Security of Air Transport Infrastructures of Europe

D8.1: Legal state of the art

Deliverable Number	D8.1
Author(s)	ERI
Due/delivered Date	M6/2019-10-30
Reviewed by	KEMEA
Dissemination Level	PU
Version of template	1.07

Start Date of Project: 2019-05-01

Duration: 24 months

Grant agreement: 832969

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969

Document contributors

No.	Name	Role (content contributor / reviewer / other)
1	Victoria Peuvrelle (ERI)	Author
2	ITTI	Contributor
3	NIS	Contributor
4	SEA	Contributor
5	KEMEA	Reviewer
6	AIA	Contributor
7	Idemia	Contributor
8	ZAG	Contributor
9	Meilin Schaper (DLR)	Reviewer

Document revisions

Revision	Date	Comment	Author
V0.1	2019-10-02	Initial draft	ERI
V0.2	2019-10-24	Review	KEMEA
V0.3	2019-10-28	Review	DLR
V0.4	2019-10-29	Final draft	ERI
V1.0	2019-10-30	V1.0	DLR

Executive summary

The present deliverable is aimed at establishing an adequate legal framework for the preparation of the research activities in SATIE so all the members of the consortium are aware of the legal challenges posed by the project and the mitigation measures that must be implemented. Cyber security practices have become critical in the past years due to the expanding use of ICT in the so-called "smart airports". These strategies are largely driven by legal compliance requirements. Considering this, a thorough revision of the current legal framework applicable to matters related to data protection and cybersecurity at EU airports will be developed in this deliverable. In this way, the requirements and principles that should guide SATIE proposed solutions are set out.

This is achieved in various steps. After introducing the project and the deliverable in section 2, section 3 goes over human rights principles relevant in SATIE, the General Data Protection Regulation, and Cybersecurity regulations. After this, section 4 analyses the impact of these laws on the Malpensa Airport and Athens International Airport. Finally, section 5 provides a set of recommendations to follow within SATIE to adhere to the legal framework set out, with the conclusions being set out in section 6.

Table of Content

List of Figures

List of Tables

List of Acronyms

Acronym	Definition
AIA	Athens International Airport
API	Advanced Passenger Information
APIS	Advanced Passenger Information System
ATCO	Air Traffic Controller
BHS	Baggage Handling System
CSIRT	Computer Security Incident Response Team
DLR	Deutsches Zentrum für Luft- und Raumfahrt (German Aerospace Center)
DMP	Data Management Plan
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DSP	Digital Service Provider
EASA	European Union Aviation Safety Agency
EDPS	European Data Protection Supervisor
ENISA	European Union Agency for Cybersecurity
ERI	Eticas Research and Innovation
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organization
ICO	Information Commissioner's Office
IDEMIA	Idemia Identity and Security France
IoT	Internet of Things
ISMS	Information Security Management System
ITMS	Information Technology Management System
ITTI	ITTI Sp. z o.o.
KEMEA	Kentro Meleton Asfaleias
MRZ	Machine-Readable Zone
n.d.	No date
NIS	Network Integration and Solutions

OES	Operators of Essential Services
SEA	SOCIETA PER AZIONI ESERCIZI AEROPORTUALI SEA SPA
TX.X	Task X.X
WP	Work Package
ZAG	Zagreb Airport

1 Introduction

SATIE (Security of Air Transport Infrastructure of Europe) is a project funded under the H2020 scheme. The topic of SATIE is SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe.

The SATIE project attempts to address the threats to airports that the process of digitalisation is creating, as it blurs the lines between the digital world and reality. In order to do so, SATIE adopts a holistic approach about threat prevention, detection, response and mitigation in the airports, while **guaranteeing the protection of critical systems, sensitive data and passengers**. That means going beyond security strategies that only address either physical or digital threats. In order to handle complex scenarios in which both threats are combined, SATIE develops an **interoperable toolkit which improves cyber-physical correlations, forensics investigations and dynamic impact assessment at airports.**

The toolkit will be tested in three demonstrations as part of which the system will be integrated into a simulation platform. During the demonstrations, the tool's efficiency and interoperability will be validated. These demonstrations will take place in Italy, Greece and Croatia, the countries where the three partner organizations acting as end users are located.

1.1 Aim of the deliverable and outline

SATIE's workload has been divided up into 9WPs. D8.1 is part of WP8 which is dedicated to ethics, privacy and regulations. WP8 has the following objectives:

- O1: Establishing the legal and ethical framework for SATIE.
- O2: Providing legal and ethical recommendations for both development and demonstrations.
- O3: Conducting a privacy and societal impact assessment of the project development on the above basis.

Within WP8, T8.1 (Legal state of the art on privacy and cybersecurity within EU air borders) is aimed at constructing a relevant and up-to-date legal state of the art for SATIE and thus seeks to fulfill O1 and O2. Even though an analysis about compliance with data protection regulations and related recommendations will be produced in this Deliverable, O3 will be mostly tackled in D8.4 (Privacy and Societal Impact Assessment) which will build upon the framework and conclusions laid down in this deliverable.

In line with Task 8.1 description, D8.1 will focus on the following areas:

- Human rights, with an emphasis on the rights to privacy, non-discrimination and integrity.
- The definition of the legal provisions framing the technical functionalities oriented towards reducing malicious actions caused by cyberattacks and data breaches.
- Privacy and data protection regulations.
- Applicable cybersecurity regulations.
- Other relevant regulations and standards concerning security at airports and databases.
- Two case studies.

