunnel Scanner (integrating different technologies).

2.1.2.3 Security related requisites

Id	*Description*
SR1	Passport and fingerprints reader: The document reader application will not retain any passenger's information. Information will be volatile
SR2	Passport and fingerprints reader: The system will authenticate if the machine-readable zones (text fields) matches the information stored in the document chip.
SR3	Passport and fingerprints reader: The system will check the expiration date of the document.
SR4	Passport and fingerprints reader: All transmission of passenger's data to the backend system will be done in accordance with the regulations regarding data privacy
SR5	Passport and fingerprints reader: The system will authenticate the security features included in the visa
SR6	Passport and fingerprints reader: The system will check the validity date included in the visa
SR7	Passport and fingerprints reader: All actions made with the application will be logged.
SR8	Passport and fingerprints reader: Data transmission will have enough physical and digital security
SR9	Soft Biometrics: All actions made with the system will be logged.
SR10	Soft Biometrics: Data transmission will have appropriate physical and digital security
SR11	Face detection and recognition: All actions made with the system will be logged.
SR12	Face detection and recognition: Data transmission will have appropriate physical and digital security
SR13	People detection and tracking: All actions made with the system will be logged.
SR14	People detection and tracking: Data transmission will have appropriate physical and digital security
SR15	Foreground and Background subtraction: All actions made with the system will be logged.
SR16	Foreground and Background subtraction: Data transmission will have appropriate physical and digital security
SR17	Distinctive region or pattern of interest: All actions made with the system will be logged.
SR18	Distinctive region or pattern of interest: Data transmission will have appropriate physical and digital security
SR19	Video summarisation: All actions made with the system will be logged.
SR20	Video summarisation: Data transmission will have appropriate physical and digital security
SR21	System will be developed in line with GPDR, namely Article 25, implement in such a way that safeguards privacy and data protection principles 'data protection by design' and 'data protection by default", namely: — The system SHALL secure certain internal data and services (i.e. personal data) from other data and system networks. — The system SHALL establish procedures to protect documents, computer media, information/data, and documentation from unauthorized disclosure, modification, removal, and destruction. The System shall establish measures to properly dispose of discarded or unused media.

Id	*Description*
	— The system SHALL support access control, and authorized users must comply with the requirements set by the specific laws of the country the system resides in. — The system MUST comply with existing business rules, regulations and legislation constraints. — Integrity: data MAY not be modified in an unauthorized way. For example, we need to be sure that data sent over a network arrives unaltered.

Part II: Constraints on the technical requirements

3 Social acceptance requirements

3.1 Introduction

One of the key aspects of PERSONA is developing a tailored method for assessing the impacts of the carefully selected current and new generation no-gate technologies against *social acceptance* issues. But, precisely, what is the meaning of 'societal acceptance' of a technology? And why for PERSONA is social acceptance so important to be compared with other chief aspects such as "ethics" and "regulation"?

To answer these questions, we will proceed in this paragraph as follows:

- In a first part, the conceptual history of "social acceptance" as impact benchmark for evaluating technology will be reconstructed (Section 3.2);
- In the second part, there will be outlined a very brief literature review of the most used approaches in literature to detect the social acceptance of users (Section 3.3).
- Going on, the argumentation will go more in specifics of PERSONA's context, explaining the approach of PERSONA to understand the social acceptance of no-gate technologies as insights in support of the definition of PERSONA method of impact assessment (Section 3.4).
- Finally, in the last paragraph we will go forward on, applying the previous theoretical framework to the architecture of the expected PERSONA questionnaire for user perception analysis. There will be benchmarked the criteria of social acceptance we will use in the questionnaire (Section 3.5).

3.2 Social acceptance of technology: A brief history of the concept

Social acceptance and technologies are entities that appear to be increasingly intertwined. Whether a device is considered "cool" or "smart" might influence impression and acceptance, and thus affect the willingness to use it – even when unwatched. Despite being highly useful and usable, some devices might also reveal information the user does not want to reveal, which might result in privacy breaches or stigmatization. In public spaces, interactions with an interface may affect or even intrude the social sphere of others, cause discomfort and social tension. According to some observers, the massive circulation of fake news on social media has co-caused historically consistent events such as Brexit or the presidential election of Donald Trump (Cambridge Analytica).[10]

Regardless of the veracity of these hypotheses, a fact is undeniable: social acceptance, understanding the reality, and impacts of technologies are factors that condition each other reciprocally. For this reason, the study of user perceptions is increasingly adopted through dedicated questionnaires in the research projects where emerging technologies are to be tested / demonstrated / evaluated.

But social acceptance has emerged only over last decades as an evaluative concept of technologies. When in 80' initial computers and artificial intelligence entered in people's homes and lives, "usability" and "utility" were considered the main features for assessing the user-friendly character of the novel devices (van de Poel Ibo & Lambèr, 2011). Researchers, developers, implementers, in improving the

[10] (Lovink, 2016).

machines, thought the technology as an artefact, as an external entity in the world. Devices were machines at most seen as external extension of the human body and for this reason, to make them more acceptable, it was enough to improve the control panel of their usability. Even when in 1994 Nielsen named "social acceptability" as an essential part of system acceptability (Nielsen, 1994), this novel concept remained a purely descriptive parameter in R&D of technology (Malhotra & Galletta, 1999). In this period, a certain technological positivism was dominating the scene, which has not allowed to consider technology as an interactive rationality of the "rise of the network society".(Castells, 1996) More progresses have taken place with the "technology acceptance research" that have been extended the acceptability to incorporate social factors (this progress is evident, for example, in the *Technology Acceptance Model* (TAM) (Adams, Nelson, & Todd, 1992).

Finally, the latest developments in the fields of social robotics and human-robot-interaction[11], ubiquitous computing and surveillance systems, mobile ICT apparatus have forced designers, experts, engineers and social scientists to reflect on social acceptance as a separate and autonomous corpus of evaluation for assessing the performance of emerging technologies not per se, rather always referring to the psychological, social, cultural, ethical models behind the human-technology interaction (Brey, 2017).

3.3 Overview of existing approaches and relate benchmarks

In the following section, a brief overview of the current approaches to study social acceptance. Most of this literature review is taken by the studies of Davis (1989) and Venkatesh et al. (2003).[12]

3.3.1 Theory of Reasoned Action (TRA)

Drawn from social psychology, TRA is one of the most fundamental and influential theories of human behaviour. It has been used to predict a wide range of behaviour. Davis et al. (1989) applied TRA to individual acceptance of technology and found that the variance explained was largely consistent with studies that had employed TRA in the context of other behaviour (Davis, 1989).

3.3.1.1 TRA benchmarks

Attitude Toward Behavior	An individual's positive or negative feelings (evaluative affect) about performing the target behavior (Ajzen & Fishbein, 1975).
Subjective Norm	The person's perception that most people who are important to him think he should or should not perform the behavior in question.[13]

3.3.2 Technology Acceptance Model (TAM)

TAM is tailored to IS contexts and was designed to predict information technology acceptance and usage on the job. Unlike TRA, the final conceptualization of TAM excludes the attitude construct in order to better explain intention parsimoniously (Venkatesh & Davis, 2000). TAM has been widely applied to a diverse set of technologies and users.

[11] (Feil-Seifer & Matarić, 2011)(Coeckelbergh, 2012).
[12] (Davis, 1989) (Venkatesh, Morris, Davis, & Davis, 2003).
[13] Ibid.

3.3.2.1 TAM benchmarks

Perceived Usefulness	The degree to which a person believes that using a particular system would enhance his or her job performance.[14]
Perceived Ease of Use	The degree to which a person believes that using a particular system would be free of effort.[15]
Subjective Norm	Adapted from TRA.

3.3.3 Social Cognitive Theory (SCT)

One of the most powerful theories of human behavior is social cognitive theory. Compeau and Higgins (1999) applied and extended SCT to the context of computer utilization (Compeau & Higgins, 1995). This model studied computer use but the nature of the model and the underlying theory allow it to be extended to acceptance and use of information technology in general.

3.3.3.1 SCT benchmarks

Outcome Expectations—Performance	The performance-related consequences of the behavior. Specifically, performance expectations deal with job related outcomes.[16]
Outcome Expectations—Personal	The personal consequences of the behavior. Specifically, personal expectations deal with the individual esteem and sense of accomplishment.
Self-efficacy	Judgment of one's ability to use a technology (e.g. computer) to accomplish a particular job or task.
Affect	An individual's liking for a particular behavior (e.g. computer use).
Anxiety	Evoking anxious or emotional reactions when it comes to performing a behavior (e.g., using a computer).

3.3.4 Unified theory of acceptance and use of technology (UTAUT)

The unified theory of acceptance and use of technology (UTAUT) and its extended theoretical frameworks are very popular and widely used to predict behavioural intention for the adoption of technology. Initial UTAUT derived from its predecessor models i.e. Technology Acceptance Model (TAM) and the Theory of Reasoned Action (TRA). To sum up, this approach created by Venkatesh et al. (2003)[17] is a method constructed around three determinants of usage direct expression of intention and behaviour, and one direct determinant of user behaviour. Gender, age, experience, and voluntariness of use are posited to moderate the impact of the four key constructs on usage intention and behaviour.

[14] (Davis, 1989).
[15] Ibid.
[16] Ibid.
[17] (Venkatesh et al., 2003) (Davis, 1989).

3.3.4.1 UTAUT benchmarks

Performance expectancy (PE)	User's expectation on the performance of technology influences his/her intention to adopt the technology.
Effort expectancy (EE)	Effort expectancy is defined as the degree of ease associated with the use of the system.
Social influence (SI)	Social influence is defined as the degree to which an individual perceives that important others believe he or she should use the new system.
Facilitating conditions (FC)	Facilitating conditions are defined as the degree to which an individual believes that an organizational and technical infrastructure exists to support use of the system.

3.4 Social "acceptance" and ethics "acceptability": PERSONA specific approach

In the PERSONA project, much emphasis is placed on the internal link between perceptions and social acceptance. This link is often mentioned. The goal is not to enter too much into the debate on the meaning of "perception" and on how it should be studied in relation of the understanding of social acceptance. In PERSONA the perceptions are assumed as those insights of travelers and end-users and they will be studied through questionnaires (D3.3) in order to understand the perception-related effects and side effects of no-gate crossing point solutions. The main point here is to stress the assumption that perceptions constitute in PERSONA the subjective and emotional status though which the acceptance of a given no-gate crossing point solution is "socialized".

The literature gave ample evidence of the importance of this nexus between emotion, sociality and values to assess "risky" technology.[18]

There are many philosophical and anthropological reasons to explain this mediation role that acceptance plays between perceptions and values, sociality and ethics. Firstly, technologies are increasingly becoming "ubiquitarian", distributed and decentralized systems[19]. Therefore, in a world where technology is no longer anthropomorphized (the cyborg, the humanoid), nor a concrete object delimited in the world (a simple machine), rather an invisible servant or, as Weiser argued in 1996, a "ubiquitous computing" (Weiser, 1993), perceptions become the main empirical channel for accepting the reality. The second reason is referred to role of "technological mediation".[20] Technologies help to shape the relations between human beings and the world. Rather approaching technologies as material objects opposed to human subjects, or as mere extensions of human beings, technologies are mediators of human-world relations. From this point of view, therefore, the ways people accept technologies are important phenomena to be studied because they incorporate, more or less unreflectedly, the levels of interaction between human beings and the world. By studying the technological imagination of people, we understand the values people give to the society where they live or want to live, and, accordingly, the moral and ethical constrains to which people rely on to govern the complexity of this world.

[18] (Roeser, 2010).
[19] Carnevale, A. and Occhipinti, C. (2019) "Ethics and Decisions in Distributed Technologies: A Problem of Trust and Governance Advocating Substantive Democracy", International conference *DECON 2019*.
[20] (Ihde, 1990) (Latour, 1994).

It seems now clearer that acceptance is a cluster concept with many meaningful nuances that can refer, on the one hand, to the world of subjective perceptions and emotional states, and, on the other hand, to the shared human values and therefore to the ethical principles of society. In order to set the PERSONA requirements in the right light of this nuance, we think is opportune to make distinction by introducing the difference between "**acceptance**" and "**acceptability**".

Taebi detects as the terms acceptance and acceptability have been used in different senses throughout the literature in the social sciences and humanities.[21] "Acceptance" has more to do with sociality, while "acceptability" more in relations with principles and ethics. He makes the following distinction:

- Social acceptance refers to the fact that a new technology is accepted—or merely tolerated—by a community.
- Ethical acceptability refers to a reflection on a new technology that takes into account the moral issues that emerge from its introduction.

A similar distinction is applied, for example, in the PARENT research project,[22] in which the social acceptability protocol (D3.2) has provided guiding principles for the implementation and running of Living Labs in the PARENT Project's Pilots. In the mentioned deliverable, the distinction in some way acts against the background of the internal project requirements, as shown in the following passage

1) There is a principle of 'acceptability' qua legitimacy and ethical 'rightness' of policies, regulations, applications, technologies and developments which we try to pursue in the three PARENT Pilots. That is to say, that there is an ethically and socially acceptable way to innovate energy systems, regardless of the extent to which such innovation is accepted at the market or household levels. This may be termed a normative level, that nevertheless refers to empirically verifiable events, especially as these make up individual decision making and reasoning about smart meters and smart energy;
2) There is a de facto 'acceptance', mainly in terms of the ways in which people, in their everyday practices interact with energy monitoring devices and applications: whether or not they actually change behaviour, and whether or not new forms of interactions stabilize and can be discerned. For instance, people enjoying the use of energy platform regardless of the fact that they are required to share private consumption data which they would not be willing to share had the platform not existed.

PERSONA benchmarks on acceptance move from this background where "social acceptance" refers to perception and human relationships while "ethics acceptability" refers to principles and societal values.

PERSONA benchmarks are built on a measurement progressiveness that puts on the basis the primary and most immediate perception of the no-gate solutions (their facilitating capacity) and then, increasingly going up in the quality of the experience, it passes through other types of perceptions that define acceptability in a range that goes from subjective perceptions to more socialized ones that have to do with societal models. Below we illustrate the diagram of the benchmarks:

[21] (Taebi, 2017).
[22] Cf. http://www.parent-project.eu/.

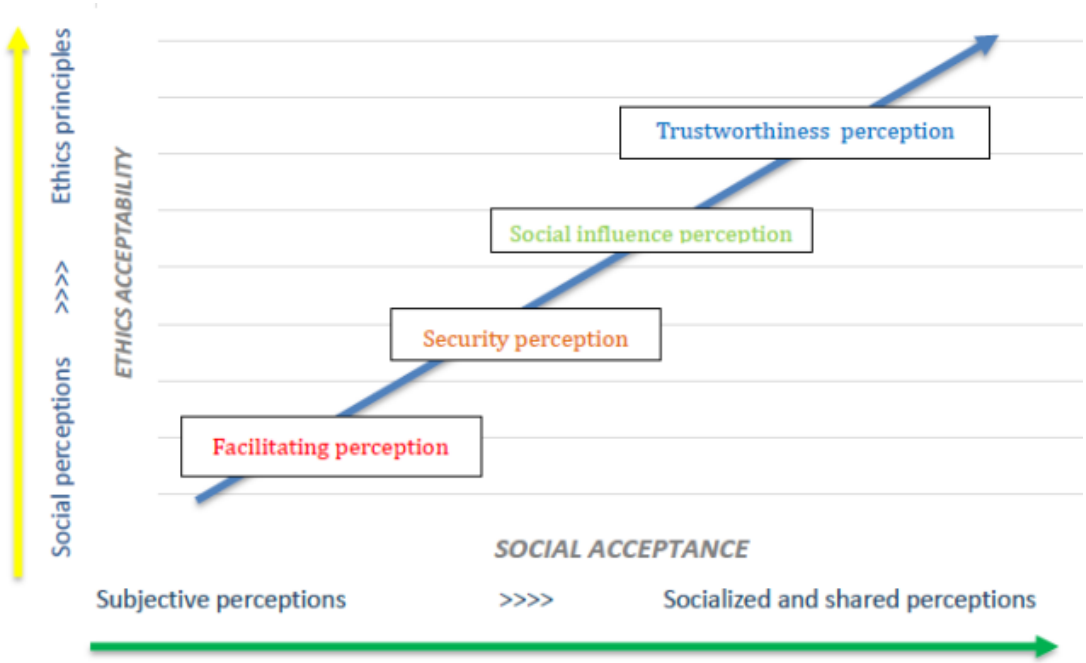

Figure 1 - Graphics of PERSONA acceptance benchmarks

3.5 Benchmark

1. *Facilitating perception*

This benchmark is deduced by the study Venkatesh et al. (2003).[23] Facilitating perceptions are defined as the degree to which an individual believes that an organizational and technical no-gate infrastructure exists to facilitate crossing point solutions.

2. *Security perception*

Security perceptions are expectancy defined as the degree of security associated with the use of the no-gate technologies as secure crossing point solutions. By security here we refer to the concept of 'human security', as opposed to the traditional security paradigm of 'state security' or 'national security'. Human security paradigm states that the proper referent for security is the individual rather than the state.[24]

It is important to note that the increase of perception of security does not necessarily increases the risks associated. For instance, having military personnel patrolling a border crossing point may increase the feeling of security, but it does not necessarily decrease the risk of possible terrorist attacks.

3. *Social influence perception*

This benchmark is deduced by the study Venkatesh et al. (2003).[25] Social influence perceptions are defined as the degree to which an individual perceives that important others or society as such believe he or she should use the no-gate system.

[23] (Venkatesh, Morris, Davis, & Davis, 2003).
[24] (Dratwa, 2014) p. 65.
[25] (Venkatesh et al., 2003).

4. Trustworthiness perception

This benchmark is deduced by the report *Ethics guidelines for trustworthy AI* recently delivered by the High-Level Expert Group.[26] Trustworthiness perceptions are defined as the degree to which an individual considers that a no-gate technology is plied in acceptable ways that go beyond their security and social influence. This benchmark refers to the imagination of the developers rather than to the machines. No-gate solutions are acceptable to the extent that developers/practitioners/operators ensuring in their use the compliance with all applicable laws and regulations, demonstrating respect for, and ensure adherence to, ethical principles and values.

These social acceptance requirements can be summarized in the following table:

Id	***Description***
SAR1	Facilitating perception requirement 1: users find the system useful and more efficient to cross the border.
SAR2	Facilitating perception requirement 2: users have the resources necessary to use the system.
SAR3	Security perception requirement 1: users find the system more secure from a data protection and privacy perspective.
SAR4	Security perception requirement 2: users find the system more secure against threats to human security such as terrorism.
SAR5	Social influence perception requirement 3: the organization is supportive in helping people using the system.
SAR6	Trustworthiness perception requirement 1: the users trust the system will correctly identify them.
SAR7	Trustworthiness perception requirement 2: the users trust the authorities will manage their personal data responsibly.
SAR8	Trustworthiness perception requirement 3: the users trust the system is compliant with applicable law and regulations.

[26] Cf. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

5 Ethical requirements

5.1 Introduction

5.1.1 Why ethics?

As noted in the section before, it is not enough that a new borderless crossing technology is simply 'accepted' by (some) of its users. Even if it is accepted, it might still be the case that the given technologies clash with some higher-level ethical principles.

To delve into this issue, this section deals with 'what kind of ethics' would be relevant for the integrated impact assessment method of PERSONA. In recent years, emerging technologies have become a major interest for the field of (applied) ethics. The uncertainty of technological developments, and the possible disruptive effects thereof, such as in the field of borderless crossing technologies for travellers and border control authorities, call for flexible approaches that could help to timely predict negative and positive impacts of a given initiative. The new area of ethics of technology has emerged with a plethora of different approaches which combine more traditional ethical analysis to foresight analysis.[27]

Among these approaches, generic frameworks for ethical impact assessment have been proposed to ensure that ethical impacts of a given initiative are identified and addressed (Wright & Mordini, 2012). Elaborating on these works, the goal of PERSONA is to include 'ethics' in its tailor-made integrated impact assessment method for borderless crossing technologies (D3.1). This section will provide an ethics benchmark against which the impacts of such technologies on ethical principles will be evaluated.

5.1.2 What is an ethics benchmark?

Establishing an ethics benchmark is difficult since ethics is, according to some definitions, a discursive practice that cannot be 'entrenched' in an unchanging or rigid set of standards or yes/no questions. To assess a given border technology ethically, it is nevertheless necessary to provide the assessor (who is not necessarily acquainted with academic discussions in ethics of technology) with tools that can guide her throughout the assessment process. Such guidance can be provided by general principles, that still need to be specific to the context of border crossing and the EU cultural landscape. In this sense, commonly or widely accepted general principles would be the 'standards' against which a given technology is assessed, in line with our definition of benchmark in section 1.2 (for instance: borderless crossing technologies need to respect autonomy; does the current initiative do so?).

The first step to create such a list of general principles (against which the impacts of borderless crossing technologies will be assessed) is to look in detail into well-known ethical principle-based methods and contrast/integrate them with EU principles recently developed by expert groups appointed by the European Commission (EC). The second step will be to come up with an integrated list of principles and further unpack each principle in its subprinciples and issues that could arise in the contexts relevant for PERSONA. The resulting list of issues will constitute the basis to develop the questionnaire to be included in the first version of the method in D3.1.

[27] (Brey, 2017).

5.1.3 Method: A principle-based method

The method used to establish this ethics benchmark is a principle-based one (otherwise known, originally with a negative connotation, as 'principlism'). Simply put, it consists of a set of principles which claim *prima facie* moral obligations, that are in turn put into practice by being specified for a given context (in PERSONA's case: border control).[28] Principles are action guides like rules, but they differ from the latter insofar as the guidance that principles provide is more general or abstract.[29] This method has been adopted in many different fields (above all: biomedical research) since it offers a practical guidance to solve ethical dilemmas without being stuck in theoretical debates about what is the most appropriate approach to follow at a normative level (notably deontology, utilitarianism or virtue ethics).

The PERSONA benchmark will include ethical principles and categorize them in a similar way as those delineated by Beauchamp & Childress.[30] In their *Principles of Biomedical Ethics,* Beauchamp & Childress developed four principles (i.e. autonomy, beneficence, non-maleficence and justice) in the context of bioethics in the United States. In particular, their principles originated from the work of the "National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research" which was later presented in the Belmont Report (1979).[31] At that time, as scandals in biometrics research were taking place,[32] new understandable and up to date frameworks and guidelines were needed to guide medical researchers and at the same time protect patients and research subjects. Similarly, today, given the potential ethical impacts of new generation border technologies, e.g. discrimination or data protection concerns resulting from the use of facial recognition or other airport security measures, ethics guidelines and frameworks are needed to guide technology developers and LEAs to use border crossing technologies responsibly. In order to improve Beauchamp & Childress' categorization and tailor it to the field of border crossing and to the European context, we will integrate it with the human rights delineated in the Charter of Fundamental Rights of the European Union (CFR),[33] as well as with some recent EC's guidelines and reports, and their relative principles, in the next sections.

5.1.4 Justification

There are several justifications for the use of this approach, already largely used in bioethics, in the context of border control technologies.

First of all, there is a practical need to consider. This approach was chosen for its usability appeal. It can be easily understood by assessors who are not familiar with normative moral theories or academic discussions as the principles are rooted in "common morality", i.e. "a set of basic moral norms that in the course of human history, have proved to be of fundamental importance for the prevention of harm to, and the general flourishing of, communities and societies".[34] In other words, the strength of this approach is that no specific normative theory is chosen, and actually the principles are developed to find an agreement between the main competing theories of deontology and utilitarianism (or

[28] (T. L. Beauchamp & Rauprich, 2015).
[29] (Horton, 2002).
[30] (T. L. Beauchamp & Childress, 2001).
[31] (US Department of Health Education and Welfare, 1978).
[32] One of the most infamous cases is the Tuskegee syphilis study (1932-1972) conducted by the US Public Health Service. The effects of the disease were studied over this period on several African American patients, who were not informed by doctors that, by 1947, penicillin had become a standard treatment for the disease.
[33] Charter of Fundamental Rights of the European Union, OJ C 202, 07.06.2016.
[34] (T. L. Beauchamp & Rauprich, 2015).

moderate forms thereof). At the same time, a principle-based method for impact assessment is not a mere checklist approach where ethics is used instrumentally by the assessor, who would just be engaged in 'ticking boxes'. Instead, the generality of the principles allows for and requires a certain amount of practical engagement, thus helping the assessors to familiarize with ethical reflection and to identify new ethical issues.

Second, some theoretical arguments can justify the choice of a principle-based method. It is true that the project PERSONA is not concerned with traditional bioethical issues (medical testing, end of life, abortion, etc.), but it could be argued that biometrics technologies (massively employed in border control) are a branch of the field of biotechnology, whereby bioethics is concerned.[35][36] In fact, the body and the 'measurement' of it (think of fingerprints, face and vein recognition, DNA, etc.) play a crucial role for these technologies.

Moreover, the US Department of Homeland Security,[37] as well as many EC experts' groups (such as the European Group on Ethics in science and new technologies, EGE), have implicitly or explicitly argued for a similar approach for the ethical use of Information and Communication Technologies (ICTs), Artificial Intelligence (AI), autonomous and digital technologies (see following section). All these fields are somehow interrelated with the technologies PERSONA is focused on. In fact, borderless crossing technologies include so-called second-generation biometrics, which capture (bodily) signals from the distance, in integrated and more and more smart or automated environments (Mordini & Tzovaras, 2012).

Finally, the principles are well grounded in the EU values stated in the European Convention of Human Rights (ECHR)[38] and in the Charter of Fundamental Rights of the European Union (CFR).[39] Delineating the relation between principles and human rights is not the primary scope of this deliverable. To simplify, we argue for a thesis of correlativity of principles and human rights.[40] Both principles and human rights are basic norms of common morality, and principles can be translated in correlative rights and vice versa. For instance, the principle of autonomy translates into to the right to have one's autonomy respected.

A problem with this approach might be that PERSONA aims to improve border guards and travellers' experience, when using borderless crossing technologies, *both* EU and third country nationals. Therefore, it might be argued that EU principles could not apply to travellers from outside EU with different value systems and to whom neither the ECHR nor the CFR apply. For the sake of the present deliverable, without going too much into academic debates, it can be replied that several characteristics of principle-based ethics make it global and cross-cultural since the principles are universally applicable.[41] Many attempts to develop a global or multicultural perspective on bioethics have already been made (T. Beauchamp, 2015). Similarly, this deliverable is one of the first attempts to promote a global perspective on the ethics of borderless crossing technologies.

This assumption on the universality of human rights and correlative principles is in line with the reflections of the EDPS' Ethics Advisory Group (2018):[42]

[35] Think of, for instance, the ethical debate around CRISPR, a gene editing technology.
[36] (Wickins, 2007).
[37] Cf. D. (Dittrich & Kenneally, 2012).
[38] Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4 November 1950, European Treaty Series (ETS) 5.
[39] Charter of Fundamental Rights of the European Union, OJ C 202, 07.06.2016.
[40] (T. L. Beauchamp & Rauprich, 2015).
[41] (T. L. Beauchamp & Rauprich, 2015).
[42] (EDPS Ethics Advisory Group, 2018), pp. 9-10.

> *"Notwithstanding the great variety in which different countries around the globe respond to the challenges of digitization, there are commonalities in how human beings experience the digital world and in how they may become vulnerable in light of their new technological condition".*

5.1.5 Critiques of principle-based ethics

The principle-based approach is by some considered too abstract or high-level, and it would offer no guidance in practice. Beauchamp & Childress reply that the principles are indeed general, but they need to be specified according to the context, on a case by case basis. The same would hold for borderless crossing technologies. In fact, the principles here will be referred to major ethical issues of border crossing technologies. However, since the spectrum of the most advanced technologies in this sector (D2.1) and their use cases (D1.2) are way too broad to provide an exhaustive ethical analysis here, the assessor is expected to further specify the principles on a case by case basis (e.g. applying them to a smart tunnel on a specific border).

At this point, one could argue that, in the specific context, tensions could arise between principles (which are all at the same level and not in a hierarchical relation). A classic example in bioethics is paternalism, where the doctor tries to override the patient's autonomous choice to improve her health. In this case, there is a conflict between the principle of respect for autonomy and that of beneficence.[43] A similar case related to PERSONA could be that of predictive policing in an airport where borderless crossing technologies are deployed. The initiative may help to reduce crime and/or improve security, but at the cost of surveilling people and infringe their liberty and privacy.[44] The question of paternalism is also relevant in the case of *automated* biometrics technologies at the borders, especially when it comes to embedded ubiquitous sensors and networks, and decisions are made without the human being 'in the loop' anymore. To this regard, Spiekermann and Pallas coined the expression "technology paternalism".[45]

The strategy of a principle-based method to solve conflicts between principles is twofold: either the conflict is dissolved by further specifying the principles (and showing how the moral dilemma/dichotomy at a further scrutiny is actually a 'fake' one) or the conflicts are decided through a balancing exercise.[46] For example, it could be shown how in a specific case (say, the introduction of a system of new generation cameras at an airport) privacy and security *should not* be understood as an abstract trade-off. The language of trade-off is often enforced in contexts (cultures, organizations) which systematically favours security (e.g. to defend travellers from terrorist attacks), while both privacy and security could be enforced without loss on either of the two.[47]

5.2 Benchmark

5.2.1 The four principles

Beauchamp and Childress present four general principles, which are not in a hierarchical relation but are on the same level (they have equal importance):

[43] (T. L. Beauchamp & Rauprich, 2015).
[44] (AI HLEG, 2019) p. 13.
[45] (Spiekermann & Pallas, 2006).
[46] (T. L. Beauchamp & Rauprich, 2015).
[47] (van Lieshout, Friedewald, Wright, & Gutwirth, 2013).

1) *Autonomy*: an autonomous person can be defined as a person who is able to deliberate on her goals and act upon such deliberations. Respecting autonomy therefore means taking into account opinions and choices of people and do not prevent them to act in a certain way. This includes also providing necessary information to make the subject able to make autonomous judgments.
2) *Non maleficence*: this principle means 'do not harm'. In biomedical ethics, this is probably the oldest principle and it is in line with the medical maxim '*Primum non nocere'* (first of all, do not harm [the patient]).
3) *Beneficence*: this is the other side of the non-maleficence principle, and it means to actively benefit and help others. This principle was originally merged with non-maleficence in the Belmont report.
4) *Justice*: the principle refers to how social goods or benefits should be distributed among the population. In a nutshell, it requires that equals should be treated equally, and unequals unequally but in proportion to their inequalities.

5.2.1.1 Principle-based method in the domain of ICT

Relevant to this benchmark is also the Menlo report (2012) published by the US Department of Homeland Security.[48] The report provides an ethical framework for Information and communication technologies research (ICTR) by drawing on the three principles of the Belmont report (1979) and adding a fourth principle, i.e. respect for law and public interest. This principle includes two applications, i.e. compliance and transparency and accountability. Compliance means that researchers should engage in due diligence to identify laws and otherwise regulatory requirements and design ICTR that respect such requirements. Transparency refers to the availability and communication of methods and results obtained, while accountability demands that the researcher is accountable for her actions.

5.2.1.2 Principle-based method in EU documents

Although the reference to bioethical principle-based ethics is not mentioned directly, a similar approach has been followed by different EU expert groups in the field of AI, robotics and digital ethics. Some examples are:

- The High-Level Expert Group (HLEG) on Artificial Intelligence (AI) (2019)[49] sets out 4 principles for trustworthy AI: respect for human autonomy, prevention of harm, fairness, explicability. Their method is particularly relevant for the present deliverable: first, they follow its minimalistic approach to principles (only 4, very general). Second, they unpack each principle in more specific 'requirements' (e.g. the principle of 'fairness' includes the requirements of 'avoidance of unfair bias' and 'accessibility and universal design').
- The EGE's document on Artificial Intelligence, Robotics and Autonomous systems (2018)[50] articulates 9 principles: Human dignity, autonomy, responsibility, justice, equity and solidarity, democracy, rule of law and accountability, security, safety, bodily and mental integrity, data protection and privacy, sustainability.

[48] (Dittrich & Kenneally, 2012).
[49] (AI HLEG, 2019), p. 18.
[50] (European Group on Ethics in Science and New Technologies, 2018), pp. 16-19.

- The EDPS' ethics advisory group report (2018)[51] lists seven traditional European values that could be impacted by developments in the field of digital technologies (i.e. dignity, autonomy, freedom, solidarity, equality, democracy and trust).

5.2.1.3 Principle-based method in other relevant fields

In the field of Technology Assessment (TA), Palm & Hansson (Palm & Hansson, 2006) argue for a check-list approach that includes nine ethical aspects that should be considered while evaluating an emerging technology. The idea is that such approach has the advantage to be 'neutral' with regard to normative ethical theories and flexible enough to allow for a "continuous dialogue" rather than "a single evaluation at a specific point in time".[52] The nine ethical aspects they consider are the following:

1) Dissemination and use of information
2) Control, influence and power
3) Impact on social contact patterns
4) Privacy
5) Sustainability
6) Human reproduction
7) Gender, minorities and justice
8) International relations
9) Impact on human values

In March 2019, The Biometrics Institute[53] published seven ethical principles to ensure the responsible and ethical use of biometrics. This approach has the advantage of being tailored to the field of PERSONA, but puts on the same level very general principles (e.g. equality, dignity) with more specific ones (e.g. promotion of privacy enhancing technologies), thus leaving unclear what the relations between such principles are. The principles are as follows[54]:

1) Ethical behaviour
2) Ownership of the biometric and respect for individuals' personal data
3) Serving humans
4) Justice and accountability
5) Promotion of privacy enhancing technology
6) Recognise dignity of individuals and families
7) Equality

From the short overview made in this section, it is clear that some of the principles occurs in different contexts and domains, although in slightly different formulations. In particular, many different principles can be actually subsumed under the original ones delineated by the Belmont report.

[51] (EDPS Ethics Advisory Group, 2018), p. 16.
[52] (Dittrich & Kenneally, 2012), p. 543.
[53] The Biometrics Institute is an Australian institute founded in 2001 which mission is to promote responsible and ethical use of biometrics (https://www.biometricsinstitute.org/).
[54] Cf. https://www.biometricsinstitute.org/ethical-principles-for-biometrics/

Following the principle of the 'Occam's razor',[55] and as a result of the integration of the different principles from different sources, we will keep a minimalistic approach. The following is the list for the present benchmark:

1) Respect for autonomy (including human dignity),
2) Non maleficence/beneficence,
3) Justice,
4) Explicability.

Human dignity was integrated in the principle of respect for autonomy to tailor the list to the EU context (in fact, human dignity is a foundational concept in the ECHR and CFR) and non-maleficence and beneficence were merged just like in the formulation of the Belmont report. Explicability is taken from the HLEG on AI. Each principle will be unpacked into further requirements, which will be in turn related to the field of border crossing technologies. For each principle and relative requirements, a set of questions will be put forth to help the assessor to evaluate the impact of a given initiative on such principles. This question-based approach to ethics is in line with that adopted by the European Commission.[56]

5.2.2 Respect for Autonomy

The principle of respect for autonomy (rooted in Kantian moral philosophy) requires respecting the two basic conditions of being autonomous, namely liberty and agency[57] or, differently put, negative and positive freedom.[58] Liberty must be intended as absence of interference by others which can prevent meaningful choice, such as inadequate understanding or incomplete information. Agency refers to the capacity of an agent to self-initiate her actions or act freely accordingly to her plans. The principle of respect for autonomy therefore has both a negative and positive obligations. On the one hand, the actions of the agent should not be subjected to constraints by others; on the other hand, individuals should be encouraged to make their own decisions by being informed and assisted.

Threats to autonomy in the use of borderless crossing technologies take place whenever humans are not 'kept in the loop' anymore. This means that, on the one hand, travellers should not be coerced, deceived or manipulated when crossing a borderless gate. It has to be avoided that e.g. biometric data are travellers are processed without them being aware or sufficiently informed, when a profile or identity is imposed upon them without taking into account their personal stories, or when their freedoms are not protected. On the other hand, oversight of border customs over work processes of borderless systems must be assured, meaning that borderless crossing systems should follow human-centric design principles and leave opportunity to operators to take over decisions made my machines.[59] This is in line with the principle of human dignity, rooted in the Kantian notion of human persons as end in themselves and not as mere means (Kant & Reath, 1997). The idea is that each and every person has an inherent dignity that cannot be violated. The CFR explicitly mentions the foundational role of human dignity (art. 1). The threat posed by borderless crossing technologies is

[55] Attributed to the medieval philosopher William of Ockham (c. 1287-1347), the idea is that among competing theoretical models, one should pick the one with the fewest assumptions (*Non sunt multiplicanda entia sine necessitate*).
[56] Cf. Section 'ethics' in the H2020 online manual: https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm
[57] (T. L. Beauchamp & Rauprich, 2015).
[58] (Berlin, 2017).
[59] (AI HLEG, 2019), p. 12.

that travellers might be treated as mere means (or objects, codes, bodily identifiers) instead of actual people of 'intrinsic worth' with personal stories (possibly of struggle, poverty and sufferance).

The principle of respect for autonomy includes the following requirements: informed consent, respect of freedoms and identity.

- Informed consent: the users of borderless crossing technologies should be reasonably informed about the data that are being processed and about how the system works, in order to interact and possibly challenge it.
- Respect of freedoms (art. 6, 10, 45 CFR)[60]: individuals (notably travellers and border customs) should remain free to make decisions from themselves. Mechanisms for human oversight should be in place to ensure human intervention in particular situations (e.g. in cases of false positives or false negatives).
- Identity: Individuals must be granted 'the ability to define their unique identity'. Compatibly with the architecture of the identification system, the 'what' element of one's identity (a biometric token such as a fingerprint, but also the number of our passport) should not take over or disregard the 'who' element of identity (personal stories, the complexity of one's lived experience).[61]

5.2.3 Non maleficence/beneficence

The principle of non-maleficence/beneficence requires to actively making efforts to promote people's well-being. The term beneficence must therefore be intended as a strong obligation and not, as the term is often used in common language, as acts of charity which go beyond strict obligation (Horton, 2002). Two complementary rules are part of this principle: 1) do not harm; 2) maximize possible benefits and avoid possible harms.

In the context of border crossing, in its positive formulation (beneficence), the principle encompasses the principles "serving humans" and "promoting privacy enhancing technologies" formulated by the Biometrics Institute (2019). More generally, it requires to take into account the well-being of all users, including travellers (EU and third country), and not only that of LEAs or of companies and institutions developing the technologies. In its negative formulation (non-maleficence) it requires to take into account possible harms in a variety of areas such as misuse, safety, bodily integrity and privacy and data protection. More practically, this principle includes also that the technological systems should be technically robust and not open to malicious use.

The principle includes the following requirements: dual use, technical robustness and safety, privacy and data protection.

- *Dual use and misuse*: 'dual use' goods are products or technologies that can be used both for civilian and military purposes. 'Misuse' refers to technologies that are used against the original purposes (e.g. 'function creep', i.e. data are used beyond the original purpose of processing).
- *Technical robustness and safety*: technologies deployed at the border could be inaccurate or unreliable due to their technical limitations (e.g. facial recognition subject to spoofing, fingerprint reader does not work in certain environmental conditions).
- *Privacy and data protection* (art. 7 & 8 CFR). For a detailed explanation see section 6.2.1 and 6.2.2 below.

[60] Right to liberty and security of the person (art. 6 CFR); Freedom of thought, conscience and religion (art. 10 CFR); Freedom of movement and of residence (art. 45 CFR).
[61] (Ajana, 2010).

5.2.4 Justice

The principle of justice is broad and refers to the idea of "fairness in distribution" or "what is deserved". The principle is not respected whenever some benefit to which a person is entitled is denied (without any compelling reason) or whenever there is an unequal distribution of benefits and burdens.[62] Of course, what a 'just' distribution means depends on the theory of justice one holds. The most well-known theories of justice are utilitarian, libertarian or egalitarian (or Rawlsian). In short, the utilitarian idea is that a just distribution is the one that produces as much happiness (or positive ratio costs/benefits) as possible (Mill, 1991). Libertarian theories claim that a just distribution is the one resulting from a certain 'fair' procedure or legitimate means. In other words, the fact that one is entitled to certain goods depends on how she achieved them throughout time (Nozick, 1974). Conversely, liberal theories hold that what matters is the end result of a distribution, and that the state should intervene to maximize the benefits of those who are worse off to re-equilibrate injustices resulting from historical processes.[63]

In the context of biometrics and border technologies, it has been often pointed out how such systems can be very convenient for some but increase discrimination of others .[64] This would lead on the one hand to the reinforcement of privileges of some groups (like EU and US citizens) and on the other to the increased discrimination of other groups (like asylum seekers). consider the FLUX traveller program for US and Dutch frequent intercontinental travellers, which is based on biometrics identifiers among which fingerprints and eye imaging.[65] In brief, so-called 'low risk passengers', i.e. "with no criminal records, no customs or immigration conviction" can apply for the program. If the interview and security threat assessment is successful, they can have, at a cost of paying an additional fee, the advantage of skipping queues and border checks.[66] The principle of justice aims to ensure equal and just distribution of benefits and costs in border crossing and ensure that travelers are free from unfair biases or stigmatization.[67]

The principle includes the following requirements: Equality, accessibility, accountability

- *Equality* (art. 20 CFR):[68] the users are ensured equal distribution of benefits and costs by using borderless crossing technologies, without any unfair bias or stigmatization.
- *Accessibility*[69]: the technologies are designed to be usable by people with disabilities.
- *Accountability*: mechanisms have to be in place to ensure accountability and responsibility for designing and deploying biometrics systems and their outcomes.

5.2.5 Explicability

This principle is important to maintain the trust of users in technological systems. It refers to the fact that the processes need to be transparent, the purposes of the technology communicated, and the decisions made can be explained to the people affected. It is important to note that explicability is a

[62] (T. L. Beauchamp & Rauprich, 2015).
[63] (Rawls, 1999).
[64] (Ajana, 2010).
[65] (Aas, 2011).
[66] Ibi, p. 336.
[67] (AI HLEG, 2019) p. 12.
[68] Including also: Non-discrimination (Art. 21 CFR); The rights of the elderly (Art. 25 CFR).
[69] Integration of persons with disabilities (Art. 26 CFR).

matter of degree: a 'full' explanation is not always possible, especially in cases where black-boxed' algorithms are involved.[70]

This principle is particularly relevant for border crossing and PERSONA, which also aims to investigate the acceptance of the newest crossing point solutions for travelers and LEAs. Especially since black-boxed algorithms can carry out the biases of their designers (e.g. facial recognition trained for white male adults, thus having a lower accuracy and higher error rate for women, older or black people) could be used resulting in discriminatory practices (e.g. further scrutiny for minorities or women who are not 'recognized' by the system).

The principle includes the following requirements: transparency and legal due diligence.

- *Transparency*: the data collected, the functioning of the system and business models should be traceable, explainable, and communicated to users.
- *Legal due diligence*: designers, biometrics companies, LEAs and border control authorities should engage in identifying laws and otherwise regulatory requirements and design borderless technologies that respect such requirements.[71]

5.3 Ethics requirements

To conclude, this chapter started off by asking the question of how an ethics benchmark would look like in the context of border control and the PERSONA project. To answer the question, a principle-based method was used to come up with a list of four ethics principles, which were further 'unpacked' in sub-principles or requirements. To sum up, the table below provides the reader with the ethics requirements identified in the chapter, along with a short description thereof.

Id	*Description*
ER1	Informed consent: the users of borderless crossing technologies should be reasonably informed about the data that are being processed and about how the system works, in order to interact and possibly challenge it.
ER2	Respect of freedoms: individuals (notably travellers and border customs) should remain free to make decisions from themselves. Mechanisms for human oversight should be in place to ensure human intervention in particular situations (e.g. in cases of false positives or false negatives).
ER3	Identity: Compatibly with the architecture of the identification system, the 'what' element of one's identity (a biometric token such as a fingerprint, but also the number of our passport) should not take over or disregard the 'who' element of identity (personal stories, the complexity of one's lived experience).
ER4	Dual use and misuse: 'dual use' goods are products or technologies that can be used both for civilian and military purposes. 'Misuse' refers to technologies that are used against the original purposes (e.g. 'function creep', i.e. data are used beyond the original purpose of processing).
ER5	Technical robustness and safety: technologies deployed at the border could be inaccurate or unreliable due to their technical limitations (e.g. facial recognition subject to spoofing, fingerprint reader does not work in certain environmental conditions).
ER6	Privacy and data protection

[70] (AI HLEG, 2019) p. 13.
[71] See (Dittrich & Kenneally, 2012).