In addition to the above, the following is said in section 5.2 of the Grant Agreement (Societal Impact) about D8.1:

> *"the current set of legal constraints and requirements will be presented in D8.1, putting a special emphasis on European regulations, especially those regarding privacy and data protection. We will consider regulations, case law and other legal documents, such as the European Convention on Human Rights."*

Lastly, D8.1 is specifically aimed at accomplishing O12 of SATIE (Ensuring compliance with ethics, privacy and regulations) according to the Grant Agreement. The activity towards this objective is defined as "Deliver applicable privacy and cybersecurity requirements within EU air borders". As for the measure of success, it is the number of applicable versus applied security requirements and recommendations. Therefore, the recommendations made in this deliverable will attempt to be as relevant and applicable as possible in order to maximise the proportion of recommendations that are actually implemented and, thus, contribute to achieving the project's goals.

1.2 Involvement of the different partners in the deliverable

Eticas (ERI) leads D8.1. Nevertheless, a number of partners also contribute to it. In the description of T8.1 the contribution of the different partners D8.1 is broken down in the following manner:

KEMEA reviews cybersecurity requirements established by the legal state of the art and provides remarks.

ITTI and **NIS** contribute by the analysis of the NIS directive and GDPR regulation in the context of airport service providers.

AIA, SEA, ZAG provide and check local and national regulations applicable in the three airports.

IDEMIA refines the applicability of GDPR to the anomaly detection and processing of passenger data.

All the above partners have contributed to this deliverable with their inputs and revisions in line with their above described role.

2 Setting the scene

2.1 Cybersecurity at the smart airport

New systems and technologies at airports, currently developed in the context of the smart airport concept (Boutin, Fechtel, Ho Loh & Tan, 2016), can contribute to increase their exposure to cyberattacks (ENISA, 2016). In particular, it has been noted that this process "paves the way for new attack vectors or pathways and exposes airport assets to a larger attack surface" (ENISA, 2016:9). SATIE seeks to reduce these risks while making interoperable databases and systems, including the Traffic Management Intrusion and Compliance System (TraMICS). This document will establish the legal basis for the integration of SATIE subsystems to the security infrastructure of EU airports and proposed enhancements of existing technologies. The consortium made a point of complying with both relevant regulations and fundamental ethical principles. With this purpose, the elaboration of this legal framework will involve the review of the most **relevant pieces of legislation concerning the legal fields that were deemed relevant for SATIE**. In addition to that, such examination is followed by a series of guidelines and recommendations that are aimed to achieve legal compliance by SATIE.

2.2 The SATIE system

Though SATIE is a security research project, some of its solutions necessitate the use of personal data, are more directly involved with humans or have more relevant implications in terms of airport security and logistics. It is important therefore to take into account the possible outputs of the project on these individuals. SATIE is not, however, a personal data heavy project, nor is it intrusive. Indeed, **once deployed, the only systems that will require the use of personal data** are:

- Task 3.3: **Access control of restricted areas with real time facial recognition of participants** (only allowed staff from airports) in order to verify that only those who are allowed access enter these zones. Data will be collected and processed by airport authorities. This will be validated in T6.5.
- Task 4.2: **Speaker verification and stress detection of participants** (Air Traffic Controllers)**,** in order to identify them and detect possible security threats created by third-parties. Data will be collected and processed by air navigation service providers and in some cases airport authorities. This will be validated in T6.2.
- Task 4.4: **Linkage of participant's MRZ data** (passengers) **with their baggage,** in order to re-identify the owner of baggage that has lost its tag. Furthermore, API data of passenger provided by airport carriers will be sent to the national local authorities. This will be validated in T6.3.

Concerning the **fieldwork or research activities to be conducted in SATIE** for the development of the above toolkit, the first requirement handed in described the use of personal data in T3.3 and T4.4 in the following manner:

> *In Tasks 3.3 and 4.4, IDEMIA needs to test the correct functioning and unitary development of their systems, which does not require much biometric data. These compose the majority of*

> *the tests that IDEMIA will carry out, and only requires the data of the developer and perhaps their close colleagues. The data in such cases is not retained, and IDEMIA's developers have been trained regarding the importance of data access and data life cycles. After this stage, the algorithms need to be trained, fine-tuned and the accuracy worked on, for which more participants are involved. IDEMIA anticipates that they might need to carry out such tests for T3.3. They are considering installing the system in an open area at their premises, where panels explain what is happening and where some of the system's developers are present to help staff interested in participating. If data needs to be collected, the participant signs a consent form. These data are securely stored and to which the access requires the DPO's approval. (SATIE consortium, 2019).*

When demonstrated in the airports in T6.3 and T6.5, the API data and facial biometrics of consortium members or dummy data shall be used to validate the activities tested in T3.3 and T4.4.

In Task 4.2, DLR will be testing conformance monitoring alerts with Air Traffic Controllers (ATCOs) and/or internal participants. The only personal data collected in that case is the name of the person whilst filling the consent form and pseudonymised voice recordings, which will be managed according to the standards and protocols established in the DMP. SAV will be testing speaker verification and stress detection prior integration into TraMICS at their premises. Testing the system's ability to notice stress/emotion in participants' voice will require participants, of which the name, surname, age, sex, contact email, voice audio recording, skin resistance, heartbeat and electroencephalogram data will be recorded. SAV keeps the identification data (meta-data referring to name, biological sex, contact information) separately from the voice and bio-signal data of the data subjects. They will also use existing databases (their own databases as well as publicly available third-party databases). The activities carried out in T4.2 will not be validated at any airports.

2.3 Applicable regulations

In order to accurately determine the legal frameworks and requirements to be considered during the development and implementation of SATIE, its technical specifications, functionalities as well as relevant socio-technical aspects need to be accounted for. This includes both the characteristics of the system (functions, subsystems, etc.) and its main human-machine dynamics (actors involved in its management, persons or objects monitored/surveilled, etc.). In this regard, this document addresses regulations concerning **cybersecurity at airports** to define the requirements to be fulfilled by those security systems aimed at preventing and coping with complex attacks in these contexts. Supranational regulations establishing legal requirements for surveillance activities conducted by the competent authorities at the EU airports, which may be relevant for SATIE design or implementation, will therefore be examined in order to establish the legal scope of action in this regard.