Id	*Description*
ER7	Equality: the users are ensured equal distribution of benefits and costs by using borderless crossing technologies, without any unfair bias or stigmatization.
ER8	Accessibility: the technologies are designed to be usable by people with disabilities.
ER9	Accountability: mechanisms have to be in place to ensure accountability and responsibility for designing and deploying biometrics systems and their outcomes.
ER10	Transparency: the data collected, the functioning of the system and business models should be traceable, explainable, and communicated to users.
ER11	Legal due diligence: designers, biometrics companies, LEAs and border control authorities should engage in identifying laws and otherwise regulatory requirements and design borderless technologies that respect such requirements.

7 Legal and otherwise regulatory requirements

The legal and regulatory frameworks relevant for establishing PERSONA benchmark, against which the impact of the selected no-gate crossing point solutions will be assessed, may be grouped in two main categories:

1) **fundamental right related** rules, especially concerning **privacy and data protection**, adopted both at European Union and Council of Europe level.[72] Privacy and data protection are particularly worthy of consideration because, with the entry into force of the General Data Protection Regulation (GDPR), the Law Enforcement Directive (LED) and the Regulation 2018/1725 (the so called EUDPR, i.e. the GDPR for European institutions, bodies, agencies and offices), data protection impact assessment (DPIA) became a legal obligation in certain situations (e.g. where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is **likely to result in a high risk** to the rights and freedoms of natural persons),[73] meaning that DPIA will constitute a nuance of the PERSONA impact assessment. A clarification is nevertheless necessary in this respect: also border management related instruments contain *sui generis* data protection rules, to be coordinated with the GDPR, LED, EUDPR (and Europol) ones.
2) **border management related** instruments, adopted at European Union level, encompassing the rules disciplining EU large scale databases and their management,[74] other exchanges of information,[75] border practices and rules on passports and ID documents.[76]

This part of the deliverable concerns the legal requirements applicable to PERSONA adopting a fundamental right perspective. After providing an overview on the fundamental rights that may be affected by border-crossing points solutions, it will focus on the European legal framework on privacy and personal data protection, which is worthy of specific consideration due to the introduction of DPIA as legal obligation for certain types of processing operation. The next Chapter will deal with border management related instruments.

7.1 Introduction: Democracy and the Rule of law

> *"The European Union is founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities. These values are common to the Member States in a*

[72] e.g. the European Charter on Fundamental Rights (CFR), the Treaty on the Functioning of the European Union (TFEU), the Treaty on the European Union, as regards EU primary law; the GDPR, the LED, the EUDPR, Europol regulation as regards EU secondary law; the modernised Convention for the Protection of Individuals with regard to automatic processing of personal data (Convention 108 +).
[73] See Art. 35 GDPR, Art. 27 LED, Art. 39 EUDPR.
[74] i.e. the Schengen Information System (SIS II), the Visa Information System (VIS) and the European Asylum Dactyloscopy Database (Eurodac), the Entry/Exit system (EES), the European Travel Information and Authorisation System (ETIAS) and the European Criminal Records Information System on Third Country Nationals (ECRIS-TCN), that are supposed to become interoperable and that are (or will be) managed by eu-LISA [European Commission press release, *Security Union: Commission proposal for a stronger eu-LISA Agency adopted*, Brussels, 9 November 2018 https://europa.eu/rapid/press-release_IP-18-6324_en.htm]
[75] As the frameworks of Prüm decision, European Border Surveillance System (EUROSUR), Passenger Name Records (PNR) and Advanced Passenger Information (API).
[76] Passport regulation and ID card regulation.

society in which pluralism, non-discrimination, tolerance, justice, solidarity and equality between women and men prevail".

This is the wording of Article 2 TEU, expression the core values of European identity and the principle of homogeneity (Blanke & Mangiameli, 2013). Notwithstanding the wording 'values' may suggest a lack of normativity, providing that "Values are fundamental ethical convictions, while principles are legal norms", in reality the meaning here is two folded. Values are either constitutional foundations and principles with enforceable content, as witnessed by the enforcement mechanism provided for in Art. 7 TFEU triggered in case of risks or their actual systematic violations.[77] Moreover, these European values are so important that only those countries respecting them and committed to promote them may apply to become members of the Union (Art. 49 TEU).

At the same time, "The Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime" [Art. 3(2) TEU]. It is with this goal in mind that the internal borders checks were abolished and an integrated system management for external border was created, together with a common policy on visa; that certain aspects of asylum process and immigration were harmonised; that efforts against illegal immigration and other forms of international crimes were intensified; that EU-large scale databases were created.[78]

When the Smart border package (that lead to the adoption of the EES and to the amendments of the Schengen Border Code) and the interoperability proposals were proposed by the European Commission in 2013 and 2017,[79] concerns were raised by various stakeholders (e.g. EDPS, FRA, NGOs, academia etc.) about the negative impacts that the new rules would have had on fundamental rights in general and privacy/data protection in particular. On the one hand, interoperability is not indeed just a technical choice, but it entails a political approach that somehow blurs the lines between various policy goals (e.g. asylum, migration management, law enforcement, counterterrorism...), risking to equate the notions of terrorists and criminals with foreigners.[80] Interoperability therefore entails much more than interconnecting ICT-systems: it has technical, semantic, social, cultural, economic, organisational and legal dimensions.[81]

From a data protection perspective, overlapping of different policy goals, participation of different entities and diverse processing operations create uncertainty about the proper legal regime applicable (e.g. GDPR, LED, EUDPR, or Europol regulation). Moreover, it has been outlined how the intrusion to privacy generated by processing large amounts of personal data, including biometric ones, may affect democracy and society, being privacy is an inherent value to liberal democratic and pluralist societies, other than a cornerstone for the enjoyment of human and civil rights.[82]

An example of clashes between Art. 2 TEU and Art. 3(2) TEU is given by the case C-291/12 Michael Schwarzv Stadt Bochum, about Regulation No 2252/2004 (Passport regulation),

The ECJ was requested to rule about the validity of the regulation in the light of the Charter of Fundamental Rights of the European Union, in so far as it obliges any person applying for a passport to provide fingerprints and provides for those fingerprints to be stored in that passport.

[77] (Mader, 2019).
[78] (Engström & Heikkilä, 2014).
[79] https://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/smart-borders-package_en9
[80] EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, Brussels 16 April 2018.
[81] (De Hert & Gutwirth, 2006).
[82] (European Union Agency for Fundamental Rights, 2017) p. 12.

"Although the taking and storing of fingerprints in passports constitutes an infringement of the rights to respect for private life and the protection of personal data, those measures are in any event justified by the aim of protecting against any fraudulent use of passports.

In that regard, the Court finds that the contested measures pursue, in particular, the general interest objective of preventing illegal entry into the EU. To that end, they are intended to prevent both the falsification of passports and the fraudulent use thereof. First of all, it is not apparent from the evidence available to the Court, nor has it been claimed, that those measures do not respect the essence of the fundamental rights at issue. Next, the Court finds that the contested measures are appropriate for attaining the aim of protecting against the fraudulent use of passports, by significantly reducing the likelihood that, owing to an error, unauthorised persons will be allowed to enter the EU. Lastly, the contested measures do not go beyond what is necessary to achieve the above aim. The Court has not been made aware of any measure which would be sufficiently effective and less of a threat than the taking of fingerprints.

The Court observes in particular that iris-recognition technology is not yet as advanced as fingerprint-recognition technology and that, owing to the significantly higher costs currently involved in using the former technology, it is less suitable for general use. With regard to the processing of fingerprints, the Court notes that fingerprints play a particular role in the field of identifying persons in general. Thus, comparing fingerprints taken in a particular place with those stored in a database makes it possible to establish whether a certain person is in that particular place, whether in the context of a criminal investigation or in order to monitor that person indirectly. However, the Court also notes that the regulation explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder. Moreover, the regulation does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone. The regulation not providing for any other form or method of storing those fingerprints, it cannot in and of itself be interpreted as providing a legal basis for the centralised storage of data collected thereunder or for the use of such data for purposes other than that of preventing illegal entry into the EU".[83]

The FRA has outlined how this case law is not automatically applicable to national ID: the Court indeed assessed the proportionality of limiting the right to respect for private and family life and the right to data protection against the aims of preventing falsification and fraudulent use of passports and, by extension, the objective of preventing irregular entry into the EU. Nevertheless, national identity cards, unlike passports, are not primarily used for crossing the external border but are conversely mainly used for interactions with e.g. administration, banks and other private actors in their own country and to move across borders within the Schengen area, without being subject to border checks. That is why the necessity of processing the same biometric identifiers as in passports is not automatically justified in light of the CJEU's above case law.[84]

[83] Court of Justice of the European Union PRESS RELEASE No135/13 Luxembourg, 17 October 2013, https://curia.europa.eu/jcms/upload/docs/application/pdf/2013-10/cp130135en.pdf

[84] FRA Opinion 3/2018 on Fundamental rights implications of storing biometric data in identity documents and residence cards (Vienna 5 September 2018).

7.3 Fundamental rights

No-gate crossing point solutions and EU-large scale databases may affect fundamental rights other than privacy and data protection. This is actually acknowledged in part of the legal framework on border management above mentioned, that also refers to other European and international instruments to whom competent authorities, both national and European, should conform in the performance of their tasks. Relevant rights include, but are not limited to:

- **Human dignity** (Art. 1 CFR and Art. 2 TEU)
- **Right to integrity of the person** (Art. 3 CFR)
- **Prohibition of inhuman or degrading treatment** (Art. 4 CFR)
- **Non-discrimination** (Art. 21 CFR and Art. 2 TEU).
- **Right to asylum** (Art. 18 CFR)
- **Protection in the event of removal, expulsion or extradition** (Art. 19 CFR)
- **Rights of the child** (Art. 24)
- **Rights of the elderly** (Art. 25 CFR)
- **Integration of persons with disabilities** (Art. 26 CFR)

Notwithstanding these provisions, rules on fingerprinting given by children are not uniform: whereas EES Regulation and Visa code provide for the exemption of children under age 12 to provide fingerprints, Eurodac for instance fixes the threshold at 14 years old.

Examples:

When applying the Schengen borders code, Member States shall act in full compliance with relevant Union law, including the ***Charter of Fundamental Rights of the European Union*** *('the Charter'), relevant international law, including the* ***Convention Relating to the Status of Refugees*** *done at Geneva on 28 July 1951 ('the Geneva Convention'), obligations related to access to international protection, in particular the principle of non-refoulement, and fundamental rights* (Art. 4 SBC).

1. Border guards shall, in the performance of their duties, fully respect human dignity, in particular in cases involving vulnerable persons.
Any measures taken in the performance of their duties shall be proportionate to the objectives pursued by such measures.
2. While carrying out border checks, border guards shall not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation. (Art. 7 SBC)

Member States shall collect biometric identifiers of the applicant comprising a photograph of him and his 10 fingerprints in accordance with the safeguards laid down in the ***Council of Europe's Convention for the Protection of Human Rights and Fundamental Freedoms****, in the* ***Charter of Fundamental Rights of the European Union*** *and in the* ***United Nations Convention on the Rights of the Child*** (Art. 13 Visa Code).

The procedure for taking fingerprints shall be determined and applied in accordance with the national practice of the Member State concerned and in accordance with the safeguards laid down in the ***Charter of Fundamental Rights of the European Union****, in the* ***Convention for the Protection of Human Rights and Fundamental Freedoms*** *and in the* ***United Nations Convention on the Rights of the Child*** (Art. 3 Eurodac Regulation).

Each competent authority shall ensure that the use of the EES, including the capturing of biometric data, is in accordance with the safeguards laid down in the ***Convention for the Protection of Human Rights and Fundamental Freedoms****, in the* ***Charter of Fundamental Rights of the European Union and in the United Nations Convention on the Rights of the Child****. In particular, when capturing a child's data, the best interests of the child shall be a primary consideration* (Art. 10 EES Regulation).

Processing of personal data within the ETIAS Information System by any user shall not result in discrimination against third-country nationals 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. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly and persons with a disability. The best interests of the child shall be a primary consideration (Art. 14 ETIAS Regulation).

1. The European Border and Coast Guard shall guarantee the protection of fundamental rights in the performance of its tasks under this Regulation in accordance with relevant Union law, in particular the Charter, relevant international law — including the ***1951 Convention Relating to the Status of Refugees****, the* ***1967 Protocol thereto and obligations related to access to international protection, in particular the principle of non-refoulement****. […]*
3. In performing of its tasks the European Border and Coast Guard shall take into account the special needs of children, unaccompanied minors, persons with disabilities, victims of trafficking in human beings, persons in need of medical assistance, persons in need of international protection, persons in distress at sea and other persons in a particularly vulnerable situation. (Art. 34 Frontex Regulation]

Processing of personal data for the purposes of this Regulation shall not result in discrimination against persons on any grounds such as gender, 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. It shall fully respect human dignity and integrity and fundamental rights, including the right to respect for one's private life and to the protection of personal data. Particular attention shall be paid to children, the elderly, persons with a disability and persons in need of international protection. The best interests of the child shall be a primary consideration. [Interoperability]

The fundamental rights protected in the Charter may be limited, but limitations must be i) **provided by law**, i.e. an accessible legal basis formulated with sufficient precision to enable individuals to understand their obligations and regulate their conduct. The legal basis must also clearly define the scope and manner of the exercise of the power by the competent authorities to protect individuals against arbitrary interference; ii) **respect the essence of the right**, meaning that limitations that are so extensive and intrusive to be capable of emptying a fundamental right of its basic content cannot be justified. If the essence is compromised, the limitation is unlawful, and there is no need to further assess whether it serves an objective of general interest and satisfies the necessity and proportionality criteria;[85] iii) **necessary** (the measure is needed to be adopted to pursue the public interest objective and it must be the less intrusive measure compared to other options for achieving the same goal. The

[85] CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner [GC], 6 October 2015; CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC], 8 April 2014; (European Union Agency for Fundamental Rights & EDPS, 2018) p. 44-45.

CJEU applies a strict necessity test for limitations on the rights to respect for private life and protection of personal data, holding that *"derogations and limitations must apply only in so far as strictly necessary"*) **and proportional,** meaning that the advantages resulting from the limitation should outweigh the disadvantages the latter causes on the exercise of the fundamental rights at stake. To reduce disadvantages to the rights at stake, appropriate safeguards are needed;[86] iv) **pursue objectives of general interest** which must be recognised by the Union law or the need to protect the rights and freedoms of other persons (Article 3 of the TEU). These objectives need to be clearly defined and explained and a detailed description is required in order to assess the necessity of the measure.

It must be said that the understanding of "fundamental rights" and their possible limitations is not as universal as it may appear.

Examples of case law on border check related issues:(European Union Agency For Fundamental Rights (FRA), 2015)

ECtHR, Phull v. France(dec.), No. 35753/03, 11 January 2005; ECtHR, El Morsli v. France(dec.), No. 15585/06, 4 March 2008 "*Under the ECHR, the requirement for a Muslim woman to remove her headscarf for an identity check at a consulate or for a Sikh man to remove his turban at an air-port security check was found not to violate their right to freedom of religion under Article 9 of the ECHR*"

UN Human Rights Committee, Ranjit Singh v. France, Communications Nos. 1876/2000 and 1876/2009, views of 22 July 2011, para 8.4. "*The UN Human Rights Committee considered that the obligation for a Sikh man to remove his turban in order to have his official identity photo taken amounted to a violation of Article 18 of the International Covenant on Civil and Political Rights (ICCPR), not accepting the argument that the requirement to appear bareheaded on an identity photo was necessary to protect public safety and order. The reasoning of the UN Human Rights Committee was that the state had not explained why the wearing of a Sikh turban would make it more difficult to identify a person, who wears that turban all the time, or how this would increase the possibility of fraud or falsification of documents. The committee also took into account the fact that an identity photo without the turban might result in the person concerned being compelled to remove his turban during identity check*".

7.3.1 Privacy

The idea of a right to privacy, in the sense of **right to be let alone**, appeared for the first time in 1890, in a paper by Samuel Warren and Louis Brandeis.[87] The idea of privacy came as a reflection upon the appearance of new technologies (e.g. instantaneous photographs) that determined newspapers to start dealing with gossip, overstepping the limits of propriety and decency, causing harm both to the individuals portrayed and to the community, lowering social standards and morality. It must be noted, at the time, the right to privacy was elaborated merely within the paradigm of the law of the torts, conceptualised as a civil claim for damages, not as fundamental/constitutional right.

Warren and Brandeis' definition of privacy did not however explain what privacy entails and the issues in which individuals should be left alone. Conversely, it remained a vague and broad definition.

[86] EDPS (2017), Necessity Toolkit, 11 April 2017, p 5; (European Union Agency for Fundamental Rights & EDPS, 2018) p. 46.
[87] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, in *Harvard Law Review*, 1890, Vol. 4, No. 5, p 193-220.

Even today, there is no single understanding of what the right to privacy is.[88] Indeed, privacy can be **cultural**, **contextual** and **evolutive**. The author Daniel Solove provides an overview about some different theories of privacy and their shortcomings (Solove, 2008):

1) **right be let alone**, i.e. *"to live one's life as one chooses, free from assault, intrusion or invasion except as they can be justified by the clear needs of community living under a government of law"*;[89]
2) **limited access to the self**, i.e. the ability to shield oneself from unwanted public observation and discussion by others;
3) **secrecy**, where privacy is infringed by public disclosure of previously concealed information and where the interest of the individual is to avoid disclosure of personal matters;[90]
4) **control over personal information**, meaning the claim of individuals, groups or institutions to determine how, when and to what extent information about them is given to others;[91]
5) **personhood**, concerns the protection of the integrity of personality and considered to be *"those attributes of an individual which are irreducible in the selfhood"*; [92] and,
6) **intimacy**, where the focus is on the development of personal relationships and different degrees of intimacy and self-revelation.

The concept of 'private life' has been broadly interpreted in case-law, covering sensitive or confidential information, intimate situations, information that could prejudice the perception of the public against the individual, and aspects of an individual professional life and public behaviour. The assessment on whether there has been an interference or limitation with 'private life' depends on the context and facts of each case.[93]

7.3.1.1 In the Council of Europe: the European Convention on Human Rights (ECHR)

The right to privacy, more precisely the "right to respect for private and family life" is protected under Article 8 ECHR. It entails both a **negative obligation** on public authorities, that shall refrain from any actions that may creep upon private life, but, at the same time, a **positive obligation** to actively secure the respect for private life.[94] Not being an absolute right, it may be limited, providing that restrictions are **in accordance with the law** and **necessary** in a **democratic society** while **pursuing legitimate and relevant public interests** (national security, public safety, economic well-being a country, prevention of disorder or crime, protection of health or morals, protection of the rights and freedoms of others) [Art. 8(2)][95].

[88] (Robert C. Post, 2001).
[89] Justice Abe Fortas as cited in Solove, Understanding Privacy – Chapter 2, 2008, p 2.
[90] Whalen v. Roe (1977) as cited in Solove, Understanding Privacy – Chapter 2, 2008, p 5.
[91] Alan Westin as cited in Solove, Understanding Privacy – Chapter 2, 2008, p 5.
[92] Solove, Understanding Privacy – Chapter 2, 2008, p 9.
[93] (European Union Agency for Fundamental Rights & EDPS, 2018) p 20.
[94] ECtHR, I v Finland, N° 20511, 17 July 2008.
[95] (European Union Agency for Fundamental Rights & EDPS, 2018) p. 37 ff.

7.3.1.2 In primary law in the European Union: European Charter of Fundamental Rights

Under the Charter of Fundamental Rights of the European Union (CFR), that became legally binding in 2009 with the treaty of Lisbon, the right to privacy is referred as the right to **respect for private and family life** (**Art. 7**).[96] The rights guaranteed in Art. 7 correspond to those guaranteed by Art. 8 of the ECHR.

Possible limitations to Art. 7 are regulated by **Art. 52(1)**, which also recognises that the **right is not absolute**. Limitations are allowed if i) **provided by law**, ii) **respect the essence of the right**, iii) are **necessary and proportionate** and iv) meets **objectives of general interest of the Union**, including general objectives of the EU mentioned in Art. 3 of the TEU or other protected by specific provisions in the treaties, **or the need to protect the rights and freedoms of others**.

Art. 52(3) provides that the level of protection granted to rights within the system of CFR should be at least equivalent as that one within ECHR.

7.3.2 Personal data protection

The right to the protection of personal data is closely related to the right to respect for private life. The protection of personal data appeared in response to the interferences led by governments concerning the collection and use of personal information. First understood as a derivation of the right to privacy (in its understanding of 'right to informational self-determination' or 'informational privacy'), it then evolved to a separate fundamental right.[97]

Both the rights to data protection and to privacy aim at creating a personal sphere where individuals are able to develop their personalities freely and they are pre-condition to exercise other rights (e.g. freedom of expression and freedom of peaceful assembly and association).[98] Nevertheless, they are **distinct in formulation and scope**: whereas the latter consists of a general prohibition of interference, with certain exceptions, the former is considered to be an 'active right', which implements a system of checks and balances to protect individuals personal data when is being processed. To ensure the efficacy of such a system, the processing i) must be lawful, ii) individuals need to be able to exercise certain rights and iii) there should be an independent authority supervising its correct application. [99]

7.3.2.1 In the Council of Europe: Convention 108

The Convention for the Protection of Individuals with regard to automatic processing of personal data of 28 January 1981, also known as Convention 108,[100] is a legally binding international instrument in the data protection field (for States ratifying it) which applies to data processing performed by both the private and public sectors, including data processing by the judiciary branch and law enforcement authorities. It is open to every country in the Word and it is currently composed by 54 States (including all EU countries). The Parties to the Convention commit to a mutual co-operation and to ensure the highest level of data protection.

[96] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
[97] (European Union Agency for Fundamental Rights & EDPS, 2018) p 18.
[98] (European Union Agency for Fundamental Rights & EDPS, 2018) p 19.
[99] Ibid, p 18.
[100] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 108, 1981.

In 1999, amendments to Convention 108 were proposed to enable the EU to become a party but it never entered into force. In 2001, an Additional Protocol to the Convention 108 was adopted on transborder data flows to non-parties (third countries) and on the mandatory establishment of national data protection supervisory authorities. In 2018, the Convention was modernised (Convention 108+)[101] to respond to the new challenges of the digital era, the globalisation of processing operations and to allow safer exchanges of personal data.[102]

Albeit the Convention is not subject to the judicial supervision of the ECtHR, still it has been taken into consideration in its case law related Article 8 of the ECHR.[103]

The Convention aims to protects individuals against abuses which may result from processing of personal data and seeks to regulate the transborder flows of personal data. As regards the processing of personal data, the principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, for specified legitimate purposes.

7.3.2.2 In primary law in the European Union: the European Charter of Fundamental Rights and the Treaties

The right to the protection of personal data is a fundamental right recognised by the Charter.(González Fuster, 2014) EU institutions and bodies must guarantee and respect this right, as well as Member States when implementing Union law (Art. 51). This article was formulated after the Data Protection Directive[104] which included the EU *acquis* on data protection: it recognised the right and certain principles as well as an independent authority to control the implementation of those principles.

The right to the protection of personal data is not absolute. It can suffer limitations under strict conditions of Article 52 (1) and (3) of the Charter.

Within Art. 8 CFR, there are other rights connected to personal data protection that may be derived: **fair processing**, **purpose specification**, **lawful basis**, **right to access and rectification**, **supervision from an independent authority**.

Art. 16 TFEU and Art. 39 TEU set procedural requirements for the decision making in the field of data protection, other than reiterating the need to establish an independent authority. The former prescribes ordinary legislative procedure for rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law; the latter waivers this rule, setting a special legislative procedure (whose outcome is a Council decision) in the field of common foreign and security policy.

In Opinion 1/15 of the Court (Grand Chamber) of 26 July 2017 on the Draft agreement between Canada and the European Union on Transfer of Passenger Name Record data from the European Union to Canada, the Court provided guidance on the scope of necessity and proportionality test.

It ascertained that the operations to be performed on the PNR data under the Draft Agreement constituted an interference with the fundamental right to data protection guaranteed in Article 8 of the Charter but that they could be justified since data protection is not an absolute right. The Court stated that any justification would have to specify the purpose and legal basis of processing

[101] https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1,
[102] https://rm.coe.int/leaflet-data-protection-final-26-april-2019/1680943556
[103] ECtHR, Zv. Finland, N° 22009/93, 25 February 1997.
[104] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281.

(e.g. since processing of PNR data under the Draft Agreement pursues a different objective than that for which it was collected by air carriers, thus it requires a different legal basis) and must respect the essence of the rights and freedoms at issue (in this case, the essence was respected providing that the Draft Agreement limited the purposes for which the data may be processed and contained rules to ensure security, confidentiality, and integrity of the data, and to protect it against unlawful access and processing). The main elements of criticism were: the lack of precision about the PNR data to be transferred, the weak justification for the transfer of sensitive data, providing that the only ground of protection of public security against terrorism and serious transnational crime is not sufficient; the lack of "individual re-examination by non-automated means" on case of automated analysis of PNR data;

In this case, interferences were justified by the need to fight terrorism and serious transnational crime in order to ensure public security, and that the transfer of PNR data to Canada and its subsequent processing may be appropriate to meet that objective (Kuner, 2018)

7.3.2.3 In secondary law in the European Union

The choice of the European legislators to adopt different data protection instruments depends on the different goals pursued by the various rules. Indeed, the fact that personal data protection is a fundamental right but not absolute determines it may be limited, also in a different way depending on the policy area. For instance, for law enforcement purposes, the LED provides for more flexibility for the limitations of data subjects rights rather than the GDPR.[105] Similarly, Europol, the European Agency for law enforcement cooperation, follows tailored rules on data protection comparing with the other European institutions.

As mentioned above, EU large scale databases have own data protection rules but also refer to other existing data protection instruments.

Chapter VI on data protection together with Recitals 15 and 16 Regulation 1987/2006 refer to the applicability of Directive 95/46 (now GDPR) and Regulation 45/2001 (now EUDPR), notwithstanding from Art. 1 "… purpose of SIS II shall be…to ensure a high level of security within the area of freedom, security and justice of the European Union, including the maintenance of public security and public policy and the safeguarding of security in the territories of the Member States" it may appear more appropriate to refer to Council Framework Decision 2008/977/JHA (that at the time had not been adopted yet). Nevertheless, Recital 39 Council Framework Decision 2008/977/JHA makes clear that "the relevant set of data protection provisions of … acts … governing the functioning of Europol, Eurojust, the Schengen Information System (SIS) and the Customs Information System (CIS), as well as those introducing direct access for the authorities of Member States to certain data systems of other Member States, should not be affected by this Framework Decision. The same applies in respect of the data protection provisions governing the automated transfer between Member States of DNA profiles, dactyloscopic data and national vehicle registration data pursuant to the Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime".

This approach will be changed after the entry into force of the amended Regulation: Chapter VIII is about general data processing rules, whereas new Chapter IX on data protection, in Art. 51, refers to Applicable legislation: Regulation (EU) 2018/1725 for personal data processing by eu-LISA and by the European Border and Coast Guard Agency under this Regulation. Regulation (EU) 2016/794 shall apply to the processing of personal data by Europol under this Regulation; Regulation (EU)

[105] (Sajfert & Quintel, 2019).

2016/679 for the processing of personal data by the competent authorities, exception of processing for the purposes of the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, where Directive (EU) 2016/680 applies.

The blurred lines between the goals pursued by the databases themselves and the possibility given to different authorities to access them, further complicated by the interoperability proposal, create uncertainty concerning the right legal framework applicable, with a risk of "function creep"[106].

Certain concepts, as the notions of **personal data**[107], of **data processing**[108], of **data controller and joint controllers**[109] and **data processor**[110] are the same in the various instruments. Whereas others, especially if compared with the database related legal framework, are different. For instance, the definition of **biometric data**. Whereas in GDPR and LED biometric data are very broad and mean "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", in interoperability Regulation, biometric data are only fingerprint data, facial images or both. In VIS, only fingerprints of the applicant. In EES, fingerprints data and facial images. In SIS, "personal data resulting from specific technical processing relating to the physical or physiological characteristics of a natural person, which allow or confirm the unique identification of that natural person, namely photographs, facial images and dactyloscopic data" (for border management) and includes also DNA (for police cooperation). Neither the notion of dactyloscopic data and fingerprints is homogenous in the various databases: certain databases require the insertion of all fingerprints (ECRIS-TCN), whereas others of less (e.g. EES requires four fingerprints of the index, middle finger, ring finger and little finger from the right hand where present, and otherwise from the left hand). In Return regulation, it is specified that dactyloscopic data may consist of: (a) **one to ten flat fingerprints and one to ten rolled fingerprints** of the third-country national concerned; (b) **up to two palm prints** in respect of third-country nationals **from whom the collection of fingerprints is impossible**; (c) **up to two palm prints in respect of third-country nationals who are subject to return as a criminal law sanction or who have committed a criminal offence** on the territory of the Member State which issued the return decision.

Examples of the notions of data processors and data controller in EU large scale databases:

- In the interoperability regulation in the field of borders and visa, Article 40 specifies that, in relation to the processing of data in the shared BMS, the Member State authorities that are controllers for the EES, VIS and SIS respectively shall be controllers in relation to the

[106] EDPS Reflection paper on the interoperability of information systems in the area of Freedom, Security and Justice (Brussels, 17 November 2017).
[107] i.e. information related to an identified or identifiable person, the data subject.
[108] i.e. 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.
[109] i.e. the natural or legal person, public authority, competent 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.
[110] i.e. the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

biometric templates that they enter into the underlying systems and shall have responsibility for the processing of the biometric templates in the shared BMS.

- In relation to the processing of data in the CIR, the Member State authorities that are controllers for the EES, VIS and ETIAS respectively, shall be controllers in relation to data referred to in Article 18 [of the Regulation] that they enter into the underlying systems and shall have responsibility for the processing of those personal data in the CIR. In relation to the processing of data in the MID, the European Border and Coast Guard Agency shall be a data controller in relation to the processing of personal data by the ETIAS Central Unit; the Member State authorities adding or modifying the data in the identity confirmation file shall be controllers and shall have responsibility for the processing of the personal data in the MID.
- In relation to the personal data in the shared BMS, CIR, MID, eu-LISA is considered data processor (Art. 41 interoperability regulations)

Examples of the various definitions of fingerprints	
'fingerprint data' means the data relating to the four fingerprints of the index, middle finger, ring finger and little finger from the right hand where present, and otherwise from the left hand	EES
fingerprint data· means the data relating to fingerprints of all or at least the index fingers, and if those are missing, the prints of all other fingers of a person, or a latent fingerprint.	EURODAC
'fingerprint data' means the data relating to plain and rolled impressions of the fingerprints of each of a person's fingers	ECRIS-TCN

Defining who is data processor and data controller is fundamental define the obligations laying on the various stakeholders (e.g. only data controllers have the duty to perform a DPIA) and to enable data subjects to exercise their rights.

Data protection principles

There are **data protection principles** that, albeit differently nuanced depending on the legal instruments, are still common to all of them. A typical catalogue comprises:

- **Lawful processing** meaning that there shall be a legal basis for data processing
- **Purpose limitation** meaning that data shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes
- **Data minimisation** meaning that data shall be adequate, relevant and not excessive in relation to the purposes for which they are processed
- **Accuracy** meaning that data shall be accurate and when necessary kept up to date, and that 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
- **Storage limitation** meaning that they shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed
- **Integrity and confidentiality** meaning that they 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.

- **Accountability** meaning that data controller shall be responsible for, and be able to demonstrate compliance those principles

In the SIS database, there is a difference between the minimum data necessary for entering an alert and the data that the database can contain.	
For the purpose of **refusing entry into and stay on the territory of the Member States**	
Regulation (EU) 1987/2006	**Regulation (EU) 2018/1861**
Information on persons in relation to whom an alert has been issued, must not exceed (Art. 20) (a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; I place and date of birth; (d) sex; (e) **photographs**; (f) **fingerprints**; (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert; (k) a reference to the decision giving rise to the alert; (ka) the type of offence; (l) action to be taken; (m) link(s) to other alerts issued in SIS II in accordance with Article 37 [links between alerts].	Any alert in SIS which includes information on persons shall contain only the following data (Art. 20) (a) surnames; (b) forenames; (c) names at birth; (d) previously used names and aliases; (e) any specific, objective, physical characteristics not subject to change; (f) place of birth; (g) date of birth; (h) gender; (i) any nationalities held; (j) whether the person concerned: (i) is armed; (ii) is violent; (iii) has absconded or escaped; (iv) poses a risk of suicide; (v) poses a threat to public health; or (vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541; (k) the reason for the alert; (l) the authority which created the alert; (m) a reference to the decision giving rise to the alert; (n) the action to be taken in the case of a hit; (o) links to other alerts pursuant to Article 48; (p) whether the person concerned is a family member of a citizen of the Union or other person who is a beneficiary of the right of free movement as referred to in Article 26; (q) whether the decision for refusal of entry and stay is based on: (i) a previous conviction as referred to in point (a) of Article 24(2); (ii) a serious security threat as referred to in point (b) of Article 24(2); (iii) circumvention of Union or national law on entry and stay as referred to in point (c) of Article 24(2);

	(iv) an entry ban as referred to in point (b) of Article 24(1); or (v) a restrictive measure referred to in Article 25; (r) the type of offence; (s) the category of the person's identification documents; (t) the country of issue of the person's identification documents; (u) the number(s) of the person's identification documents; (v) the date of issue of the person's identification documents; (w) **photographs and facial images**; (x) **dactyloscopic data** [encompassing both fingerprints and palmprints]; (y) a copy of the identification documents, in colour wherever possible.
Minimum data necessary to issue an alert (Art. 23) (a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases, which may be entered separately; (d) sex; (k) a reference to the decision giving rise to the alert; (l) action to be taken.	**Minimum data necessary to issue an alert** (Art. 22) (a) surnames; (g) date of birth; (k) the reason for the alert; (m) a reference to the decision giving rise to the alert; (n) the action to be taken in the case of a hit; (q) grounds on which the decision of refusal to entry is based.
For the purpose of **police and judicial cooperation in criminal matters**	
Council Decision 2007/533/JHA	**Regulation (EU) 2018/1862**
SIS II shall contain only those categories of data which are supplied by each of the Member States (Art. 20) (a) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately; (b) any specific, objective, physical characteristics not subject to change; (c) place and date of birth; (d) sex; (e) **photographs**; (f) **fingerprints**; (g) nationality(ies); (h) whether the person concerned is armed, violent or has escaped; (i) reason for the alert; (j) authority issuing the alert;	SIS shall contain only those categories of data which are supplied by each Member State (Art. 20): (a) surnames; (b) forenames; (c) names at birth; (d) previously used names and aliases; (e) any specific, objective, physical characteristics not subject to change; (f) place of birth; (g) date of birth; (h) gender; (i) any nationalities held; (j) whether the person concerned: (i) is armed; (ii) is violent; (iii) has absconded or escaped; (iv) poses a risk of suicide;

(k) a reference to the decision giving rise to the alert; (l) action to be taken; (m) link(s) to other alerts issued in SIS II pursuant to Article 52; (n) the type of offence.	(v) poses a threat to public health; or (vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541; (k) the reason for the alert; (l) the authority which created the alert; (m) a reference to the decision giving rise to the alert; (n) the action to be taken in the case of a hit; (o) links to other alerts pursuant to Article 63; (p) the type of offence; (q) the person's registration number in a national register; (r) for alerts referred to in Article 32(1), a categorisation of the type of case; (s) the category of the person's identification documents; (t) the country of issue of the person's identification documents; (u) the number(s) of the person's identification documents; (v) the date of issue of the person's identification documents; (w) **photographs and facial images**; (x) **relevant DNA profiles** [only for missing persons who need to be placed under protection]; (y) **dactyloscopic data**; (z) a copy of the identification documents, in colour wherever possible.
Minimum data for issuing an alert (Art. 23) surname(s) and forename(s), name(s) at birth and previously used names and any aliases which may be entered separately; sex; action to be taken; a reference to the decision giving rise to the alert (if available)	**Minimum data for issuing an alert** (Art. 23) surnames date of birth; the reason for the alert; the action to be taken in the case of a hit

There are also **data subjects' rights** to be respected, albeit their scope may vary depending on the different policy areas:

- Right to information
- Right to access
- Right to rectification
- Right to erasure
- Right to restriction
- Right to lodge a complaint with a supervisory authority or of seeking a judicial remedy
- Right not to be subject to a decision based solely on automated processing

Data protection remedies can be exercised in three main layers under EU law, namely: before the data controller (or processor); before DPAs; before national courts (Galetta & De Hert, 2015).

In relation to EU large scale databases, data subjects have the **right of access**, **rectification** of inaccurate data and **erasure** of unlawfully stored data**,** other than right of **restrictions of processing.** Nevertheless, those rights can be limited due to the nature and goals pursued by such control.

For instance, in case of SIS, for police and judicial cooperation in criminal matters, Art. 67 Regulation 1862 stipulates that "A Member State shall take a decision not to provide information to the data subject, in whole or in part, in accordance with national law, to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the data subject concerned, in order to: (a) avoid obstructing official or legal inquiries, investigations or procedures; (b) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; (c) protect public security; (d) protect national security; or (e) protect the rights and freedoms of others.

In cases referred to in the first subparagraph, the Member State shall inform the data subject in writing, without undue delay, of any refusal or restriction of access and of the reasons for the refusal or restriction. Such information may be omitted where its provision would undermine any of the reasons set out in points (a) to (e) of the first subparagraph. The Member State shall inform the data subject of the possibility of lodging a complaint with a supervisory authority or of seeking a judicial remedy. The Member State shall document the factual or legal reasons on which the decision not to provide information to the data subject is based. That information shall be made available to the supervisory authorities. For such cases, the data subject shall also be able to exercise his or her rights through the competent supervisory authorities." Therefore, either **direct access and indirect access** are foreseen.

Data transfers and right to access by competent authorities and European agencies and bodies

Under European law, restrictions or prohibitions on the free movement of personal data between EU Member States for reasons connected with the protection of natural persons regarding personal data processing are forbidden. When data flows for purposes related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties are subject to Directive 2016/680, that aims to ensure that the exchange of personal data by competent authorities within the Union is not restricted or prohibited for data protection reasons. Nevertheless, when it is about to flows to third countries and international organisation, the approach is more protective and in principle the transfer is admissible only in so far as the third country or international organisation ensure level of protection "essentially equivalent"[111] to that one granted in the country of origin.[112]

The legal framework on EU databases maintain as general rule the prohibition for data transfers, but with some specificities.

For example, in case of Eurodac, data recorded in the Central System shall not be transferred or made available to the authorities of any third country, international organisation or private entity established in or outside the Union, except for those third countries to which Regulation (EU) No 604/2013 applies.

[111] Case C-362/14 Judgment of the Court (Grand Chamber) of 6 October 2015 Maximillian Schrems v Data Protection Commissioner

[112] (European Union Agency for Fundamental Rights & EDPS, 2018) p. 249-254

For return decisions, data transfers to third countries are in principle allowed under the conditions set in Art. 15 of the Return regulation and on the basis of Art. 49 GDPR.

Data stored in VIS may be transferred e.g. to UN organisations (such as UNHCR), International Organization for Migration (IOM), the International Committee of the Red Cross if conditions of Art. 31 are satisfied.

With the interoperability regulations and the update of the legal framework, the possibilities for national and European authorities to access data contained in the various database for different purposes have increased.

For example, in the case of SIS, the following authorities have access to data for the following purposes:
For the time being
National competent authorities responsible for the identification of third country nationals for the purposes of:
(a) border control in accordance Schengen Borders Code;
(b) other police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities.
National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charge, **in the performance of their tasks**, as provided for in national legislation, and by their coordinating authorities.
Authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation relating to third-country nationals in the context of the application of the Community acquis relating to the movement of persons in accordance with Member State law [Art. 27(3) Regulation 1987/2006]
[all to be included in list sent to eu-LISA]
Europol within their mandate (Art. 41 Council Decision 2007/533/JHA)
Eurojust within their mandate (Art. 42 Council Decision 2007/533/JHA)
Vehicle registration services (directly if governmental, indirectly via a national competent authority if not) for the sole purpose of checking whether vehicles presented to them for registration have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings and only for: (a) data concerning motor vehicles with a cylinder capacity exceeding 50 cc; (b) data concerning trailers with an unladen weight exceeding 750 kg and caravans; (c) data concerning vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated. (Art. 1 Regulation 1986/2006)

By 28 December 2021
National competent authorities responsible for the identification of third country nationals for the purposes:
(a) border control, in accordance with Schengen Borders Code;
(b) police and customs checks carried out within the Member State concerned, and the coordination of such checks by designated authorities;
(c) the prevention, detection, investigation or prosecution of terrorist offences or other serious criminal offences or the execution of criminal penalties, within the Member State concerned, provided that Directive (EU) 2016/680 applies;
(d) examining the conditions and taking decisions related to the entry and stay of third-country nationals on the territory of the Member States, including on residence permits and long-stay visas, and to the return of third-country nationals, as well as carrying out checks on third-country nationals who are illegally entering or staying on the territory of the Member States;

(e) security checks on third-country nationals who apply for international protection, insofar as authorities performing the checks are not 'determining authorities' as defined in point (f) of Article 2 of Directive 2013/32/EU of the European Parliament and of the Council, and, where relevant, providing advice in accordance with Council Regulation (EC) No 377/2004;
(f) examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Visa Code;
(g) verifying different identities and combating identity fraud in accordance with Chapter V of Regulation (EU) 2019/817.
National competent authorities responsible for naturalisation, as provided for in national law, for the purposes of examining an application for naturalisation
National judicial authorities, including those responsible for the initiation of public prosecutions in criminal proceedings and for judicial inquiries prior to charging a person, in the performance of their tasks, as provided for in national law, and by their coordinating authorities for the purposes of Art. 24 [Conditions for entering alerts for refusal of entry and stay] and 25 [Conditions for entering alerts on third-country nationals subject to restrictive measures]
National competent authorities responsible for the identification of third country nationals for the purposes of examining visa applications and taking decisions related to those applications including on whether to annul, revoke or extend visas, in accordance with Visa Code, have right to access and search data related to "blank official documents which have been stolen, misappropriated, lost or purport to be such a document but are false" and "issued identity documents, such as passports, identity cards, residence permits, travel documents and driving licences which have been stolen, misappropriated, lost or invalidated or purport to be such a document but are false" [Art. 38(2)(k)(l)].
[Art. 34 Regulation 1861/2018]
Vehicle registration services (directly if governmental, indirectly via a national competent authority if not) for the sole purpose of checking whether vehicles presented to them for registration have been stolen, misappropriated or lost or are sought as evidence in criminal proceedings and only for: motor vehicles regardless of the propulsion system; trailers with an unladen weight exceeding 750 kg; caravans; vehicle registration certificates and vehicle number plates which have been stolen, misappropriated, lost or invalidated or purport to be such a document or plate but are false; identifiable component parts of motor vehicles [points (a), (b), (c), (m) and (p) of Art. 38(2) Regulation 1862/2018] [Art. 45 Regulation 1862/2018].
Europol where necessary to fulfil its mandate [Art. 35 Regulation 1861/2018]
European Border and Coast Guard teams, teams of staff involved in return-related tasks, and members of the migration management support teams insofar it is necessary for the performance of their task and as required by the operational plan for a specific operation. [Art. 36 Regulation 1861/2018]

In the case of the European search portal, Art. 7 Regulation 817/2019 provides that:

1. The use of the ESP shall be reserved to the Member State authorities and Union agencies having access to at least one of the EU information systems in accordance with the legal instruments governing those EU information systems, to the CIR and the MID in accordance with this Regulation, to Europol data in accordance with Regulation (EU) 2016/794 or to the Interpol databases in accordance with Union or national law governing such access.
Those Member State authorities and Union agencies may make use of the ESP and the data provided by it only for the objectives and purposes laid down in the legal instruments governing those EU information systems, in Regulation (EU) 2016/794 and in this Regulation.
2. The Member State authorities and Union agencies referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the central systems of the EES, VIS

and ETIAS in accordance with their access rights as referred to in the legal instruments governing those EU information systems and in national law. They shall also use the ESP to query the CIR in accordance with their access rights under this Regulation for the purposes referred to in Articles 20, 21 and 22.
3. The Member State authorities referred to in paragraph 1 may use the ESP to search data related to persons or their travel documents in the Central SIS referred to in Regulations (EU) 2018/1860 and (EU) 2018/1861.
4. Where provided for under Union law, the Union agencies referred to in paragraph 1 shall use the ESP to search data related to persons or their travel documents in the Central SIS.
5. The Member State authorities and Union agencies referred to in paragraph 1 may use the ESP to search data related to travel documents in the Interpol databases, where provided for and in accordance with their access rights under Union and national law.