A second dimension to be covered by this legal analysis concerns **those standards framing the data interoperability within airports and other security systems**, mainly with databases managed by third processors or controllers. It should be noted that the new system concerning untagged baggage will associate these objects to the identity (personal data) of potential data subjects involved. Furthermore, the API anomaly verification system will share the API data with national authorities. The legal analysis will therefore have to address both specific regulations concerning existing databases and also those regulations or legal provisions posing requirements for the interoperability of systems to be interoperated in order to deploy the SATIE toolkit.

Furthermore, in line with the above, the **data management of the systems will be considered in light of the GDPR**, starting by the potential of the system for personal identification and its profiling capabilities. The GDPR is the main legal text on data protection that is examined in this document given the fact that it is the main regulation on data protection in the EU and that SATIE is a system intended to be used by airport operators and not by the security authorities, in which case the so called Police Directive could also be applicable. Issues around the unified access control system will have to be considered, mainly due to the use of biometrics and video analytics with the purpose of identifying objects, threats and preventing possible attacks. The Traffic Management Intrusion and Compliance System (TraMICS) will also process biometric information, being the speaker verification and stress detection system. Two issues will have to be properly addressed in this regard. On the one hand, biometrics for the purpose of uniquely identifying a natural person is considered sensitive data under the GDPR (Art. 9), which requires special safeguards in their treatment. On the other hand, the automation of data processing is also subjected to the requirements posed by this regulation concerning automated decision making.

Concerning the analysis of these regulatory frameworks, data protection principles and applicable GDPR requirements will be established, while possible tensions with the NIS and the rest of regulations will also be examined. The examination will also analyse the proportionality of the system security strategy, including the encryption framework for secured IoT communications on BHS or the use of the software or the ITMS for processing personal data related to threats detection, following the specifications defined in the GDPR.

Lastly, concerning security and data management, relevant aspects of international standards (ISO 27001) for the development of the risk assessment platform with cyber-physical threat analysis (RIS) will be considered. For instance, packet inspection and file analysis must also follow aviation specific rules, which in many cases correspond to both national regulations and national standards for aviation security.

Taking all the above into consideration,, the relevance of **human rights within the context of SATIE is discussed**. The focus will be placed on the rights to privacy, integrity and non-discrimination. All three ones are particularly important from a research standpoint, but also for the outcomes of the project. As a matter of fact, the Privacy and Societal Impact Assessment carried out in D8.4 will necessarily draw from the findings concerning human rights that are included in this deliverable, as a central element that will determine the project's level of social acceptability and alignment with basic universal human rights.

The rights to privacy, integrity and non-discrimination will be examined from a twofold perspective. First, how these rights will be observed during the project's lifetime. Second, the challenges that the outcomes of the project could potentially pose to human rights. The right to privacy will only be briefly examined as part of this section due to the fact that Section 2.2 addresses this regulatory field extensively. As for non-discrimination, it will be analysed by making a particular emphasis on gender, given that its importance for the project was highlighted in the Grant Agreement.

Furthermore, data protection and privacy will be tackled, where the General Data Protection Regulation (GDPR) and other relevant pieces of legislation will be examined along with other sources on the matter, such as the opinions and guidelines issued by the European Data Protection Supervisor (EDPS). This section's aim will be to break down the most important aspects of the regulation in order to ensure the right to privacy and data protection of both research participants and future travelers that will come in touch with the system once it is implemented. By doing this, the SATIE consortium expects to apply the principle of "Privacy by Design" established by the GDPR.

Then, the NIS directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.) is accounted for in order to provide partners with the legal principles and guidelines that should inform both the project's development and its technological outcomes in regards to cybersecurity. The European directive is examined along with the national legal instrument that has been used to transpose it to the member states in which demonstrations are to be carried out in order to ensure that the legal recommendations account for national specificities.

Thus, the national legal systems of the three countries in which demonstrations will be carried out will be looked into.

3 Legal framework: Identification and analysis

3.1 Human rights

The SATIE project purports to provide a set of security solutions to airports, hence bettering the security of infrastructures through which millions of people go by. This means that the effect on humans, and for the purpose of this deliverable, the effects on human rights, of all of the solutions, not only those that use personal data, should be considered.

Due the above-explained characteristics of the SATIE system, one of the issues to be considered is how it deals with social identifiers. When dealing with personal data, one of the first concerns is that of privacy; how will the solutions developed impact on the right to privacy of passengers, staff, and anyone at the airports which the systems developed in SATIE might impact?

In order to fully understand what the right to privacy entails, and how SATIE systems might impact it, the following definitions in various international instruments are of relevance:

Charter of Fundamental Rights of the European Union.

Article 7:

Everyone has the right to respect for his or her private and family life, home and communications.

European Convention on Human Rights.

Article 8:

1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a **public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society** in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Universal Declaration of Human Rights.

Article 12:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks

The right to privacy **is not an absolute right**, but a conditional one; someone's privacy might be breached for legitimate purposes, in a proportional manner. The European Convention on Human

Rights hints towards this in its second paragraph. Therefore, SATIE must deal with passengers' personal data in a proportional manner and according to the legal standards on data protection.

The right to the protection of personal data, if not to be extensively developed in this section, is worth mentioning too:

<u>**Charter of Fundamental Rights of the European Union**</u>

Article 8:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

This article emphasises the principle of **purpose limitation and two of the data protection rights that people enjoy in the European Union**, namely the right to access and rectification. The right to data protection is detailed in the General Data Protection Regulation, which constitutes the main regulatory framework on the topic in the European Union. It is worth mentioning here, however, that protecting personal data has become sufficiently important to be considered a fundamental right, and is therefore to be carefully protected.

Furthermore, **non-discrimination** was identified by the consortium as a fundamental value in SATIE within the context of the processing of personal data belonging to passengers. Measures to avoid discrimination are developed in D8.3, which is defined as follows by different legal texts:

<u>**Charter of Fundamental Rights of the European Union.**</u>

Article 21. Non-discrimination:

1. Any discrimination based on any ground such as 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 shall be prohibited.

2. Within the scope of application of the Treaties and without prejudice to any of their specific provisions, any discrimination on grounds of nationality shall be prohibited.

<u>**European Convention on Human Rights.**</u>

Article 14. Prohibition of discrimination:

The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

Article 1. General prohibition of discrimination (Protocol No. 12):

1. The enjoyment of any right set forth by law shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.

2. No one shall be discriminated against by any public authority on any ground such as those

mentioned in paragraph.

Universal Declaration of Human Rights.

Article 7:

All are equal before the law and are entitled without any discrimination to equal protection of the law. All are entitled to equal protection against any discrimination in violation of this Declaration and against any incitement to such discrimination.

Although a set of personal data is used within SATIE both to query the passengers against the Government watch lists ("screening") prior to the arrival of the plane and to identify abnormal behaviours, the system is designed to conduct these tasks without violating the right to equality against the law. Still, it should still be noted that algorithms will be developed to automate these tasks, so these systems will have to be monitored in order to ensure compliance with the security standards for ML defined by the GDPR, which will be explained in the following section. Moreover, the identification of suspicious behaviours, implemented under the concept of extended passenger identity, will have to be based on fair and legal grounds particularly concerning protected groups detailed above (Article 21 of the Charter of Fundamental Rights of the European Union) and following the requirements on non-discrimination concerning border checks established in Article 7 of the Schengen Border Code[1].

Article 7:

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.

Lastly, the **right to integrity**, defined in the following manner, is also relevant when considering that one of the activities of SATIE seeks to detect stress levels in participants, and once implemented, in certain Air Traffic Controllers. End users of the SATIE toolkit must be protected against possible psychological implications of the stress detection system and the labour rights of the airport and air navigation service provider staff guaranteed when collecting their personal data with security purposes. The literature has revealed how surveillance or monitoring systems used at work can cause anxiety and increase stress among other mental health problems (Lee and Kleiner, 2003; West and Bowman, 2016). Ensuring that this is not promoted by the SATIE subsystems aimed at monitoring the airport staff, should be one of the goals of the project.

[1] It should still be noted that Border Guards will not directly interact with the SATIE toolkit.

Charter of Fundamental Rights of the European Union

Article 3:

1. Everyone has the right to respect for **his or her physical and mental integrity**.

2. In the fields of medicine and biology, the following must be respected in particular:

(a) the free and informed consent of the person concerned, according to the procedures laid down by law;

(b)the prohibition of eugenic practices, in particular those aiming at the selection of persons;

(c) the prohibition on making the human body and its parts as such a source of financial gain;

(d) the prohibition of the reproductive cloning of human beings.

Finally, one of the main concerns in terms of the right to integrity are the effective consequences that **security checks based on the systems integrated to the SATIE toolkit** may have over passengers. SATIE identification of anomalies regarding passengers' data or the detection of an unexpected event, could lead to alert SOC operators and security authorities at airports about potentially harmful individuals. In this context, security response **might lead to false positives** affecting the right to integrity of affected individuals. One of the innovations proposed by SATIE, the correlation between cyber and physical threats, is particularly relevant in this regard, since it may either reduce or multiply the risks of misidentification depending on the target outcomes and the security mechanisms in place. Nevertheless, since SATIE is aimed at preventing and aborting physical and/or cyber-attacks, interruption of airport services and potentially harmful situations for travelers, these risks should be reduced at minimum. Events to be addressed by the system include injuries, loss of life, distress and psychological impact on passengers, riots or physical attacks. In this line, the system seeks to contribute to reach the cybersecurity goals established by the EASA[2] concerning safe air travel in Europe and worldwide. Still, in order to be well aligned with the spirit of the Convention and Charter above, the system must be able to integrate proactive mechanisms for preventing and monitoring false positives.

3.2 Data Protection

3.2.1 The General Data Protection Regulation (GDPR)

3.2.1.1 Personal data

As briefly mentioned above, protection of personal data is considered a fundamental right in the European Union, and its main legal framework consists of the GDPR. Given that SATIE does process personal data, a framing of this right is required. First of all, personal data is defined in article 4 as such:

Article 4 (1):

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in

[2] Protocols are available at https://www.easa.europa.eu/document-library/general-publications?publication_type%5B%5D=144

particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The subject of the data protection rights granted by the GDPR are defined as data subjects, who are natural persons to whom data can be linked. Correctly identifying what data are personal data for data subjects is of the utmost important for the legal analysis of SATIE's outcomes and research process. **Personal data can be any information that either identifies or allows for the identification of natural persons**. The GDPR gives a number of examples but does not provide a comprehensive list. This is due to the fact that even data that seems to not be problematic from a data protection standpoint has proven to allow for the identification of individuals (Narayanan and Shmatikov, 2008).

The advance in the interoperability between existing systems at airports proposed by SATIE involves the gathering of airports' staff personal data and also the exchanging of travelers' personal data in order to effectively prevent possible threats and enhance anomaly detection and incident response. **The identifiers to be collected/processed by the SATIE toolkit include biographical data** from passports or the baggage registration service, provided by the corresponding border control authorities. Check-in data and the extended passenger identity with baggage tracking will be used, including the Travel Document information ("MRZ" Machine Readable Zone) of all passengers checked-in, the flight data, and when possible the seat and luggage information. Moreover, the system will process special categories of personal data (Article 9 GDPR, see description below), in particular **facial biometrics and voice print of airport workers**, which requires to integrate specific safeguards for their handling.