Personal data protection:

- Regulation (EU) 2016/679 i.e. the General Data Protection Regulation (GDPR), replacing former Directive 95/46/EC[113]
- Directive (EU) 2016/680 i.e. the law enforcement Directive (LED), replacing former Council Framework 2008/977/JHA[114]
- Regulation (EU) 2018/1725 i.e. the General Data Protection Regulation for European Institutions (EUDPR), replacing former Regulation (EC) 45/2001[115]
- Regulation (EU) 2016/794 i.e. Europol Regulation[116]
- Regulation (EU) 2018/1726 i.e. eu-LISA Regulation[117]

[113] OJ L 119, 4.5.2016, p. 1–88
[114] OJ L 119, 4.5.2016, p. 89–131
[115] OJ L 295, 21.11.2018, p. 39–98
[116] OJ L 135, 24.5.2016, p. 53–114
[117] OJ L 295, 21.11.2018, p. 99–137.

8 Border management related instruments

8.1.1 European large-scale databases

There are several different large-scale IT databases are used at European level to facilitate police cooperation and to help manage borders and migration.

8.1.1.1 Schengen Information System II (SIS II)

The legal framework related to the SIS II has undergone significant revisions, whose effects in EU legal order will deploy full effects by December 2021, when the Commission will adopt a decision setting the date on which SIS operations start pursuant to the new Regulations.[118]

SIS II is the database containing **alerts for missing/wanted objects and people**. Before the adoption of 2018 Regulations, alerts were created and could be consulted only by competent national authorities (e.g. national border control, police, customs, judicial, visa and vehicle registration authorities)[119]. But one of the main novelties of the new framework is that **Europol**, **European Border and Coast Guard teams**, **teams of staff involved in return-related tasks**, and **members of the migration management support teams will have access to SIS database** (Art. 35 and 36 Regulation 2018/1861), together with **Eurojust** (Art. 48, 49, 50 Regulation 2018/1862) will be able to consult SIS database when necessary to fulfil their mandate.

Hereafter, the current alert categories contained in SIS II:

- **Refusal of entry or stay** [Art. 24 Regulation (EC) No 1987/2006] This alert category covers **third-country nationals** who are not entitled to enter into or stay in the Schengen Area.
- **Persons wanted for arrest** [Art. 26 Council Decision 2007/533/JHA] This alert category covers persons for whom a European Arrest Warrant or Extradition Request (Associated Countries) has been issued.
- **Missing persons** [Art. 32 Council Decision 2007/533/JHA] The purpose of this alert category is to find missing persons, **including children**, and to place them under protection if lawful and necessary.
- **Persons sought to assist with a judicial procedure** [Art. 34 Council Decision 2007/533/JHA] The purpose of this alert category is to find out the place of residence or domicile of persons sought to assist with criminal judicial procedures (for example witnesses).
- **Persons and objects for discreet or specific checks** [Art. 36 Council Decision 2007/533/JHA] The purpose of this alert is to obtain information on persons or related objects for the purposes of prosecuting criminal offences and for the prevention of threats to public or national security.
- **Objects for seizure or use as evidence in criminal procedures** [Art. 38 Council Decision 2007/533/JHA] This alert covers objects (for example vehicles, travel documents, credit cards,

[118] See Art. 65 in combination with Art. 66 Regulation 2018/1861 and Art. 78 in combination with Art. 79 Regulation 2018/1862 and also http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-the-revision-of-the-schengen-information-system-ii

[119] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en. For further details on alerts categories, please refer to https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/alerts-and-data-in-the-sis_en

number plates and industrial equipment) being sought for the purposes of seizure or use as evidence in criminal proceedings[120].

The new types of alerts that will be introduced by 2021 are:

- **Return decisions** will be introduced to improve the enforcement of return decisions issued to irregularly staying third-country nationals [Regulation (EU) 2018/1860]
- **Unknown wanted persons** containing only dactyloscopic data, i.e. complete or incomplete sets of fingerprints or palm prints discovered at the scenes of terrorist offences or other serious crimes under investigation, to be entered where there is very high degree of probability they belong to a perpetrator of the offence. [Art. 40 Regulation 1862/2018]
- **Preventive alerts on persons who are in need of protection**, in addition to existing alerts on missing persons (children in high risk of abduction and people in need) [Art. 32 Regulation 1862/2018][121]

SIS' architecture is composed of: 1) a central system (**Central SIS**) constituted by: (i) a **technical support function** (**CS-SIS**) containing the **SIS database**, including a **backup** CS-SIS, located in the two technical sites of eu-LISA; (ii) a **uniform national interface** (**NI-SIS**). 2) a national system (**N.SIS**) in each Member States, consisting of the national data systems which communicate with Central SIS, **including at least one national or shared backup N.SIS**. Also, a **N.SIS may contain** a data file, a **national or shared copy** containing a complete or partial copy of the SIS database. This is to ensure uninterrupted availability to end users. Member States intending to establish a shared copy or shared backup N.SIS to be used jointly shall agree their respective responsibilities in writing and notify their arrangement to the Commission. 3) a **communication infrastructure between CS-SIS, backup CS-SIS and NI-SIS** ('the Communication Infrastructure') **that provides an encrypted virtual network dedicated to SIS data and the exchange of data** between SIRENE Bureaux and that ensure the uninterrupted availability of SIS. It shall include **redundant and separated paths** for the connections between CS-SIS and the backup CS-SIS and shall also include redundant and separated paths for the connections between each SIS national network access point and CS-SIS and backup CS-SIS.

Member States shall enter, update, delete and search SIS data through their own N.SIS. It shall not be possible to search the data files of other Member States' N.SIS, except in the case of shared copies.

Moreover, each Member State operating SIS has set up a national SIRENE Bureau, **operational 24/7**, **responsible for any supplementary information exchange** and coordination of activities connected to SIS II alerts[122]. SIS II indeed only contains the indispensable information (i.e. alert data) allowing the identification of a person or an object and the necessary action to be taken. But, for implementing certain provisions foreseen under the SIS II legal instruments, and for SIS II to function properly, either on a bilateral or multilateral basis, in addition, Member States shall exchange supplementary information related to the alert[123]. The purposes of the exchange of information include: following a hit to allow the appropriate action to be taken (e.g. matching an alert); dealing with the quality of SIS II data (e.g. when data has been unlawfully entered or is factually inaccurate); dealing with data subjects' rights, in particular the right of access to data…

[120] Ibid.
[121] European Commission – Statement, Security Union: Commission welcomes agreement on a reinforced Schengen Information System (Brussels, 12 June 2018) http://europa.eu/rapid/press-release_STATEMENT-18-4133_en.htm
[122] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/sirene-cooperation_en
[123] Commission Implementing Decision (EU) 2017/152 1.1.

Since March 2018, the Automated Fingerprint Identification System (AFIS) allows identifying persons just on the basis of his/her fingerprints (a "one-to-many" search), whereas before fingerprints were used to confirm the identity of a person following a check on his/her name and/or date of birth. [124]

With the entry into force of the new legal framework, the goal will be to use **photographs and facial images to identify persons in the context of regular border crossing points** (Art. 33 and 43 Regulations 1861 and 1862).

SIS related legal framework:[125]

- Convention Implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic, on the gradual abolition of checks at their common borders, 19 June 1990[126]
- 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 (cooperation on vehicle registration)[127] that will be repealed by Regulation 2018/1862 by 28 December 2021
- 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) (border control cooperation)[128] that will be repealed by Regulation 2018/1861 by 28 December 2021
- Commission Recommendation C(2006)5186 of 6 November 2006 establishing a common "Practical Handbook for Border Guards (Schengen Handbook)" to be used by Member States' competent authorities when carrying out the border control of persons (as amended)
- Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II) (law enforcement cooperation)[129] that will be repealed by Regulation 2018/1862 by 28 December 2021
- Commission Decision 2010/261/EU of 4 May 2010 on the Security Plan for Central SIS II and the Communication Infrastructure[130] that will be repealed by Regulation 2018/1862 by 28 December 2021
- 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) as amended by Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU)

[124] https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/alerts-and-data-in-the-sis_en
[125] See also: (European Union Agency for Fundamental Rights 2018, p. 23).
[126] OJ L 239, 22.9.2000, p. 19–62.
[127] OJ L 381, 28.12.2006, p. 1–3.
[128] OJ L 381, 28.12.2006, p. 4–23.
[129] OJ L 205, 7.8.2007, p. 63–84.
[130] OJ L 112, 5.5.2010, p. 31–37.

2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA[131]

- Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II)[132] [notified under document C(2017) 5893]
- Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011[133]
- Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals[134] that will apply by 28 December 2021
- Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006[135]
- Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU[136]

8.1.1.2 Visa information system (VIS)

VIS is the large-scale IT-system related to **short-stay visa**, enabling the **exchange of visa information** and the **matching of biometric data to verify the authenticity of a visa.**[137]

As regards the architecture, VIS is composed by a 1) **central Visa Information System** (CS-VS), for which operational management eu-LISA is responsible; a 2) national system (**N-VIS**) in each Member State, for which single Member States are in charge; and a 3) **communication infrastructure** connecting them, again managed by eu-LISA.[138]

The objective of the database (Art. 2 Regulation 767/2008) is the implementation of the common visa policy, consular cooperation and consultation between central visa authorities by facilitating the exchange of data between Member States on applications and on the decisions relating thereto, in order:

[131] OJ L 77, 23.3.2016, p. 1–52.
[132] OJ L 231, 7.9.2017, p. 6–51.
[133] OJ L 295, 21.11.2018, p. 99–137.
[134] OJ L 312, 7.12.2018, p. 1–13.
[135] OJ L 312, 7.12.2018, p. 14–55.
[136] OJ L 312, 7.12.2018, p. 56–106.
[137] (Quintel, 2018) p. 6, 7.
[138] https://www.data-protection-authority.gv.at/the-visa-information-system

(a) to facilitate the visa application procedure; (b) to prevent the bypassing of the criteria for the determination of the Member State responsible for examining the application; (c) to facilitate the fight against fraud; (d) to facilitate checks at external border crossing points and within the territory of the Member States; (e) to assist in the identification of any person who may not, or may no longer, fulfil the conditions for entry to, stay or residence on the territory of the Member States; (f) to facilitate the application of Regulation (EC) No 343/2003 [establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national]; (g) to contribute to the prevention of threats to the internal security of any of the Member States.

Therefore, **administrative goals are combined with security and law enforcement ones**.

Commission's proposal to upgrade the VIS is aimed at: expanding the scope of the database by adding long stay-visas and residence permits to the system; enabling more thorough background checks on visa applicants; closing security information gaps through better information exchange between Member States and ensuring full interoperability with other EU-wide databases.[139]

VIS related legal framework:

- Council Decision 2004/512/EC of 8 June 2004 establishing the Visa Information System (VIS)[140]
- 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)[141] as (lastly) amended by Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa
- Regulation (EC) No 810/2009 of the European Parliament and of the Council of 13 July 2009 establishing a Community Code on Visas[142] as (lastly) amended by Regulation (EU) 2016/399
- Commission Decision 2006/648/EC of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System[143] [notified under document number C(2006) 3699]
- Commission Implementing Decision C(2019) 3464 final amending Commission Decision No C(2010) 1620 final of 19 March 2010 establishing the Handbook for the processing of visa applications and the modification of issued visa ("Visa Handbook")
- Proposal COM(2018) 302 final [2018/0152(COD)] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EC) No 767/2008, Regulation (EC) No 810/2009, Regulation (EU) 2017/2226, Regulation (EU) 2016/399, Regulation XX/2018 [Interoperability Regulation], and Decision 2004/512/EC and repealing Council Decision 2008/633/JHA
- 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

[139] https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Vis
[140] OJ L 213, 15.6.2004, p. 5–7.
[141] OJ L 218, 13.8.2008, p. 60–81.
[142] OJ L 243, 15.9.2009, p. 1–58.
[143] OJ L 267, 27.9.2006, p. 41–43.

(Schengen Borders Code) as amended by Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA[144]

8.1.1.3 Dublin system: the EUROpean Asylum DACtyloscopy database (Eurodac) and DubliNet netwok

Eurodac is the EU database storing fingerprints of asylum seekers and irregular migrants entering in a Member State or Associated Country. Each time someone applies for asylum in one of the 28 EU Member States and Associated Countries, their fingerprints are transmitted to the Eurodac central system. Therefore, it is valuable tool for officers deployed at borders and hotspots.[145]

The database is so structured:

1) **Central System**, i.e. a computerised central fingerprint database composed of a **Central Unit** and a **Business Continuity Plan and System**;
2) **Communication Infrastructure** between the Central System and Member States that provides an encrypted virtual network dedicated to Eurodac data;
3) single **National Access Point** [Art. 3 Regulation (EU) No 603/2013].

DubliNet is the secure electronic communication network between the national authorities dealing with asylum applications through which the two involved Member States can exchange personal data through different from Eurodac data (e.g. name, date of birth, nationality, photo, details on family members and in some cases addresses).

The Proposal to revise Eurodac Regulation is aimed at extending Eurodac's scope, allowing the storage of and searching using biometric data of irregular migrants found illegally staying in the EU, and at facilitating returns to contribute to the fight against irregular migration.[146]

Eurodac related legal framework:

- Dublin Regulation (EU) No 604/2013 of the European Parliament and of the Council of 26 June 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 (recast)[147]
- 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

[144] Ibid. 131.
[145] https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Eurodac
[146] Ibid.
[147] OJ L 180, 29.6.2013, p. 31–59.

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[148]

- Commission Regulation (EC) No 1560/2003 of 2 September 2003 laying down detailed rules for the application of Council Regulation (EC) No 343/2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national[149]
- Proposal COM(2016)272 final [2016/0132 (COD)] for a Regulation of the European Parliament and of the Council 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], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast)

8.1.1.4 Entry/Exit System (EES)

The EES will electronically register the time and place of entry and exit of **third-country nationals**, **both those requiring a visa and those visa-exempt**, admitted for a short stay of 90 days in any 180-day period and calculate the duration of their authorised stay, **other than those refused to entry**. **It will replace the obligation to stamp the passports of third-country nationals which is applicable to all Member States** (but stamps will continue to be posed till the system will be implemented). The EES is expected to improve the management of external borders, to address the phenomenon of overstaying reducing irregular migration, and to facilitate the management of migration flows. Furthermore, it aims to contribute to the fight against terrorism and serious crime and to ensure a high level of internal security.[150]

The technical architecture will be the following: 1) a **central system** which will operate a computerised central database of biometric and alphanumeric data (a mix of letters and numbers); 2) a **national uniform interface** in each participating country; 3) a **secure communication channel between the EES central system and the central system of the VIS**; 4) 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); 5) a **data repository** to obtain customisable reports and statistics; 6) a **web service** to enable non-EU nationals to verify their remaining authorised stay.[151]

Albeit Member States remain free to decide whether and to what extent to make use of technologies, the implementation of EES will change border practices defined in the Schengen borders code, opening for a higher degree of automation. Regulation (EU) 2017/2225 introduced new concepts as "self-service system", i.e. an automated system which performs all or some of the border checks that are applicable to a person and which may be used for pre-enrolling data in the EES; "e-gate" i.e. an infrastructure operated by electronic means where an external border or an internal border where

[148] OJ L 180, 29.6.2013, p. 1–30.
[149] OJ L 222, 5.9.2003, p. 3–23.
[150] Cf. shttps://ec.europa.eu/home-affairs/what-we-do/networks/european_migration_network/glossary_search/entryexit-system-ees_en
[151] Cf. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A4326388

controls have not yet been lifted is actually crossed; "automated border control system" means a system which allows for an automated border crossing, and which is composed of a self-service system and an e-gate; "confirmation of the authenticity and integrity of the chip data" means the process by which it is verified, through the use of certificates, that the data on the electronic storage medium (chip) originate from the issuing authority and that they have not been changed.

The implementing rules of EES provide for performance values for biometric accuracy, whose monitoring need to be carried on by eu-LISA at least monthly. The minimum performance values are: the **failure to enrol rate** (FTER), i.e. the proportion of registrations with insufficient quality of the biometric enrolment; the **false positive identification rate** (FPIR), i.e. the proportion of returned matches during a biometric search which do not belong to the checked traveller; the **false negative identification rate** (FNIR) i.e. the proportion of missed matches during a biometric search even though the traveller's biometric data were registered.

The False Match(ing) Rate (FMR) is the proportion of impostor attempts that are falsely declared to match a template of another object (a person's biometric template). The False Non-Match(ing) Rate (FNMR) is the proportion of genuine attempts that are falsely declared not to match a template of the same object.

EES related legal framework:

- 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[152]
- 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[153]
- Commission Implementing Decision (EU) 2019/326 of 25 February 2019 laying down measures for entering the data in the Entry/Exit System (EES)[154]
- Commission Implementing Decision (EU) 2019/329 of 25 February 2019 laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES)[155]

8.1.1.5 European Travel Information and Authorisation System (ETIAS)

ETIAS is a **pre-travel authorisation system for visa exempt travellers**. Its key function is to verify if a third country national meets entry requirements before travelling to the Schengen area. The information submitted, via an online application ahead of their arrival at borders enabling pre-travel assessment of irregular migration risks, security or public health risk checks. This shall be done by automatically processing each application submitted against EU and relevant Interpol databases, and

[152] OJ L 327, 9.12.2017, p. 1–19.
[153] OJ L 327, 9.12.2017, p. 20–82.
[154] OJ L 57, 26.2.2019, p. 5–9.
[155] OJ L 57, 26.2.2019, p. 18–28.

a dedicated ETIAS watch-list whilst respecting clearly defined screening rules.[156] ETIAS' architecture consists of 1) the **ETIAS Information System** [including a **ETIAS central system**, a **National Uniform Interface** (NUI) and a secured **Communication Infrastructure** connecting them and the other interoperable databases]; 2) the **ETIAS Central Unit**, established within Frontex and operational 24/7; 3) **ETIAS National Units**.

ETIAS related legal framework:

- 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[157]
- Regulation (EU) 2018/1241 of the European Parliament and of the Council of 12 September 2018 amending Regulation (EU) 2016/794 for the purpose of establishing a European Travel Information and Authorisation System (ETIAS)[158]

8.1.1.6 European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)

ECRIS-TCN will be a centralised system allowing Member State's authorities to identify which other Member States hold criminal records on the third country nationals or stateless persons being checked, so that they can then use the existing ECRIS system to address requests for conviction information only to the identified Member States.[159] The architecture is composed by:

1. a **central system** in which identity information on convicted third-country nationals is stored;
2. a **national central access point** in each Member State;
3. a **communication infrastructure** between them;
4. an **interface software** enabling the connection of the competent authorities to the central system via the national central access points and the communication infrastructure referred.

ECRIS related legal framework:

- Regulation (EU) 2019/816 of the European Parliament and of the Council of 17 April 2019 establishing a centralised system for the identification of Member States holding conviction information on third-country nationals and stateless persons (ECRIS-TCN) to supplement the European Criminal Records Information System and amending Regulation (EU) 2018/1726[160]
- Directive (EU) 2019/884 of the European Parliament and of the Council of 17 April 2019 amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third-country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA[161]

[156] Cf. https://www.eulisa.europa.eu/Newsroom/News/Pages/ETIAS-Regulation-published-in-the-Official-Journal.aspx
[157] OJ L 236, 19.9.2018, p. 1–71.
[158] OJ L 236, 19.9.2018, p. 72–73.
[159] Cf. https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn
[160] OJ L 135, 22.5.2019, p. 1–26.
[161] OJ L 151, 7.6.2019, p. 143–150.

8.1.1.7 Interoperability

With the entry into force of the two regulations on **interoperability**, one for the EU information systems in the field of **borders and visa** [i.e. Regulation (EU) 2019/817, applicable to the EES, VIS, ETIAS and SIS] and one in the field of **police and judicial cooperation, asylum and migration** [i.e. Regulation (EU) 2019/818 applicable to Eurodac, SIS and ECRIS-TCN], those databases will become interoperable.

The regulations establish a **European search portal** (ESP), allowing competent authorities to search multiple EU information systems simultaneously (including Europol data[162] and Interpol databases[163]), using both biographical and biometric data ;[164] a **shared biometric matching service** (BMS), enabling to search and compare biometric data (fingerprints and facial images) from several systems, that will store biometric templates;[165] a **common identity repository** (CIR), containing biographical and biometric data of third-country nationals available in several EU information systems;[166] a **multiple identity detector** (MID), checking whether the biographical identity data contained in the search exists in other systems covered, to enable the detection of multiple identities linked to the same set of biometric data.[167]

The ESP shall be composed of: (a) a **central infrastructure**, including a search portal enabling the simultaneous querying of the EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN as well as of Europol data and the Interpol databases; (b) a **secure communication channel** between the ESP, Member States and Union agencies that are entitled to use the ESP; (c) a **secure communication infrastructure** between the ESP and the EES, VIS, ETIAS, Eurodac, Central SIS, ECRIS-TCN, Europol data and the Interpol databases as well as between the ESP and the central infrastructures of the CIR and the MID.

The BMS shall be composed of: (a) a **central infrastructure**, which shall replace the central systems of the EES, VIS, SIS, Eurodac and ECRIS-TCN respectively, to the extent that it shall store biometric templates and allow searches with biometric data; (b) a **secure communication infrastructure** between the shared BMS, Central SIS and the CIR.

The CIR shall be composed of: (a) a **central infrastructure** that shall replace the central systems of respectively the EES, VIS, ETIAS, Eurodac and ECRIS-TCN to the extent that it shall store certain kinds of data [as referred to in Article 18]; (b) a **secure communication channel** between the CIR, Member States and Union agencies that are entitled to use the CIR in accordance with Union law and national law; (c) a **secure communication infrastructure** between the CIR and the EES, VIS, ETIAS, Eurodac and ECRIS-TCN as well as with the central infrastructures of the ESP, the shared BMS and the MID.

The new regulations do not modify the rights of access as set out in the legal basis relevant for each European information system. The European search portal will flag where data or links exist in

[162] i.e. cross-checking aimed at identifying connections or other relevant links between information related to: (i) persons who are suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or who have been convicted of such an offence; (ii) persons regarding whom there are factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent; (b) analyses of a strategic or thematic nature; (c) operational analyses.
[163] i.e. Interpol Stolen and Lost Travel Document database (SLTD database) and the Interpol Travel Documents Associated with Notices database (TDAWN database)
[164] Art. 6 Regulation (EU) 2019/817.
[165] Art. 12 Regulation (EU) 2019/817.
[166] Art. 17 Regulation (EU) 2019/817.
[167] Cf. https://www.consilium.europa.eu/en/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement s

relation to a query, but the system will only show each authority the data to which they already have a right of access under previous legislation setting up the different databases.[168]

Interoperability legal instruments:

- Regulation (EU) 2019/817 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of borders and visa and amending Regulations (EC) No 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 and (EU) 2018/1861 of the European Parliament and of the Council and Council Decisions 2004/512/EC and 2008/633/JHA[169]
- Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816[170]

8.1.2 Other instruments related to border management and/or exchange of information

8.1.2.1 Prüm decision

Council Decision 2008/615/JHA stems from a multilateral treaty signed in 2005 by Belgium, Germany, Spain, France, Luxembourg, the Netherlands and Austria but it has been transformed into a legal instrument binding all EU countries. Aimed to improve cross-border cooperation between EU countries' police and judicial authorities to more effectively combat terrorism and cross-border crime, it focuses particularly on automated exchanges of information.

The decision sets out rules with regard to the **automated transfer of DNA profiles, dactyloscopic data and certain national vehicle registration data**; supply of data in relation to major events; supply of information in order to prevent terrorist offences; other measures for stepping up cross-border police cooperation (Art. 1). EU countries must establish national DNA analysis files for the purpose of investigating criminal offences. Reference data, consisting of the non-coding part of the DNA and of a reference number that does not enable an individual to be identified, must be made available to other EU countries to carry out automated searches. Searches are performed via national contact points by comparing DNA profiles, but only on the basis of individual cases and in a hit/no-hit manner. EU countries must also make available reference data from the national automated fingerprint identification systems (AFIS). The searches are carried out by comparing dactyloscopic data and, similarly to DNA searches, only in individual cases on a hit/no-hit basis. National contact points must also be given access to certain national vehicle registration data via automated online searches. Other measures for enhancing cross-border police cooperation. EU countries can carry out joint patrols and other joint operations to prevent criminal offences and to maintain public order and security on a given EU country's territory. EU countries are to provide mutual assistance to each other in cases of mass gatherings and other comparable major events, disasters and serious accidents.[171]

[168] https://www.consilium.europa.eu/en/press/press-releases/2019/02/05/interoperability-between-eu-information-systems-council-presidency-and-european-parliament-reach-provisional-agreement
[169] OJ L 135, 22.5.2019, p. 27–84
[170] OJ L 135, 22.5.2019, p. 85–135
[171] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Ajl0005

Prüm legal framework:

- Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime[172]
- Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime[173]

8.1.2.2 European Border Surveillance System (Eurosur)

Eurosur is a multipurpose system for cooperation between involving the EU Member States and Frontex. It was set up to improve situational awareness and increase reaction capability at external borders. It is aimed to prevent cross-border crime and irregular migration and contribute to protecting migrants' lives. As regards the structure, each Member State has a **National Coordination Centre** (NCC) which **coordinates and exchanges information** among all the authorities responsible for external border surveillance as well as with other NCCs and Frontex. The Member State maintains its national situational picture providing an overview of the situation at its external border, including the events taking place and assets deployed, as well as relevant background information and analysis. Frontex maintains a European situational picture and common pre-frontier intelligence picture that contain information on the situation at European borders and the pre-frontier area. This information is available to all the EU Member States. Furthermore, neighboring Member States share the situational picture of their neighboring external border sections with each other. Member States can request Frontex' assistance in selective monitoring of areas or vessels of interest for Eurosur purposes by using tools like satellite imagery or ship reporting systems. This can be used to detect cases of irregular migration or cross-border crime, but also to locate a boat in distress.[174]

Eurosur related framework:

- Regulation (EU) No 1052/2013 of the European Parliament and of the council of 22 October 2013 establishing the European Border Surveillance System (Eurosur)[175]
- Proposal COM(2018)631 final [2018/330 (COD)] for a Regulation of the European Parliament and of the Council on the European Border and Coast Guard and repealing Council Joint Action n°98/700/JHA, Regulation (EU) n° 1052/2013 of the European Parliament and of the Council and Regulation (EU) n° 2016/1624 (Frontex Regulation) of the European Parliament and of the Council

8.1.2.3 Passenger Name Records (PNR) legal framework

Passenger Name Records are the information, such as dates of travel, travel itinerary, ticket information, contact details, travel agent, means of payment, seat number and baggage information, provided by passengers and collected by airlines, in the normal course of their business, for enabling reservations and carrying out the check-in process. They are an important law enforcement tool aimed

[172] OJ L 210, 6.8.2008, p. 1–11
[173] OJ L 210, 6.8.2008, p. 12–72
[174] Cf. https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/border-crossing/eurosur_en
[175] OJ L 295, 6.11.2013, p. 11–26

at allowing to prevent, detect and investigate terrorism and other forms of serious crime (such as drugs, human trafficking, child sexual exploitation and others).

In case of PNR, it is evident how the purposes for which data are processed can become blurred: what is *prima facie* collected by carriers for commercial purposes and performance of contracts, has also a utility for combating crimes.

PNR related framework:

- 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[176]
- 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[177]
- 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[178]

8.1.2.4 Advanced passenger information (API) directive

Carriers, i.e. any natural or legal person whose occupation it is to provide passenger transport by air, have an obligation to transmit, by the end of the check-in, at the request of the authorities responsible for carrying out checks on persons at external borders, information (e.g. 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 Member States, code of transport, departure and arrival time of the transportation, total number of passengers carried on that transport the initial point of embarkation) concerning the transported passengers carried to an authorised border crossing point through which these persons will enter the territory of an Schengen Member State.

API legal framework:

- Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data[179]

8.1.2.5 Custom Information System (CIS)

The Customs Information System+ (CIS+) is part of the Anti-Fraud Information System (AFIS) a central database managed by OLAF that provides for a means for the exchange, storage and rapid dissemination of information among the designated competent authorities, to improve effectiveness of the cooperation and control procedures of the designated competent authorities.[180] Data entered into the CIS relate to goods, means of transport, businesses, persons, trends in fraud, availability of expertise, goods detained, seized and confiscated and cash detained, seized and confiscated.

[176] OJ L 119, 4.5.2016, p. 132–14.
[177] OJ L 186, 14.7.2012, p. 4–16.
[178] OJ L 215, 11.8.2012, p. 5–14.
[179] OJ L 261, 6.8.2004, p. 24–27.
[180] Cf. https://ec.europa.eu/anti-fraud/sites/antifraud/files/17_cisplus_en.pdf

The CIS system helps to prevent, investigate and prosecute breaches of EU customs or agricultural legislation.

CIS legal framework:

- 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[181]
- Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes[182]

8.1.2.6 Identity cards regulation

The Regulation provides for technical rules related to ID cards issued by Member States. Pursuant to Art. 3(5), identity cards will have to include a highly secure storage medium, having sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data, containing a **facial image** of the holder of the card and **two fingerprints** in interoperable digital formats. For the capture of biometric identifiers, Member States shall apply the technical specifications as established by Commission Implementing Decision C(2018) 7767.[183]

For faces: FULL FRONTAL IMAGE complying with ICAO Doc 9303 7th edition, Part 9 and ISO/IEC 19794-5:2005, Biometric Data Interchange Formats –Part 5: Face Image Data.

For fingerprints:

The primary fingerprints to be incorporated into the European Passport shall be PLAIN IMPRESSIONS OF THE LEFT AND RIGHT INDEX FINGER.

For each hand, if the index finger is injured or missing, or has an ISO/IEC 19794-4 score of 0 to 25, a plain impression of the middle finger, ring finger or thumb of the same hand shall be recorded where a higher ISO score is available.

If all fingers on one hand are of the low-quality score indicated above, a plain impression of the finger with the best score shall be taken.[184]

Albeit it is related to ID cards and residence documents issued to EU citizens and their family Members exercising the right of free movement, it is still relevant for the legal benchmark because also those subjects are checked when crossing external borders. Therefore, no gate crossing point solutions should be capable to read ID cards.

Identity cards requirements:

- Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence

[181] OJ L 82, 22.3.1997, p. 1–16.
[182] OJ L 323, 10.12.2009, p. 20–30.
[183] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/borders-and-visas/document-security/docs/comm_decision_c_2018_7774_f1_annex_en.pdf
[184] Ibid.

documents issued to Union citizens and their family members exercising their right of free movement[185] applicable from 2 August 2021

8.1.2.7 Passports regulation

The regulation does not apply to National ID cards issued by Member States to their nationals nor to temporary passports and travel documents having a validity of less than 12 months. Ex Art. 1, passports and travel documents shall include a highly secure storage medium which shall contain a **facial image and two flat fingerprints** in interoperable formats (children younger than 12 and person where fingerprinting is physically impossible are exempted). The data shall be secured and the storage medium shall have sufficient capacity and capability to guarantee the integrity, the authenticity and the confidentiality of the data. Biometric identifiers shall be taken by qualified and duly authorised staff of the national authorities responsible for issuing passports and travel documents and shall only be used for verifying: (a) the authenticity of the passport or travel document; (b) the identity of the holder by means of directly available comparable features when the passport or travel document is required to be produced by law.

Even in this case, albeit it is related to passports issued to EU citizens, it is still relevant for the legal benchmark because also those subjects are checked when crossing external borders.

Passports requirements:

- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

8.1.2.8 Dual-use items regulation

Dual-use items are those items, including software and technology, which can be used for both civil and military purposes. They include all goods which can be used for both non-explosive uses and that can assist in any way in the manufacture of nuclear weapons or other nuclear explosive devices.[186]

EU export controls regime reflect commitments agreed upon in key multilateral export control regimes[187] and include: common export control rules, including a common set of assessment criteria and common types of authorisations (individual, global and general authorisations); a common EU list of dual-use items; a 'catch-all clause' for non-listed items which could be used e.g. in connection with a Weapon of Mass Destruction (WMD) programme; controls on brokering dual-use items and their transit through the EU; specific control measures to be introduced by exporters, such as record-keeping and registers; provisions setting up a network of competent authorities supporting the exchange of information and the consistent implementation and enforcement of controls throughout the EU. Dual-use items may be traded freely within the EU, except for some particularly sensitive items, which transfer within the EU remains subject to prior authorization.[188]

[185] OJ L 188, 12.7.2019, p. 67–78.
[186] Art. 1 Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.
[187] Such as the Australia Group, the Wassenaar Arrangement, the Nuclear Suppliers Group and the Missile Technology Control Regime; UN Security Council Resolution 1540; The Nuclear Non-Proliferation Treaty; the Chemical Weapons Convention; the Biological Weapons Convention.
[188] https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/

The regime is relevant for border control and management considering the progressive militarisation of border surveillance. For instance, Unmanned Aerial Vehicles and satellite applications are considered dual-items and have been deployed by certain member states for border surveillance[189]

Dual-use items – legal requirements:

- Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items[190]

8.1.2.9 Unmanned aircraft systems

Rules concerning unmanned aircraft systems are relevant providing that they may be employed for border surveillance activities.[191]

Unmanned aircraft systems – legal requirements:

- Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems[192]
- Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft[193]

8.2 European bodies and agencies involved in border management

The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (**eu-LISA**)[194] is in charge of the operational management of SIS, VIS, Eurodac and of the preparation, development and operational management of EES, ETIAS and ECRIS-TCN[195]. Operational management consists of "the tasks necessary to keep large-scale IT systems functioning in accordance with the specific provisions applicable to each of them, including responsibility for the communication infrastructure used by them. The large-scale IT systems must not exchange data or enable sharing of information or knowledge unless authorised by a specific EU law".[196]

[189] https://research.utwente.nl/en/publications/deploying-drones-in-policing-european-borders-constraints-and-cha
[190] OJ L 134, 29.5.2009, p. 1–269
[191] Frontex for instance, the European Border and Coast Guard Agency, has begun testing the use of Remotely Piloted Aircraft Systems (RPAS) in Greece, Italy and Portugal to monitor the European Union's external borders. <https://frontex.europa.eu/media-centre/news-release/frontex-begins-testing-unmanned-aircraft-for-border-surveillance-zSQ26A>
[192] OJ L 152, 11.6.2019, p. 1–40
[193] OJ L 152, 11.6.2019, p. 45–71
[194] Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011
[195] https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems
[196] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4374366

From a data protection point of view, the supervision of these EU large-scale IT databases is shared between the European Data Protection Supervisor (**EDPS**) and national Data Protection Authorities (DPAs) that together form Supervision Coordination Groups (SCGs).[197]

The **European Border and Coast Guard** (commonly known as **Frontex**)[198] oversees the effective implementation of integrated border management at the external borders of the European Union (EU) as well as of the Schengen associate countries (Iceland, Norway, Liechtenstein and Switzerland).[199] The components of integrated border management encompass e.g. border control, search and rescue operations, analysis of the risks for internal security and analysis of the threats that may affect the functioning or security of the external borders; technical and operational measures within the Schengen area which are related to border control and designed to address illegal immigration and to counter cross-border crime better; return of third-country nationals who are the subject of return decisions issued by a Member State; use of state-of-the-art technology including large-scale information systems etc. [Art. 4 Regulation (EU) 2016/1624].

As regards other asylum related issues, the **European Asylum Support Office** (EASO) contributes to the development of the Common European Asylum System by facilitating, coordinating and strengthening practical cooperation among Member States on the many aspects of asylum.[200]

As anticipated, **Europol** (the European agency for law enforcement cooperation) and **Eurojust** (the European agency for judicial cooperation), will have margin to access data contained in the SIS.

The **European Anti-Fraud Office** (OLAF) is in charge of managing CIS+.

eu-LISA legal framework:

- Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011[201]
- 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[202]
- Regulation (EU) No 439/2010 of the European Parliament and of the Council of 19 May 2010 establishing a European Asylum Support Office[203]
- 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

[197] https://edps.europa.eu/data-protection/supervision-coordination_en
[198] 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
[199] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:230103_3
[200] https://easo.europa.eu/about-us
[201] OJ L 295, 21.11.2018, p. 99–137.
[202] OJ L 251, 16.9.2016, p. 1–76.
[203] OJ L 132, 29.5.2010, p. 11–28.

and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA[204]

- Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA[205]
- Regulation (EU, Euratom) No 883/2013 of the European Parliament and of the Council of 11 September 2013 concerning investigations conducted by the European Anti-Fraud Office (OLAF) and repealing Regulation (EC) No 1073/1999 of the European Parliament and of the Council and Council Regulation (Euratom) No 1074/1999[206]

8.3 Functional requirements of contemporary practices of border management

Before providing an overview of contemporary practices of border management, it is necessary to preliminarily give some definitions pursuant to Art. 2 of the Regulation (EU) 2016/399 [the so called Schengen Borders Code (SBC)].

First of all, it is necessary to clarify the concept of **border**. Borders may be internal or external. I**nternal borders** may be common land borders, including river and lake borders, of the Member States; airports of the Member States for internal flights; sea, river and lake ports of the Member States for regular internal ferry connections. "Internal" must be read in the sense of involving exclusively the territories of Member States and not third countries.

Residually, **external borders** refer to the Member States' land borders, including river and lake borders, sea borders and their airports, river ports, sea ports and lake ports, that are not internal.

Border crossing points are **crossing points authorised by the competent authorities for the crossing of external borders.** They can be **shared**, when situated either on the territory of a Member State or of a third country, at which **Member State border guards and third-country border guards carry out exit and entry checks one after another in accordance with their national law and pursuant to a bilateral agreement**.

Conversely, **internal borders may be crossed at any point without a border check on persons**, irrespective of their nationality, being carried out (Art 22 SBC). It is only exceptionally, and as *extrema ratio*, when there is a serious threat to public policy or internal security in a Member State, that Member State may exceptionally reintroduce border control at all or specific parts of its internal borders for a limited period of up to 30 days or for the foreseeable duration of the serious threat if its duration exceeds 30 days (Art. 25 SBC). The Schengen borders code indeed explicitly provides for the absence of border control of persons crossing the internal borders between the Member States of the Union and lays down rules governing border control of persons crossing the external borders of the Member States of the Union.

In the light of the above, it is possible infer that the "no-gate crossing point" solutions for which PERSONA will develop a tailored impact assessment method will be normally employed only at the external borders of the Union, except in those exceptional cases where internal borders control are temporarily reintroduced or have not been lifted yet.

[204] OJ L 135, 24.5.2016, p. 53–114.
[205] OJ L 295, 21.11.2018, p. 138–183.
[206] OJ L 248, 18.9.2013, p. 1–22.

Then, there is a difference between border controls and border checks. **Border control** is the activity carried out at a border, in accordance with and for the purposes of this Regulation, in response exclusively to an intention to cross or the act of crossing that border, regardless of any other consideration, consisting of border checks and border surveillance. Therefore, border control is the umbrella term encompassing border checks and surveillance.

Border checks are the checks carried out at border crossing points, to ensure that persons, including their means of transport and the objects in their possession, may be authorised to enter the territory of the Member States or authorised to leave it.

Finally, **border surveillance** refers to the activity of surveillance of borders between border crossing points and the surveillance of border crossing points outside the fixed opening hours, in order to prevent persons from circumventing border checks. Its goals are to prevent unauthorised border crossings, to counter cross-border criminality and to take measures against persons who have crossed the border illegally.

No-gate crossing point solutions may therefore serve either border checks and border surveillance purposes.

Functional requirements: border management practices
External borders may be crossed only at border crossing points and during the fixed opening hours [*even if derogations are possible*] and Member States shall introduce penalties, in accordance with their national law, for the unauthorised crossing of external borders at places other than border crossing points or at times other than the fixed opening hours. (Art. 5 SBC)
Border guards shall, in the performance of their duties, fully respect human dignity, in particular in cases involving vulnerable persons. Any measures taken in the performance of their duties shall be proportionate to the objectives pursued by such measures. While carrying out border checks, border guards shall not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation (Art. 7 SBC)
Exceptionally, on entry and on exit, **as to persons enjoying the right of free movement under Union law**,[207] in case the checks against the SIS, the other EU databases, the Interpol databases [including the Stolen and Lost Travel Document (SLTD)] and the national databases would have disproportionate impact on the flow of traffic, Member States may decide to carry out those checks on a targeted basis at specified border crossing points, following an assessment of the risks related to the public policy, internal security, public health or international relations of any of the Member States. For passenger data received in accordance with Directive 2004/82/EC[208] or other EU/national law, checks against databases may be carried out in advance. Where those checks are carried out in advance on the basis of such passenger data, the data received in advance shall be checked at the border crossing point against the data in the travel document. The identity and the nationality of the person concerned, as well as the authenticity and validity of the travel document for crossing the border, shall also be verified (Art. 8 SBC)
On entry and on exit, **third-country nationals** shall be subject to thorough checks against the SIS, the VIS the other EU databases, the Interpol databases (including the SLTD) and the national

[207] I.e. Union citizens, third-country nationals who are members of the family of a Union citizen exercising his or her right to free movement to whom Directive 2004/38/EC applies; third-country nationals and their family members, whatever their nationality, who, under agreements between the Union and its Member States, on the one hand, and those third countries, on the other hand, enjoy rights of free movement equivalent to those of Union citizens (Art. 2 SBC).
[208] Council Directive on the obligation of carriers to communicate passenger data.

databases. For passenger data received in accordance with Directive 2004/82/EC[209] or other EU/national law, checks against databases may be carried out in advance. Where those checks are carried out in advance on the basis of such passenger data, the data received in advance shall be checked at the border crossing point against the data in the travel document. The identity and the nationality of the person concerned, as well as the authenticity and validity of the travel document for crossing the border, shall also be verified (Art. 8 SBC)
Border checks at external borders may be relaxed as a result of exceptional and unforeseen circumstances, as those where unforeseeable events lead to traffic of such intensity that the waiting time at the border crossing point becomes excessive, and all resources have been exhausted as regards staff, facilities and organisation (Art. 9 SBC)
Member States shall provide separate lanes, in particular at air border crossing points (but they may also provide separate lanes for sea and land border crossing points) in order to carry out checks on persons. Lanes differentiate among travelers enjoying the right of free movement, visa exempted and all passports (Art. 10 SBC)
Travel documents of third-country nationals shall be systematically stamped on entry and exit, except for certain categories of travelers (e.g. Head of States and dignitaries officially announced, pilots, seamen… etc.) and when, exceptionally, the third-country national requires so if insertion might cause serious difficulties for that person (Art. 11 SBC)
Surveillance shall be carried out by stationary or mobile units which perform their duties by patrolling or stationing themselves at places known or perceived to be sensitive, the aim of such surveillance being to apprehend individuals crossing the border illegally. Surveillance may also be carried out by technical means, including electronic means (Art. 13 SBC)
Member States shall deploy appropriate staff and resources in sufficient numbers to carry out border control at the external borders in such a way as to ensure an efficient, high and uniform level of control at their external borders.
When, exceptionally, internal border controls are temporarily reintroduced, the Commission and the Member State concerned shall inform the public in a coordinated manner on the decision, in particular the start and end date of such a measure, unless there are overriding security reasons for not doing so (Art. 34). At the request of the Member State concerned, the other Member States, the European Parliament and the Commission shall respect the confidentiality of information supplied in connection with the reintroduction and prolongation of border control (Art. 35)
As a general rule, **persons travelling in vehicles** may remain inside them during checks. However, if circumstances so require, persons may be requested to alight from their vehicles. Thorough checks will be carried out, if local circumstances allow, in areas designated for that purpose. In the interests of staff safety, checks will be carried out, where possible, by two border guards (Annex VI SBC)
The competent authorities of the Member States shall ensure that the airport operator takes the requisite measures to **physically separate the flows of passengers on internal flights from the flows of passengers on other flights**. Appropriate infrastructures shall be set in place at all international airports to that end (Annex VI SBC)
Border checks will normally not be carried out on the aircraft or at the gate, unless it is justified on the basis of an assessment of the risks related to internal security and illegal immigration. Checks will normally not be carried out in the transit area, unless it is justified on the basis of an assessment of the risks related to internal security and illegal immigration; in particular checks in this area may

[209] Council Directive on the obligation of carriers to communicate passenger data.