In order to minimize the risks of handling the above data, for instance concerning their misuse, there are a number of ways in which data can be protected. One of these is to pseudonymise data, which is a process the GDPR defines as:

Article 4(5):

'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

This is a general definition which the WP29 has provided an opinion on (Article 29 Data Protection Working Party, 2012), to detail further. Pseudonymization guarantees a lower level of knowledge about an individual to re-identify this person in a database. Depending on the criticality of the database, this technical method of protecting data might be sufficient. It must be emphasized, however, that pseudonymized data remains personal data, and still falls within the scope of the GDPR.

Anonymized data, on the other hand, is not considered personal data by the GDPR. It is defined as:

Recital 26:

[...] The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

Anonymization consists in **altering the dataset containing personal data in a manner which makes it theoretically impossible to re-identify individuals**. There are various ways to alter a dataset, which can consist in grouping individuals according to certain common attributes, deleting certain fields, replacing fields with false data that are similar, making the data less precise, etc. These were also further discussed by the WP29 (2014). Anonymisation has to be distinguished from pseudonymisation, which makes it more difficult for data to be used for the re-identification of individuals, but not impossible.

The above described subsystems of the SATIE toolkit, which integrate sensitive personal data from airports' staff and passengers, use anonymization techniques at different points of the data management process. These anonymization points and the methods of anominization used in each case are described in D9.7, where the technical and organisational measures that are implemented to safeguard the rights and freedoms of the data subjects/research participants are discussed. This process is particularly relevant since involves changes in the legal status of data (Recital 26 GDPR), but also because it is one of the most important security measures for sensitive data to be conducted as part of the SATIE toolkit data life cycle. Moreover, exceptions for the disclosure of information to third parties, beyond the use of informed consent, involve that the personal information is properly anonymized in advance.

3.2.1.2 Special categories of data

As mentioned above, some of the activities to be carried out in SATIE process biometric information (T3.3 and T4.2), namely facial biometrics (T3.3) and voice biometrics (T4.2). Opinion 03/2012 of the article 29 Working Party (2012) explains that the relevant legal framework for the processing of biometric information is the Data Protection Directive (95/46/EC), now replaced by the GDPR. The GDPR defines biometric information as such in the following manner:

Article 4 (14):

'biometric data' means 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;

Biometric information being considered a special category of data, its processing is generally forbidden (Article 9.1 GDPR), unless any of the conditions established in Article 9.2 apply:

Article 9.2:

2. Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
e) processing relates to personal data which are manifestly made public by the data subject;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Taking the above into consideration, the **processing of sensitive personal data is not prohibited but subjected to further safeguards**. The sensitive data used for research purposes will be processed on the basis of informed consent, while the sensitive data processed once the system is deployed will be processed on the basis of public interest. Furthermore, as established in Article 9.2 g) GDPR, this type of processing shall be "proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject". In brief, **the management of special categories of data by the SATIE systems must be based on one of the requirements stated above and their controllers/processors (see next section) must establish special security measures for their treatment**, which may include anonymization, encryption, strong user authentication, backup solutions or data erasure.

3.2.1.3 Roles

The SATIE innovative solutions necessitate the linking of a number of different systems, some of which require the use of personal data, thus having a potential impact on human beings. It is therefore crucial to be clear on the roles and corresponding responsibilities of the different actors in this ecosystem.

The data controller is the key role in data processes involving personal data, as it is the entity which bears most of the responsibility for what happens to personal data. What a controller is is defined in article 4(7):

Article 4(7):

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

The responsibilities of the controller, on the other hand, are defined in article 24:

Article 24:

1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
3. Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Article 24 does not provide an exhaustive list of all the obligations of the controller. The following are also relevant:

- Transparent information, communication and modalities for the exercise of the rights of the data subject (Article 12 GDPR).
- Data protection by design and by default (Article 25 GDPR).
- Obligation to only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject (Article 28 GDPR).
- Records of processing activities (Article 30 GDPR).
- Security of processing (Article 32 GDPR).
- Notification of a personal data breach to the supervisory authority (Article 33 GDPR).
- Communication of a personal data breach to the data subject (Article 34 GDPR).
- Data protection impact assessment (Article 35 GDPR).
- Prior consultation (Article 36).
- Designation of the data protection officer (Article 37 GDPR).
- Transfers subject to appropriate safeguards (Article 46).

The consequences of not complying with the regulations for controllers are established in Articles from 82 to 84. Data subjects who have their data protection rights harmed as a result of a lack of compliance of the controller have the right to be compensated. Furthermore, violations of the regulation can result in administrative fines and penalties.

The controller is not necessarily the only entity processing personal data. Other entities can also process personal data on behalf of the controller. These are called processors and are defined as such:

Article 4(8):

'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

The processor does not decide on the purposes or the means to process data themselves, as it is established in Article 28.2, which also asks the processor to not engage other processors without having an authorisation from the controller:

Article 28.2:

The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

In order for the terms by which the relationship between the controller and the processor must abide to be as clear as possible, the GDPR has established that the purposes and means of the processing have to be established in a document or other legal act that is binding on the processor.

Article 28.3:

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

The terms of such agreement must not be breached by the processor unless Union or Member state law asks them to do so.

Article 29:

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

As well, controllers must keep records of the processing activities it has carried out on behalf of the controller. Such records need to include a certain number of categories, including information on the data controllers on behalf of which a given processor is processing data, the categories of data being processed, the policy on data transfer and information on technical and organisational security measures.

Article 30.2:

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
b) the categories of processing carried out on behalf of each controller;
c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1)

The above articles establish the main obligations of data processors. In general, data processors are responsible for supporting the controller in order to comply with the GDPR, not processing data for different purposes or by different means than those established by the controller, keeping records of their processing activities and, in general, abiding by the terms agreed with the controller.