be carried out on persons subject to an airport transit visa in order to check that they are in possession of such a visa (Annex VI SBC)
Functional requirements when EES will be operable [amendments to SBC introduced by Regulation 2017/2225][210]
If the travel document contains an electronic storage medium (chip), the authenticity and integrity of the chip data shall be confirmed using the complete valid certificate chain, unless this is technically impossible or, in the case of a travel document issued by a third country, impossible due to the unavailability of valid certificates (Art. 8 SBC)
On entry/exit, with the exception of third-country nationals for whom an individual file is already registered in the EES, where the travel document contains a facial image recorded in the electronic storage medium (chip) and that facial image can be technically accessed, this verification shall include the verification of that facial image, by comparing electronically that facial image with the live facial image of the third-country national concerned. If technically and legally possible, this verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip) (Art. 8 SBC)
Separate lanes for automated border control for EU/EEA/CH citizens, for third-country nationals, for all passports, for registered travellers (Annex III)
Persons whose border crossing is subject to a registration in the EES **may use self-service systems for the purpose of pre-enrolling** in the EES, provided that all of the following conditions are fulfilled: (a) the travel document contains an electronic storage medium (chip) and the authenticity and integrity of the chip data are confirmed using the complete valid certificate chain; (b) the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document by comparing the facial image recorded in the electronic storage medium (chip) with his or her live facial image; if technically and legally possible, this verification may be done by verifying the live fingerprints against the fingerprints recorded in the electronic storage medium (chip) of the travel document. (Art. 8a SBC)
Persons whose border crossing is subject to a registration in the EES **may be permitted to use a self-service system for the carrying out of their border checks**, where all of the following conditions are fulfilled: (a) the travel document contains an electronic storage medium (chip) and the authenticity and integrity of the chip data are confirmed using the complete valid certificate chain; (b) the travel document contains a facial image recorded in the electronic storage medium (chip) which can be technically accessed by the self-service system so as to verify the identity of the holder of the travel document, by comparing that facial image with his or her live facial image; and (c) the person is already enrolled or pre-enrolled in the EES (Art. 8 b SBC)
On entry and exit, the **results of the border checks carried out through the self-service system shall be made available to a border guard**. That border guard shall monitor the results of border checks and, taking into account those results, authorise the entry or exit or, otherwise, refer the person to a border guard who shall proceed with further checks. There are situations where it is mandatory to refer the person to a border guard (e.g. in case of doubts, if entry conditions are not met, in absence of e-gate…) but, in any case, the border guard supervising the border crossing may decide, based on other reasons, to refer the person using the self-service system to a border guard (Art. 8b SBC)
Persons whose border crossing is subject to a registration in the EES and who **used a self-service system for the carrying out of their border checks may be authorised to use an e-gate**. Where an

[210] See also (Working Group on ICT Solutions for External Borders (sea/land), 2019).

e-gate is used, the corresponding registration of the entry/exit record and the linking of that record to the corresponding individual file shall be carried out when crossing the border through the e-gate. Where the e-gate and the self-service system are physically separated, a verification of the identity of the user shall take place at the e-gate in order to verify that the person using the e-gate corresponds to the person who used the self-service system. The verification shall be carried out by using at least one biometric identifier (Art. 8b SBC)
Member States **are free to allow for the use of self-service systems, e-gates, or both, for border crossings by Union citizens, by citizens of a European Free Trade Association State of the European Economic Area, by citizens of Switzerland and by third-country nationals whose border crossing is not subject to a registration in the EES.** (Art. 8b SBC)
Automated border control systems shall, to the extent possible, be designed in such a way that they can be used by all persons, with the exception of children under 12 years of age. They shall also be designed in a way that fully respects human dignity, in particular in cases involving vulnerable persons. Where Member States decide to use automated border control systems, they shall ensure the presence of a sufficient number of staff to assist persons with the use of such systems. (Art. 8c)
When a third-country national benefits from the national facilitation programme, border guards may carry out the verification without comparing biometrics electronically but by comparing the facial image taken from the electronic storage medium (chip) and the facial image in the third-country national's individual EES file with that third-country national's face. Full verification shall be carried out at random and on the basis of a risk analysis.
For the sole purpose of verifying the identity of the visa holders, the authenticity, temporal and territorial validity and status of the visa or whether the conditions for entry to the territory of the Member States are fulfilled, or both, the competent authorities for carrying out checks at borders at which the EES is operated shall have access to the VIS (Art. 18 VIS Regulation)
Member State which does not yet apply the Schengen acquis in full but operates the EES shall introduce the EES without biometric functionalities at its internal land borders with a Member State which does not yet apply the Schengen acquis in full but operates the EES. Where, at those internal borders, a third-country national has not yet been registered in the EES, that third-country national's individual file shall be created without recording biometric data. Biometric data shall be added at the next border crossing point where the EES is operated with biometric functionalities (Art. 4 EES Regulation)

8.4 Technical and security requirements related to the databases

Technical and security measures	**Legal instruments**
Obligations of eu-LISA	
Adopt technical solutions to ensure **uninterrupted functioning and availability** of SIS, VIS, Eurodac, EES	See data-base related legal framework
Preparation, development and operational management of large-scale IT databases in the area of freedom, security and justice	Art. 9 eu-LISA Regulation
In respect to data security, adoption of a **security plan and a business continuity and disaster recovery plan**, with the possibility of recovering data, for SIS, VIS, Eurodac, EES, ECRIS-TCN, ETIAS (for ETIAS Central Unit, it will be up to Frontex)	See data-base related legal framework

Managing the **encrypted communication infrastructures** of the databases (except those with EuroDomain)	See data-base related legal framework
Keeps **logs and records of data processing operations**	See data-base related legal framework
Monitoring of the databases	See data-base related legal framework
Obligations on the side of Member States authorities	
Each Member State shall be responsible for setting up, operating, maintaining and further developing its national systems and connecting it to national interfaces. Each Member State shall be responsible for ensuring the **uninterrupted availability** of data to end-users.	See data-base related framework
In respect to data security, the adoption of a security plan and a **business continuity and disaster recovery plan** to ensure security before and during the transmission to and receipt from their national systems (for SIS, VIS, Eurodac, EES, ECRIS-TCN, ETIAS)	See data-base related framework[211]
Encryption of the Communication Infrastructures	See data-base related legal framework
Keep **logs and records of data processing operations**	See data-base related framework

[211] For example, in the case of SIS, the measures for the plan shall be aimed at (a) physically protect data, including by making contingency plans for the protection of critical infrastructure; (b) deny unauthorised persons access to data-processing facilities used for processing personal data (facilities access control); (c) prevent the unauthorised reading, copying, modification or removal of data media (data media control); (d) prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control); (e) prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control); (f) prevent the unauthorised processing of data in SIS and any unauthorised modification or erasure of data processed in SIS (control of data entry); (g) ensure that persons authorised to use an automated data-processing system have access only to the data covered by their access authorisation, by means of individual and unique user identifiers and confidential access modes only (data access control); (h) ensure that all authorities with a right of access to SIS or to the data processing facilities create profiles describing the functions and responsibilities of persons who are authorised to access, enter, update, delete and search the data and make those profiles available to the supervisory authorities referred to in Article 55(1) without delay upon their request (personnel profiles); (i) ensure that it is possible to verify and establish to which bodies personal data may be transmitted using data communication equipment (communication control); (j) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data-processing systems, when, by whom and for what purpose (input control); (k) prevent the unauthorised reading, copying, modification or deletion of personal data during the transmission of personal data or during the transport of data media, in particular by means of appropriate encryption techniques (transport control); (l) monitor the effectiveness of the security measures referred to in this paragraph and take the necessary organisational measures related to internal monitoring to ensure compliance with this Regulation (self-auditing); (m) ensure that, in the event of interruption, installed systems can be restored to normal operation (recovery); and (n) ensure that SIS performs its functions correctly, that faults are reported (reliability). (Art. 10 Regulation 1861/2018).
Each plan for the other databases follows a similar structure.

Application of **professional secrecy** (or equivalent) rules to all persons and bodies required to work with databases	See data-base related framework
Compliance with Commission's **common standards**, **protocols and technical procedures** to ensure the **compatibility of N.SIS with Central SIS** for the prompt and effective transmission of data. (see forthcoming implementing acts)	Art. 9(1)-(5) Regulation (EU) 2018/1861
Compliance with Commission's **technical requirements for the Communication Infrastructure**. (see forthcoming implementing acts)	Art. 15(7) Regulation (EU) 2018/1861
Compliance with Commission's **technical rules necessary for entering, updating, deleting and searching the data[212] and the common standards**. (see forthcoming implementing acts)	Art. 20(3) Regulation (EU) 2018/1861
Similarity of technical rules for searches in CS-SIS, in national or shared copies and in technical copies.	Art. 20(4) Regulation (EU) 2018/1861
Management of security incidents[213] ensuring quick, effective and prompt response.	SIS, EES, Eurodac, Interoperability
SIRENE Bureaux shall use an **encrypted virtual network** exclusively dedicated to SIS II data and the exchange of supplementary information	1.10.3**.** SIRENE Manual
Compliance with Commission's **technical rules necessary for entering and further processing the data for the purpose of dealing with misused identities**.[214] (see forthcoming implementing acts)	Art. 47(4) Regulation (EU) 2018/1861

[212] Art. 20(2) Regulation 2018/1861 "Any alert in SIS which includes information on persons shall contain only the following data: (a) surnames; (b) forenames; (c) names at birth; (d) previously used names and aliases; (e) any specific, objective, physical characteristics not subject to change; (f) place of birth; (g) date of birth; (h) gender; (i) any nationalities held; (j) whether the person concerned: (i) is armed; (ii) is violent; (iii) has absconded or escaped; (iv) poses a risk of suicide; (v) poses a threat to public health; or (vi) is involved in an activity referred to in Articles 3 to 14 of Directive (EU) 2017/541; (k) the reason for the alert; (l) the authority which created the alert; (m) a reference to the decision giving rise to the alert; (n) the action to be taken in the case of a hit; (o) links to other alerts pursuant to Article 48; (p) whether the person concerned is a family member of a citizen of the Union or other person who is a beneficiary of the right of free movement as referred to in Article 26; (q) whether the decision for refusal of entry and stay is based on: (i) a previous conviction as referred to in point (a) of Article 24(2); (ii) a serious security threat as referred to in point (b) of Article 24(2); (iii) circumvention of Union or national law on entry and stay as referred to in point (c) of Article 24(2); (iv) an entry ban as referred to in point (b) of Article 24(1); or (v) a restrictive measure referred to in Article 25; (r) the type of offence; (s) the category of the person's identification documents; (t) the country of issue of the person's identification documents; (u) the number(s) of the person's identification documents; (v) the date of issue of the person's identification documents; (w) photographs and facial images; (x) dactyloscopic data; (y) a copy of the identification documents, in colour wherever possible.

[213] I.e. events that have or may have an impact on the security of SIS or may cause damage or loss to SIS data or to the supplementary information (e.g. unlawful access to data, compromise of availability, integrity and confidentiality of data) [Art. 45 Regulation (EU) 2018/1861].

[214] Art. 47(3) "For the purpose of this Article, and subject to the explicit consent of the person whose identity has been misused for each data category, only the following personal data of the person whose identity has been misused may be entered and further processed in SIS: (a) surnames; (b) forenames; (c) names at birth; (d) previously used names and any aliases possibly entered separately; (e) any specific objective and physical characteristic not subject to change; (f) place of birth; (g) date of birth; (h) gender; (i) photographs and facial

Compliance with Commission's **technical rules for linking alerts**. (see forthcoming implementing acts)	Art. 48(6) Regulation (EU) 2018/1861
Rules on biometric data	
Compliance with Commission's **minimum data quality standards and technical specifications for searches with biometric data**. (see forthcoming implementing acts and current **Commission Implementing Decision (EU) 2016/1345**)	Art. 32(4) Regulation (EU) 2018/1861

images; (j) fingerprints, palm prints or both; (k) any nationalities held; (l) the category of the person's identification documents; (m) the country of issue of the person's identification documents; (n) the number(s) of the person's identification documents; (o) the date of issue of a person's identification documents; (p) address of the person; (q) person's father's name; (r) person's mother's name.

Fingerprints standards ▪ fingerprint images' input format and accompanying alphanumeric data shall be **compliant with ANSI/NIST** (American National Standard for Information Systems / National Institute of Standards and Technology) **binary format**. ▪ **compatibility and interoperability of CS-SIS AFIS with data captured using live-scan devices at the national level** capable of capturing and segmenting up to 10 individual fingerprints, or 'inked' fingerprints (then digitally scanned); rolled, flat or both. ▪ CS-SIS shall receive fingerprint images of a **nominal resolution of either 1 000 dpi** [to be sent in JPEG2000 (JP2)] or of **500 dpi with 256 grey levels** (to be sent in WSQ format). ▪ Fingerprint images that do not meet the quality threshold determined by the CS-SIS AFIS shall not be inserted for automated searching, but shall be stored in SIS to confirm the identity of a person and may be stored and inserted when they concern missing persons ▪ **compliance with eu-LISA tool** for checking quality ▪ CS-SIS AFIS shall insert into the biometric database fingerprint images above the quality threshold with at most one image per finger type (NIST identification 1 to 10), i.e. 1 to 10 flat prints and 1 to 10 rolled fingerprints, each of them correctly labelled as to which finger it relates, identifying also missing or bandaged fingerprints/partial (low quality). ▪ CS-SIS AFIS shall perform biometric searches (biometric identifications) using the fingerprint images above the quality threshold and with at most one image per finger type (NIST identification 1 to 10). Each fingerprint image shall be correctly labelled as to which finger it relates. Missing or bandaged fingerprints shall always be identified accordingly as specified by the SIS II ICD in compliance with the NIST standard. ▪ CS-SIS AFIS shall be able to perform biometric verifications with any number of flat or rolled fingerprints between 1 and 10. Each NIST file shall contain at most one image per finger type (NIST identification 1 to 10). The use of 'permutations' (Permutations instruct CS-SIS AFIS to perform repetitive verification between the source fingerprint(s) and all candidate fingerprints available (mostly 10) until either a positive verification takes place or all candidate fingerprints have been searched without producing a positive verification.) shall be performed for verifications by CS-SIS AFIS regardless of the fingerprint labelling. Missing or bandaged fingerprints shall always be identified accordingly as specified by the SIS II ICD in compliance with the NIST standard.	Annex Commission Implementing Decision (EU) 2016/1345
Photographs standards for SIRENE bureaux (for photographs that shall only be used to confirm the identity of a person who has been located as a result of an alphanumeric search made in SIS II): ▪ **full frontal face** pictures aspect rate 3:4 or 4:5 (as far as possible); ▪ **resolution** of at least **480 × 600 pixels with 24 bits of colour depth** (when available) ▪ when the image is acquired through a scanner, the **image size less than about 200 Kbytes** (as far as possible)	2.14.4 Sirene Manual

Fingerprints data and related NIST file for SIRENE Bureaux shall be compatible in all respects with the provisions of **Commission Implementing Decision (EU) 2016/1345** on minimum data quality standards for fingerprint records within the second generation Schengen Information System (SIS II), the annex thereto and technical standards adopted in the Committee referred to in Article 51 of the SIS II Regulation and Article 67 of the SIS II Decision	2.14.3. SIRENE Manual
High degree of reliability of identification when photographs and facial images are used to identify a person in the context of regular border crossing points.[215]	Art. 33(4) Regulation (EU) 2018/1861
The technical requirements for the photograph shall be in accordance with the international standards as set out in the International Civil Aviation Organization (ICAO) document 9303 Part 1, 6th edition. Fingerprints shall be taken in accordance with ICAO standards and Commission Decision 2006/648/EC of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System	Visa code
Input format of alphanumeric data and fingerprint images is compliant with the ANSI/NIST-ITL 1 — 2000 specified format. Minimum acceptable resolution is 500 dpi with 256 grey levels.	Annex Commission Decision 2006/648/EC
Passport stamps shall comply with Schengen Executive Committee Decision SCH/COM-EX (94) 16 rev and SCH/Gem-Handb (93) 15 (CONFIDENTIAL)	Annex IV Schengen Borders Code
CS-EES shall store the live facial image captured at the border crossing point and submitted as part of a NIST container to the CS-EES as specified by the ANSI/NIST-ITL 1-2011: Update 2015 standard (or newer version).	EES Implementing decision 2019/329
Fingerprint data with a resolution of 500 ppi shall be compressed using the WSQ algorithm (ISO/IEC 19794) while 1 000 ppi fingerprint data shall use the JPEG 2000 image compression standard (ISO/IEC 15444-1) and coding system. The target compression ratio is 15:1.	EES Implementing decision 2019/329
Data format for the exchange of fingerprint data ANSI/NIST-ITL 1a-1997, Ver.3, June 2001 (INT-1) and any future further developments of this standard.	Eurodac Regulation

8.5 Sum up of legal requirements

To sum up, the requirements of the legal benchmark may be summarised in 4 main categories:

- Fundamental rights
- Compliance with data protection rules
- Compliance with technical and security provisions

[215] After the start of the use of the functionality at regular border crossing points, the Commission shall be empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation concerning the determination of other circumstances in which photographs and facial images may be used to identify persons. [Art. 33(4)]

- Compliance with border management practices

Id	*Description*
Respect of fundamental rights	
LR 1	Respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities: providing that those are the value common to member states, on which the EU is founded, no gate crossing point solutions shall aim at them
LR 2	AFSJ where the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime: no gate crossing point solutions should be aimed at these multiple goals
LR 3	Human dignity: no-gate crossing point solutions shall respect human dignity
LR 4	Right to integrity: no-gate crossing point solutions shall safeguard the integrity of a person
LR 5	Prohibition of inhuman and degrading treatment: the use of no-gate crossing point solutions shall not constitute inhuman and degrading treatment
LR 6	Non-discrimination: no-gate crossing point solutions shall not discriminate people who opt for not using them
LR 7	Non-discrimination: no-gate crossing point solutions shall not discriminate among different users on ground of e.g. ethnicity, gender, religion …
LR 8	Right to asylum: no-gate crossing point solutions shall not hamper the right to asylum
LR 9	Non-refoulement: no-gate crossing point solutions shall not prejudice the principle of non-refoulement
LR 10	Rights of children: no-gate crossing point solutions shall be designed to protect the rights of children
LR 11	Rights of elderly: no-gate crossing point solutions shall be designed to protect the rights of elderly
LR 12	Right of people with disabilities: no-gate crossing point solutions shall be aimed at integrating people with disabilities
LR 13	Privacy: no-gate crossing point solutions shall respect the right to privacy
LR 14	Data protection: no-gate crossing point solutions shall respect the right to data protection
LR 15	Restrictions of fundamental rights: if the no-gate crossing point solution is restricting fundamental rights, then it must be i) provided by law, ii) respect the essence of the right, iii) necessary and proportionate and iv) meets objectives of general interest of the Union or the need to protect the rights and freedoms of others
Compliance with data protection rule	
LR 16	Lawful processing: when the no gate crossing point solution is processing personal data, there shall be a legal basis for data processing
LR 17	Purpose limitation: data collected by the no gate crossing point solution shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purpose

LR 18	Data minimisation: data collected by the no gate crossing point solution shall be adequate, relevant and not excessive in relation to the purposes for which they are processed
LR 19	Accuracy: data processed by the no-gate crossing point solution shall be accurate and when 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
LR 20	Storage limitation: the no-gate crossing point solution shall keep data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed
LR 21	Integrity and confidentiality: the no-gate crossing point solution shall process personal data 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
LR 22	Accountability: meaning that data controller shall be responsible for, and be able to demonstrate compliance with data protection principles
LR 23	Right to information: data subjects shall be informed about which person data the no-gate crossing point solution is collecting about them, their data subjects' rights, purposes and legal basis etc. (unless there are restrictions provided for by the law)
LR 24	Right to access (also indirect), rectification, erasure and restriction of processing: the no-gate crossing point solution shall grant data subjects rights (unless there are restrictions provided for by the law)
LR 25	Right of the data subject not to be subject to a decision based solely on automated processing that significantly affects him or her: no-gate crossing point solutions shall provide for human intervention
LR 26	Data transfers: in principle transfers of data collected by the no-gate crossing point solutions shall be restricted
LR 27	Accessibility of data in EU large database: in case the no-gate crossing point solution is connected with EU large scale databases, it shall be kept in mind that only certain EU/national authorities can have access to certain categories of data for the performance of their tasks
LR 28	Data protection impact assessment: whereas the no-gate crossing point solutions are performing data processing operations likely to result in a high risk to the rights and freedoms of individuals, in particular using new technologies, a DPIA is required (See D. 3.1)
LR 29	Logs and records of data processing operations: whereas the no gate-crossing point solution is connected to a EU large scale database, logs and records of data processing operations shall be kept
Compliance with technical and security provisions	
LR 29	Features of biometric data: no gate crossing point solutions should be capable to read data in the technical format foreseen for photographs/facial images/dactyloscopic data in documents and databases
LR 30	Common standards, protocols and technical procedures: no gate crossing point solutions when connected to EU large scale database, should comply with common standards, protocols and technical procedures as foreseen in Commission implementing decisions to ensure prompt data transfer and interoperability

LR 31	Dual use items: in case the no gate crossing point solution is classified as dual use item, in particular under Annex IV, even their intra EU-trade is subject to prior authorisation.
LR 32	Dual use items: even if goods are not listed as dual use, EU countries may still put extra controls for public security or human rights considerations
LR 33	Unmanned aircraft systems: in case the no gate crossing point solution is a UAV, border control authorities shall cooperate on safety matters with authorities ex Art. 17 Implementing Regulation (EU) 2019/947.
LR 34	Uninterrupted availability: when the no-gate crossing point solution is linked to EU large scale database, it shall ensure uninterrupted availability of data to end-users
LR 35	Management of security incidents: when the no-gate crossing point solution is linked to EU large scale database, the management of security incidents shall ensure quick, effective and prompt response
LR 36	Security and a business continuity and disaster recovery plan: they shall be in place when the no-gate crossing point solution is linked to EU large scale database
LR 37	Encryption of the communication network connecting no-gate crossing point solution and the EU large scale database
LR 38	The no gate crossing point solution shall comply with technical rules and common standards necessary for entering, updating, deleting and searching the data in EU large scale database
Compliance with border management practices	
LR 39	Opening hours and border crossing points: providing that external borders may be crossed only at certain hours at border crossing points, it shall be made clear where a no gate crossing point solution is located and when it can be employed to cross a border. No gate crossing points solutions may be used to increase the number of border crossing points and maintain them open 24/7 (albeit it must be kept in mind that border guards shall still be present) and therefore reduce the hypothesis of unauthorised crossing.
LR 40	Human right oriented design: No gate crossing point solutions shall be developed in a way to fully respect human dignity, in particular in cases involving vulnerable persons, be proportionate and not discriminate against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation
LR 41	Identity and nationality of person concerned: the no-gate crossing point solution shall be capable to verify them
LR 42	Authenticity and validity of the travel document for crossing the border: the no-gate crossing point solution shall be capable to verify them
LR 43	Different lanes to differentiate among travelers enjoying the right of free movement, visa exempted and all passports: different no-gate crossing point solutions may be applied to the different passengers
LR 44	Surveillance via technical means: no-gate crossing point solutions may be used for surveillance purposes
LR 45	Staff and resources: the employment of no-gate crossing point solutions shall not be seen as a waiver to deploy appropriate staff and resources to ensure an efficient, high and uniform level of control at their external borders.
LR 46	Reintroduction of internal border controls: the employment of no gate-crossing point solutions shall not waiver to the duty to inform the public

LR 47	Checks on vehicles: the no-gate crossing point solutions should enable people to remain inside the car during the check
LR 48	Checks in the airport: the no-gate crossing point solutions should not be carried on the aircraft or at the gate, nor in the transit area
LR 49	Checks in the airport: the no-gate crossing point solutions shall not regard passengers of internal flights
LR 50	Travel document containing chip with facial images: the verification shall include the verification of that facial image, by comparing electronically that facial image with the live facial image of the third-country national concerned. The no gate crossing point solution shall be able to do this verification.
LR 51	Travel document containing chip with facial images: if technically and legally possible, fingerprints may be used for the verification.
LR 52	Self-service system for pre-enrolling and border check: their use shall not be mandatory
LR 53	Self-service systems and e-gates may be used also by EU citizens by citizens of a European Free Trade Association State of the European Economic Area, by citizens of Switzerland and by third-country nationals whose border crossing is not subject to a registration in the EES: in this case, it shall not be considered a border check.
LR 54	Automated border control systems: shall, to the extent possible, be designed in such a way that they can be used by all persons, with the exception of children under 12 years of age.

10 Concluding remarks

To conclude, this deliverable provided a benchmark to be used to develop, and possibly conduct, the process of impact assessment tailored down to borderless crossing technologies (D3.1/D3.2). More concretely, Chapter 1 provided a general and terminological introduction to the deliverable. Then, the deliverable presented two parts. The first part (Chapter 2) described the technical requirements of the technologies considered. The second part included constraints on such technical requirements, namely social acceptance (Chapter 3), ethical (Chapter 4) and legal (Chapter 5 and 6) requirements.

The benchmark provided in this deliverable might need to be updated in the next months, especially regarding the legal requirements. If this is needed, an annex will be added to the final version of the impact assessment method (D3.2, due in M24).

The next step is to ensure that the benchmark is internally coherent, i.e. there are no contradictions between its internal components (e.g. technical vs. social acceptance requirements, or ethical vs. border management). This activity is normally carried out during the scoping and/or the appraisal phase of the impact assessment method (cf. D3.1 for further clarification).

11 Bibliography

Adams, D. A., Nelson, R. R., & Todd, P. A. (1992). Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication. *MIS Quarterly*, *16*(2), 227. https://doi.org/10.2307/249577

AI HLEG. (2019). *Building trust in human-centric AI | FUTURIUM | European Commission*. 2–36. Retrieved from https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

Ajana, B. (2010). Recombinant Identities: Biometrics and Narrative Bioethics. *Journal of Bioethical Inquiry*, *7*(2), 237–258. https://doi.org/10.1007/s11673-010-9228-4

Ajzen, I., & Fishbein, M. A. (1975). *Belief, attitude, intention and behaviour: An introduction to theory and research*. Addison-Wesley.

Alnemr, R., Cayirci, E., Corte, L. D., Garaga, A., Leenes, R., Mhungu, R., … Vranaki, A. (2016). A data protection impact assessment methodology for cloud. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9484*, 60–92. https://doi.org/10.1007/978-3-319-31456-3_4

Beauchamp, T. (2015). Common Morality, Human Rights, and Multiculturalism in Japanese and American Bioethics. *Journal of Practical Ethics*, *3*(2), 18–35.

Beauchamp, T. L., & Childress, J. F. (2001). *Principles of Biomedical Ethics*. Oxford University Press.

Berlin, I. (2017). Two Concepts of Liberty. In *The Liberty Reader* (pp. 33–57). https://doi.org/10.4324/9781315091822-3

Blanke, H.-J., & Mangiameli, S. (Eds.). (2013). *The Treaty on European Union (TEU)*. https://doi.org/10.1007/978-3-642-31706-4

Brey, P. (2017). Ethics of Emerging Technology. *The Ethics of Technology Methods and Approaches*.

Castells, M. (1996). *The Rise of the Network Society, The Information Age: Economy, Society and Culture*. Blackwell.

Coeckelbergh, M. (2012). Care robots, virtual virtue, and the best possible life. *The Good Life in a Technological Age*, pp. 281–292. https://doi.org/10.4324/9780203124581

Compeau, D. R., & Higgins, C. A. (1995). Application of Social Cognitive Theory to Training for Computer Skills. *Information Systems Research*, *6*(2), 118–143. https://doi.org/10.1287/isre.6.2.118

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

De Hert, P., & Gutwirth, S. (2006). Interoperability of police databases within the EU: An accountable political choice? *International Review of Law, Computers & Technology*, *20*(1–2), 21–35. https://doi.org/10.1080/13600860600818227

Dittrich, D., & Kenneally, E. (2012). *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*.

Dratwa, J. (2014). *Ethics of security and surveillance technologies*. Publications Office of the European Union.

Engström, V., & Heikkilä, M. (2014). *Fundamental rights in the institutions and instruments of the Area of Freedom, Security and Justice Large-Scale FP7 Collaborative Project Fundamental rights in the institutions and instruments of the Area of Freedom, Security and Justice*. (September). https://doi.org/10.7404/FRAME.REPS.11.1

European Union Agency for Fundamental Rights. (2017). *Fundamental rights and the interoperability of EU information systems: borders and security*. https://doi.org/10.2811/178106

European Union Agency for Fundamental Rights. (2018). *Under watchful eyes: biometrics, EU IT systems and fundamental rights*. https://doi.org/10.2811/29

European Union Agency For Fundamental Rights (FRA). (2015). *Handbook on European law relating to asylum, borders and immigration | European Union Agency for Fundamental Rights*. https://doi.org/10.2811/37325

European Union Agency for Fundamental Rights, & EDPS. (2018). Handbook on European data protection law

2018. In *Luxembourg: Publications Office of the European Union*. https://doi.org/10.2811/58814

Feil-Seifer, D., & Matarić, M. J. (2011). Ethical Principles for Socially Assistive Robotics. *IEEE Robot Autom Mag*.

Galetta, A., & De Hert, P. (2015). The Proceduralisation of Data Protection Remedies under EU Data Protection Law: Towards a More Effective and Data Subject-oriented Remedial System? *Review of European Administrative Law*, *8*(1), 125–151. https://doi.org/10.7590/187479815X14313382198412

González Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. https://doi.org/10.1007/978-3-319-05023-2

Horton, J. (2002). Principles of biomedical ethics. *Transactions of the Royal Society of Tropical Medicine and Hygiene*, *96*(1), 107. https://doi.org/10.1016/S0035-9203(02)90265-8

Ihde, D. (1990). *Technology and the Lifeworld*.

Kant, I., & Reath, A. (1997). *Immanuel Kant: Critique of Practical Reason* (M. J. Gregor, Ed.). https://doi.org/10.1017/CBO9780511809576

Kloza, D., van Dijk, N., Gellert, R., Böröcz, I., Tanas, A., Mantovani, E., & Quinn, P. (2017). Data Protection Impact Assessments in the European Union: Complementing the New Legal Framework towards a More Robust Protection of Individuals. *D.Pia.Lab Policy Brief, VUB: Brussels*, *1*.

Kuner, C. (2018). A. Court of Justice International agreements, data protection, and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR. *Common Market Law Review*, *55*(3), 857–882.

Latour, B. (1994). On Technical Mediation. *Common Knowledge*, *3*(2), 29–64. Retrieved from http://ecsocman.hse.ru/text/18036068/

Lovink, G. (2016). *Social Media Abyss*. Wiley.

Mader, O. (2019). Enforcement of EU Values as a Political Endeavour: Constitutional Pluralism and Value Homogeneity in Times of Persistent Challenges to the Rule of Law. *Hague Journal on the Rule of Law*, *11*(1), 133–170. https://doi.org/10.1007/s40803-018-00083-x

Malhotra, Y., & Galletta, D. F. (1999). Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation. *HICSS '99. IEEE Computer Society*.

Mill, J. S. (1991). *Collected Works of John Stuart Mill, in 33 vols* (J. M. Robson, Ed.). Retrieved from https://oll.libertyfund.org/titles/165

Mordini, E., & Tzovaras, D. (Eds.). (2012). *Second Generation Biometrics: The Ethical, Legal and Social Context*. https://doi.org/10.1007/978-94-007-3892-8

Nielsen, J. (1994). *Usability Engineering*. Elsevier.

Nozick, R. (1974). *ANARCHY ; ' STATE , AND UTOPIA*.

Palm, E., & Hansson, S. O. (2006). The case for ethical technology assessment (eTA). *Technological Forecasting and Social Change*, *73*(5), 543–558. https://doi.org/10.1016/j.techfore.2005.06.002

Quintel, T. (2018). Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3132506

Rawls, J. (1999). *A Theory of Justice*. Belknap Press.

Robert C. Post. (2001). Three Concepts of Privacy. *Georgetown Law Journal*.

Roeser, S. (2010). *Emotions and Risky Technologies* (S. Roeser, Ed.). https://doi.org/10.1007/978-90-481-8647-1

Sajfert, J., & Quintel, T. (2019). DATA PROTECTION DIRECTIVE (EU) 2016 / 680 FOR POLICE AND CRIMINAL JUSTICE AUTHORITIES. In Cole/Boehm (Ed.), *GDPR Commentary (Forthcoming)* (pp. 1–22). Elgar.

Solove, D. J. (2008). *Understanding privacy*.

Spiekermann, S., & Pallas, F. (2006). Technology paternalism – wider implications of ubiquitous computing. *Poiesis & Praxis*, *4*(1), 6–18. https://doi.org/10.1007/s10202-005-0010-3

Stewart, B. (1996). Privacy impact assessments. *Privacy Law and Policy Reporter*, *3*(4), 61–64.

Taebi, B. (2017). Bridging the Gap between Social Acceptance and Ethical Acceptability. *Risk Analysis*, *37*(10), 1817–1827. https://doi.org/10.1111/risa.12734

US Department of Health Education and Welfare. (1978). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects research: Publication No. (OS) 78-0014*. 1–705. Retrieved from videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_2.pdf

van de Poel Ibo, & Lambèr, R. (2011). *Ethics, Technology, and Engineering: An Introduction*. Wiley and Blackwell.

van Lieshout, M., Friedewald, M., Wright, D., & Gutwirth, S. (2013). Reconciling privacy and security. *Innovation: The European Journal of Social Science Research*, *26*(1–2), 119–132. https://doi.org/10.1080/13511610.2013.723378

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). Venkatesh et al (2003) User acceptance of information technology (1). *MIS Quarterly*, *27*(3), 425–478.

Weiser, M. (1993). Hot topics-ubiquitous computing. *Computer*, *26*(10), 71–72. https://doi.org/10.1109/2.237456

Wickins, J. (2007). The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification. *Science and Engineering Ethics*, *13*(1), 45–54. https://doi.org/10.1007/s11948-007-9003-z

Working Group on ICT Solutions for External Borders (sea/land). (2019). *EES Report*.

Wright, D. (2011). A framework for the ethical impact assessment of information technology. *Ethics and Information Technology*, *13*(3), 199–226. https://doi.org/10.1007/s10676-010-9242-6

Wright, D., & Mordini, E. (2012). Privacy and Ethical Impact Assessment. In *Privacy Impact Assessment* (pp. 397–418). https://doi.org/10.1007/978-94-007-2543-0_19

Annex 1: Legal and regulatory requirements in jurisdictions relevant for PERSONA test studies

Serbia

Serbia applied for the status of candidate country to the European Union in December 2009, status that was granted in March 2012.[216] This means that, to become an actual Member of the European Union, it will have to satisfy the Copenhagen criteria, that include the existence and stability of institutions guaranteeing democracy, the rule of law, human rights and respect for and protection of minorities.[217]

Within the framework of the Council of Europe, Serbia is party of the European Convention on Human Rights and of the Convention 108.

At the moment, in respect of either protection of fundamental rights, democracy, rule of law, on the one hand, and management of asylum, legal and illegal migration, visa policy and external border, the Commission assessed Serbian provisions partially in line with the *acquis* and register improvements comparing with previous years.[218]

In November 2018, it adopted a new Law on Personal Data Protection following closely EU's General Data Protection Regulation (GDPR), albeit adding some elements related to law enforcement.[219]

The main novelties about this law regard: **its scope of application**, providing that the new law has an extraterritorial ambition, i.e. it will not apply only to the processing of data carried out by Serbian controllers and processors, but also by the ones based outside of Serbia whose processing activities relate to the offering of goods or services to or monitoring the behaviour of Serbian data subjects within Serbia. **New forms and stricter requirements of data processing consent**: the new law introduces online consent, oral consent and consent by other clear affirmative action (provided that the controller is able to demonstrate that the data subject has indeed consented), necessary to cope with the digital transformation. Furthermore, the consent must be freely given, specific, informed and unambiguous. **New and expanded data subjects' rights,** that include the right to receive transparent information about the processing, to access to personal data, to withdraw consent, to be informed about data retention, to data portability, to erasure. Stronger **accountability**, **data security**, **privacy by design & by default** and the obligation to conduct a **data protection impact assessment** for processing operations which are considered more of risk to the rights and freedoms of individuals. A more **liberalised data transfer regime**, providing that controllers will be entitled to transfer personal data abroad if one of the following conditions (amongst others) is met: personal data is to be transferred to a country that ratified the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data; data transfers are performed to a country included on the EU list or the Serbian Government's list of countries providing an adequate level of data protection; data transfers are performed to a country which has a bilateral agreement with Serbia regulating data transfers;

[216] https://ec.europa.eu/environment/enlarg/candidates.htm
[217] https://ec.europa.eu/neighbourhood-enlargement/policy/glossary/terms/accession-criteria_en9
[218] Commission SWD(2018) 152 final, 2018 Serbia report (Strasbourg, 17.4.2018)
[219] https://edri.org/will-serbia-adjust-its-data-protection-framework-to-gdpr, accessed 12 August 2019

the transfer is based on the standard contractual clauses prepared by the Serbian DPA etc. The **obligation to notify data breaches**. **Sanctions**, even if lower than under GDPR.[220]

As provided into the Information Booklet for 2019 of the Commissioner for Information of Public Importance and Personal Data Protection (Serbian DPA), here are examples of data protection related legislation:

- The Commissioner's powers are specified by provisions of the Law on Free Access to Information of Public Importance ("Official Gazette of the Republic of Serbia", Nos. 120/04, 54/07, 104/09 and 36/10), the Law on Personal Data Protection (Official Gazette of the Republic of Serbia" Nos. 97/2008 and 104/2009 – new law, 68/12 – Decision of the Constitutional Court and 107/12) and the Law on General Administrative Proceedings ("Official Gazette of the Federal Republic of Yugoslavia", Nos. 33/97 and 31/01 and the „Official Gazette of the Republic of Serbia", No. 30/10).
- The Decree on the Form and the Manner of Keeping Records of Personal Data Processing ("Official Gazette of the Republic of Serbia", No. 50/09 of 10 July 2009). This regulation has been enacted by the Serbian Government.
- The Bylaw on the Official Identification Form of Persons Authorized for Inspection under the Law on Personal Data Protection ("Official Gazette of the Republic of Serbia", No. 35/09 of 12 May 2009). This regulation has been enacted by the Commissioner.
- The Bylaw on the Manner of Prior Verification of Personal Data Processing Actions ("Official Gazette of the Republic of Serbia", No. 35/09 of 12 May 2009). This regulation has been enacted by the Commissioner.
- The Data on Confidentiality Law ("Official Gazette of the Republic of Serbia", No. 104/09)

Also as regards border management, Serbia is adopting an Integrated Border Management Strategy aimed at bringing it in line with EU Standards. In February 2018, two financial agreements were signed by EU and Serbia to enhance EU support to Migration and Efficient Border Management in Serbia during the migration crisis.[221]

The operations of border services are specified by legal and sub-legal enactments regulating activities and responsibilities of border services, as well as rights and obligations of citizens in relation to crossing a state border, flow of goods and persons. Part of this matter is also settled by bi-lateral and multilateral agreements disciplining different fields (e.g. all forms of international traffic, visa régime, customs conventions, foreign trade, quarantine and plant and animal protection…). In internal legislature, some border services still apply certain laws and sub-law decrees adopted in the times of former Socialist Federal Republic of Yugoslavia, other than international agreements, which are outdated and inapplicable under the new social and economic circumstances.[222]

For a complete overview of Serbian border management instruments, see Annex III of the Integrated Border Management STRATEGY in the Republic of Serbia

[220] https://www.karanovicpartners.com/news/new-data-protection-law-serbia/ and https://eurocloud.org/news/article/serbia-new-law-on-personal-data-protection/
[221] https://europa.rs/eu-enhances-its-support-to-migration-and-efficient-border-management-in-serbia/?lang=en
[222] https://www.srbija.gov.rs/uploads/documents/strategy_border.pdf

Israel

As regards the protection of fundamental rights, Israel is signatory of several International Conventions, the International Covenant on Civil and Political Rights (ICCPR), the Convention on the Rights of the Child (CRC), Convention Relating to the Status of Refugees, Convention Relating to the status of Stateless Persons, Protocol Relating to the Status of Refugees.[223] Albeit it is not Member of the Council of Europe, still the Knesset (i.e. Israeli Parliament) was granted observer status with the Parliamentary Assembly on 2 December 1957.[224] Counterterrorism action plans are in place between EU and Israel.[225]

Privacy is a constitutional right in Israeli fundamental law. As regards data protection, in certain aspect, obligations under Israeli law exceed GDPR requirements and therefore companies that adopt a comprehensive GDPR compliance programme may still take additional actions to be fully compliant with Israeli law. For example, as regards **data security**, whereas the GDPR requires controllers and processors to take appropriate technical and organisational measures to ensure the level of security that is appropriate to the level of the risk, the Israeli Data Security Regulations impose more specific and granular requirements with respect to personal data collected and maintained in databases (e.g. detailed requirements for controlling, monitoring and recording database access, specific requirements and timeframes for performing PEN testing and rotating passwords); as to **data export**, under Israeli law, in addition to the exporter and importer executing a data transfer agreement, in many cases data subjects will either need to consent to data export, or the data recipient will need to commit to protect the information in accordance with Israeli law. Other grounds legitimising export under the GDPR are not available under Israeli law; more situations where it is mandatory to appoint a **data protection officer** (DPO), or, to use Israeli law terminology, a "data security officer". Moreover, whereas the GDPR does not include the requirement of registration of a database, Israeli law provides that certain databases must be registered with the Database Registrar, and for data exports and other activities to be notified to the Registrar. Proposed Amendment 13 to the Israeli Protection of Privacy Law (1981) will enhance Israel's data protection authority supervisory powers and fix exponentially higher penalties for Privacy Law violations.[226]

As regards privacy/data protection impact assessment, there are no obligations to conduct privacy impact assessments. Nevertheless, under the Security Regulations, organisations must conduct periodic data security risk assessments, including penetration testing, other than dataflow mapping, risk analyses, audits, employee training and similar measures.[227]

In 2009, the Israeli Knesset enacted the **Biometric Database Law,** aimed to enable identification and authentication of Israeli residents by including biometric data, namely an image of the facial features and images of the fingerprints of both forefingers, in identification documents. It regulates the establishment of a biometric database, managed by the Biometric Database Management Authority, and in which the biometric information will be kept in a secure and encrypted manner, separate from any other communication network, and in particular from the Population Registry. The database will not include any identifying information of the residents of Israel.[228]

[223] www.israel.org/MFA/MFA-Archive/1999/Pages/International%20Conventions%20on%20Human%20Rights.aspx
[224] https://www.coe.int/en/web/portal/israel
[225] https://eeas.europa.eu/headquarters/headquarters-Homepage/23264/eu-actions-counter-da%E2%80%99esh_en
[226] https://gdpr.report/news/2018/09/04/gdpr-israeli-privacy-law-key-differences/
[227] https://www.linklaters.com/en/insights/data-protected/data-protected---israel
[228] https://www.gov.il/he/departments/guides/languages_smartid

The law was amended in 2017 to render the biometric database project pilot permanent and full-scale. Collection of facial biometric information from passport or national ID applicants became mandatory, but applicants are able to opt-out of having their fingerprints taken and recorded in the database. In that case, they will be issued national ID cards or passports with a 5-year expiry date (rather than 10 years for those willing to have their fingerprints sampled and recorded). The shorter expiry period is intended to make forgeries and identity thefts more difficult. Fingerprints of children under the age of 16 will not be stored in the database and police will not be allowed to access or use the database until the Knesset promulgates regulations on this issue.[229]

Privacy and data protection related Israeli framework:

- Article 7 of Basic Law (Human Dignity and Liberty). Privacy is a constitutional right.
- Privacy Protection Act, 5741-1981 ("PPA"), contains specific privacy legislation. Chapter B of the PPA deals with data protection.
- Data Security Law 5777-2017[230]
- Biometric Database Law, 5770-2009
- 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 (2011/61/EU)

As regards border management, border crossing points and their opening hours are listed on the website of the Ministry of Foreign Affairs.[231] The types of visa provided by Israel are: immigration visa; A/1 Temporary Resident visa; A/2 Student visa; A/3 Clergy visa; A/4 visa for spouses and children; B/1 Work visa; B/2 Visitor's visa.[232]

Border management related framework:

- the Law of Return, 5710-1950, which gives Jews the right to come and live in Israel and to gain Israeli citizenship
- the Entry into Israel Law, 5712-1952

[229] https://www.israeldefense.co.il/en/node/28828
[230] https://www.gov.il/BlobFolder/legalinfo/data_security_regulation/en/PROTECTION%20OF%20PRIVACY%20REGULATIONS.pdf
[231] https://mfa.gov.il/MFA/ConsularServices/Pages/Crossing_points.aspx
[232] https://mfa.gov.il/MFA/ConsularServices/Pages/Visas.aspx