In certain cases involving the processing of a certain amount of personal data, or when the processing is a special kind of entity, the appointment of a Data Protection Officer (DPO) by said entity is required, as per article 37.1 of the GDPR:

Article 37.1:

The controller and the processor shall designate a data protection officer in any case where:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

The tasks the DPO must encure are detailed in article 39:

Article 39:

1. The data protection officer shall have at least the following tasks:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
d) to cooperate with the supervisory authority;
e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where

appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

As part of the SATIE data governance, it is expected that **airports' private and public authorities will act as data controllers of the solutions deployed in their corresponding facilities**, having to respect the above obligations. However, some of the processors involved in the management of the databases storing passengers' personal data to be used for baggage identification will also act as data controllers regarding some data exchanges. In particular, API data (Advanced Passenger Information – check-in data) will be used by SATIE. This system contains the Travel Document information ("MRZ" Machine Readable Zone) of all passengers checked-in, the flight data, and when possible the seat and luggage information. These data are collected by air companies and used by the Smart API data analysis system to query the passengers against the Government watch lists ("screening"), prior to the flight's landing. Consequently, the SATIE airports will have to follow the legal conditions established for API controllers concerning the processing of these data.

3.2.1.4 Legal basis of processing

Processing personal data can only be lawful if it is carried out on the basis of one of the following grounds:

Article 6:

Processing shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Consent is a key element in the GDPR. Indeed, in many cases, the processing of personal data is not allowed unless consent is provided; **consent thus represents the main key to processing**. People's consent has been taken advantage of during the past, which is why the GDPR strengthened the concept to make sure consent is informed and explicit.

Consent is therefore defined as follows:

Article 4(11):

'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

The conditions for consent to be valid are the following:

Article 7:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The performance of a contract, which shall include the data protection specifications involved in the work position (Art. 6 b), is the legal basis for the SATIE solutions to be implemented for identifying airports' staff or to measure the levels of stress of Air Traffic Controllers. However, in the case of the system for linking passengers with their corresponding baggage, the legal basis shall be public interest due to the specific security purposes behind this subsystem (Art. 6 e), which may involve derogations in articles 5(1)b and 9(2)(e). The ICO guidelines on public interest ("Public task", n.d.) as a lawful basis for processing establish the following conditions for public interest to be used as a lawful basis for the processing of personal data:

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.
- If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

Therefore, as already mentioned, an EU or national law must establish the obligation/capacity to process personal data on these basis. These legal provisions, including the NIS Directive and the Council Directive 2004/82/EC, will be laid down in the following sections.

3.2.1.5 Principles

Processing personal data in a fair manner which is respectful of the fundamental rights of the data subjects represents the incentives behind the data protection legislations that have proliferated in the past decades. The first ethical principles to follow were set out in 1980 by the Organisation for Economic Co-operation and Development, and have served as a baseline for subsequent legislations.

The GDPR has also drawn from these principles, and includes the following:

Article 5.1 (a):

processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);

Lawfulness processing is that which is carried out on the basis for processing established in Article 6.1 GDPR. As for the principles of fairness and transparency, they require that the data subject be informed of the existence of the processing operation and its purposes (see Article 60). Therefore, they have to do with informed consent.

Article 5.1 (b):

collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**);

The principle of purpose limitation implies that data must be collected in order to fulfil certain goals. This is also related to informed consent since data subjects must be informed of the purposes for which their data are going to be processed in order for consent to be considered truly informed and lawful (see Articles 13 and 14 GDPR).

Article 5.1 (c):

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);

The principle of data minimisation establishes that the data collected from data subjects must be kept to a minimum. In other words, such data should not be more than what is strictly necessary in order to achieve the purpose of the processing.

Article 5.1 (d):

accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (**'accuracy'**);

Data must be accurate and reflect reality, which needs to be judged in relation to the purposes of the processing. The main way in which this principle is enforced in the GDPR are the rights of the data subject, who can ask the controller to erase or rectify the data that it has regarding the data subject (Articles 16 and 17 GDPR).

Article 5.1 (e):

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (**'storage limitation'**);

The principle of storage limitation establishes that personal data should not be kept for any longer than is reasonable for achieving the purposes for which they were collected in the first place. The period can be longer if the data are being processed for one of the purposes in Article 89 GDPR (public interest, scientific or historical research purposes, and statistical purposes), which could be the case for SATIE as some of the processing activities carried out during its deployment will be justified on public interest grounds. However, that does not exempt the controller from putting in place technical and organisational measures aimed at safeguarding the rights and freedoms of the data subject, which will be discussed in D9.7.

Article 5.1 (f):

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 (**'integrity and confidentiality'**).

D9.7 is entirely dedicated to the technical and organisational measures adopted by SATIE in order to safeguard the rights and freedoms of data subjects and research participants.

Article 5.2:

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (**'accountability'**).

In order for the other principles established in the GDPR to have teeth, the principle of accountability asks for those responsible to be held accountable if they are not compliant. The sanctions and fees established in the GDPR (see Articles 83 and 84 GDPR) have been devised in order to provide incentives for good behaviour.

All of these principles should be applied by the processing entity when processing personal data. To this effect the GDPR asks the data controller to consider data protection by design and by default when developing a technology or service which requires the use of personal data:

Article 25:

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

It could be said that this very deliverable, the whole of WP8 and especially D8.2 are aimed at complying with the principles of data protection by design and by default, since they attempt to raise awareness of the potential issues that the project can create. D8.1 is also aimed at addressing them at an early stage in order to improve the level of legal compliance and ethical awareness. In this regard, beyond the analysis of legal compliance with the data protection requirements, concrete recommendations will be made in the last section to ensure that SATIE is aligned with these principles. This includes the security measures aimed at avoiding function creep, the limitation in the collection of personal data, the thorough and understandable explanation of the aims and processes behind the collection of personal data belonging to both staff and passengers-, and the establishment of a privacy by design approach to technological development concerning the three subsystems collecting personal data within SATIE.

3.2.1.6 Other relevant requirements in the GDPR

3.2.1.6.1 Secondary use

Within SATIE, staff and passengers' identification systems use personal data that has already been collected. D9.9 is fully dedicated to discussing the lawful basis for the processing of data previously collected and the appropriate technical and organisational measures in place to safeguard the rights of the data subjects.

Article 6.4 GDPR establishes the following regarding the processing of data for secondary use:

Article 6.4:

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d) the possible consequences of the intended further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

As stated above, three systems will process personal data in SATIE. These three systems will have to process data for secondary use. The legal basis for this are:

1. The performance of a contract in the case of the **Unified access control and video analytics against physical intrusion**. Here the previous purpose was to ensure that the data subjects concerned were able to access restricted areas of the airport in order to carry out their job tasks, whereas the new one is identical, but achieved by means of a different system.
2. Consent in the case of the **Traffic Management Intrusion and Compliance System**. Here the previous purpose of the data collected by SAV is the same as the new purpose: i.e. to develop a system which recognizes stress.
3. The performance of a task carried out in the public interest (national security) in the case of the **anomaly detection on passenger records (API)**. Here the previous purpose of the data collected by air companies is compatible with the new purpose: i.e. to identify passengers and their belongings.

Therefore, overall, the processing of previously collected personal data in SATIE is conducted with identical or compatible purposes than those defined for data collection. A more detailed analysis of the lawful basis for further use of previously collected data can be found in D9.9.

3.2.1.6.2 Automated decision-making

The access control activity carried out in T3.3 entails automated decision-making, in so far as the system, upon succeeding or failing to match the biometric information of the person seeking to be authenticated, shall automatically decide whether or not to allow or refuse access to restricted areas.

The GDPR makes the following statement concerning automated decision-making:

Article 22:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
2. Paragraph 1 shall not apply if the decision:
   a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
   b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
   c) is based on the data subject's explicit consent.
3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

The system developed as part of T3.3 is expected to perform an automatic decision on the basis of personal data. The consequences of being denied access to a restricted area will vary depending on the status of the individual affected. If the individual does not have access to the restricted area, the consequence will be that the system will be functioning as expected. Conversely, if the individual has access to the restricted area, **being denied access to it would mean that they could not perform certain tasks associated with their job post.** Therefore, it cannot be considered that the facial recognition system significantly affects the individual interests of the employee being denied access to the restricted area wrongfully, since such denial would be temporary. Moreover, the possible negative consequences derived from the employee being unable to carry out their work would mainly concern and be the responsibility of the controller/employer.

Still, given that the automated processing is necessary for the performance of a contract between the data subject and the data controller, the **controller should put in place measures in order to safeguard the data subject's rights and freedoms and legitimate interests**, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision as established in Article 22.3 GDPR.

Furthermore, the use of algorithms for processing passengers' API data and matching them with government watch lists, will be legally based on Art 22 (b) above. Issues with algorithmic processing as part of the SATIE deployment may include misidentification of passengers, false positives in the linkage of (suspicious) passengers and baggage as well as algorithmic bias, mainly due to inaccurate data collection techniques and or biased algorithmic models. Concrete protocols, such as the development of Algorithmic Impact Assessments as well as the evaluation and validation of the performance of the data collection tools, should be put in place for the processing of passengers' data. Even though the processing of these data will be legally authorised by a Union law (Art 22, b), these measures should be oriented towards guaranteeing the quality of the collected data and avoiding potential negative externalities of automated processing. Moreover, in line with the principle of transparency integrated into the GDPR, the aims and methods of algorithmic processing should be clearly explained to users, including explicit references to the relative impact of automation over the expected decisions.

3.2.1.6.3 Security

Ensuring the security of personal data from misuse or abuse is an essential aspect of data protection legislations. The GDPR states concerning security:

> **Article 32.1:**
>
> Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk [...].

Therefore, the GDPR's approach to **security is based on risks and the current state of the art**. Such assessment must be adapted to the SATIE specific processes and performance, as it will be done during the project demonstrations. In other words, the security measures adopted by the SATIE project and its societal impact assessments analysing legal compliance (D8.3 and D8.4) will address the requirements of Article 32.1. That is precisely the same approach adopted by the NIS Directive, which is discussed in section 3 of this deliverable. While the GDPR is concerned with the security of personal data, the NIS Directive is tasked with ensuring certain standards of cybersecurity across the European Union. In spite of this difference, both of them take a risk-based approach.

D8.3 and D8.4 are not the only ones concerned with security measures in SATIE. D9.7, D9.9, D9.10 and D9.11 are also concerned with data security, each of them from a different angle. Moreover, all partners in the SATIE consortium are committed to ensuring the highest security standards throughout the research and technological development processes.

3.2.1.6.4 Breaches

The GDPR establishes the obligation for controllers to notify the competent supervisory authority in the event of a data breach in Article 33.1:

Article 33.1:

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

Personal data breaches are defined in the following way in the GDPR:

Article 4 (12):

'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Once again, the GDPR does not establish a very specific requirement for achieving compliance. Instead, it gives a considerable degree of autonomy in the implementation process, which makes the regulation able to still be useful after technological change has taken place. However, that also creates a certain degree of legal uncertainty. In particular, the GDPR expects the data controller to assess how likely it is for a particular data breach to result in a risk to the rights and freedoms of natural persons. Recital 85 GDPR includes a list of examples of negative effects that a personal data breach can have on individuals:

Recital 85:

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as **loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned**. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

Beyond this ambiguity, SATIE does not involve particular security risks. Actually, the toolkit contributes to airports' physical and cyber security in order to globally improve the resilience of airport infrastructures, focusing on baggage handling, passenger records management, flight information display and airport operations. Moreover, the new data management systems integrating the SATIE toolkit do not add particular risks concerning the management of passengers' data. Notifications and alerts are provided to end users on the incident management platform only in case of threats detection and do not include personal data. Data security measures are in place to ensure adequate data protection, such as encryption, anonymization, access control and password protection. These measures are detailed in D9.7.

In line with the above, the GDPR establishes that the controller also needs to keep a record of any personal data breaches that includes information on its effects and the actions taken to mitigate its effects according to what is said in Article 33.5.

Article 33.5:

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Additionally, the data controller is not only obliged to notify the supervisory authority but also to notify the data subjects affected by it in those cases where a **personal data breach** is likely to result in a high risk to the rights and freedoms of natural persons as it is stated in Article 34.1.

Article 34.1:

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Once more, the GDPR leaves significant room for maneuver in the implementation, this time regarding the interpretation of what is considered undue delay.

Nevertheless, Article 34.3 provides a set of criteria with which the need for communicating the data breach to data subjects can be assessed in a more objective way.

Article 34.3:

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

In line with the above and also with the safeguarding/information obligations posed by the NIS Directive (see analysis below), it would be desirable that the SATIE system integrates an automated protocol for managing the alerts of data breaches and notify them to those affected in due time.

Otherwise, such mechanisms will have to be embedded in the standards for the personal data handling conducted by the airport authorities.

3.2.1.6.5 DPIA

The carrying out of a Data Protection Impact Assessment might be required when developing new technologies or using special categories of data. The GDPR lays down criteria so as to establish under what conditions a DPIA is needed in Article 35.

Article 35.1:

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, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

This set of criteria is aimed at facilitating the decision on if a DPIA needs to be carried out or not. The two main elements to be taken into account are how novel the technologies being developed are and the level of risk that the project presents to the data subjects rights and freedoms. Nevertheless, they are still too broad, which is why Article 35.3 specifies a list of cases in which a DPIA has to be carried out.

Article 35.3:

A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
c) a systematic monitoring of a publicly accessible area on a large scale.

D9.5 includes an opinion on the need for conducting a DPIA which takes into account each of the circumstances described in the article described above. It also factors in the guidelines issued by the ICO (Information Commissioner’s Office) on this topic. In this deliverable tasks T3.3, T4.2 and T4.4 (the tasks in SATIE that will involve the processing of personal data) are examined in the light of the GDPR and the ICO’s guidelines. The conclusions reached in this deliverable are summarised in the following excerpt:

It has been concluded that a DPIA is not mandatory within the context of SATIE. No large amounts of data will be collected or treated, sensitive data will only be collected from partners and consenting adults (facial identifiers, voice and movement) but these data won’t be able to lead to profiling of participants, will be gathered under informed consent and managed following strict security measures reflected in the Data Management Plan (D1.1). The risks for privacy that the systems present, will be identified and addressed by the consortium as part of WP8. In fact, a “Privacy and Societal Impact Assessment” will be conducted in D8.4.

Therefore, the consortium has ruled out the need for conducting a DPIA since SATIE will not threaten the data subject's data protection rights to an extent that would justify it according to the criteria set out in the GDPR.

3.3 Cybersecurity

3.3.1 NIS Directive

Cyber-security risk management practices deployed by the Schengen border controls have become decisive in the last years due to the expanding use of ICT in the so-called "smart airports", which has been partially motivated by the need to comply with new legal requirements.

The NIS Directive, officially known as Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. This directive was passed in 2016 and entered into force in May 2018, and it is the first comprehensive piece of European legislation specifically aimed at improving cybersecurity in relation to the protection of critical infrastructures. It **aims at ensuring that operators of essential services, such as air transport, appropriately address cyber risks** (Michels and Walden, 2018). In order to achieve this, the European legislator has taken a risk-based approach similar to that of the General Data Protection Regulation. This means that the NIS Directive does not require the affected organisations to implement specific policies or security measures. Instead, it obliges them to consider the risks that their activities involve and put in place preventative measures that are proportionate to their likelihood and the potential damage they could cause. The obligations imposed by the NIS Directive can be divided into two different categories (Ibid.):

- **Safeguarding obligations**: they require organisations to put in place appropriate and proportionate security measures.
- **Information obligations**: they require the sharing or disclosure of information.

The two first points of articles 14 and 16 shown below are insightful as far as understanding the obligations placed upon relevant operators by Member States:

Article 14. Security requirements and incident notification.

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.

2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

Article 16. Security requirements and incident notification.

1. Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in the context of offering services referred to in

Annex III within the Union. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

(a) the security of systems and facilities;

(b) incident handling;

(c) business continuity management;

(d) monitoring, auditing and testing;

(e) compliance with international standards.

2. Member States shall ensure that digital service providers take measures to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services referred to in Annex III that are offered within the Union, with a view to ensuring the continuity of those services.

In terms of the subjective scope of the regulation, the figure of 'operator of essential services' is defined in article 4(4) of the NIS Directive:

> *'operator of essential services' means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2).*

The types of entities in annex II in the air transport sector include airports and Air Navigation Service Providers, which are relevant in the context of SATIE.

The NIS Directive refers to point (1) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council, which defines airports in the following way:

> *'airport' means any land area specifically adapted for the landing, taking-off and manoeuvring of aircraft, including the ancillary installations which these operations may involve for the requirements of aircraft traffic and services, including the installations needed to assist commercial air services;*

Concerning the definition of air traffic control services, the NIS refers to article 2 of Regulation 549/2004 as such:

1. *'air traffic control (ATC) service' means a service provided for the purpose of:*
    a. *preventing collisions: — between aircraft, and — in the manoeuvring area between aircraft and obstructions; and*
    b. *expediting and maintaining an orderly flow of air traffic;*

To summarise, the NIS directive outlines that:

- Member states should set up their own national cybersecurity strategy, with objectives, national priorities, proactive, response and recovery measures; awareness, training and education policies; encouraging cooperation between the public and private sectors; a list of actors involved in the implementation of the strategy, and regulatory measures.
- Member states should designate a single national contact point to ensure international cooperation and connection with other Member States. With regard to controls over the implementation of the directive, it will instead be possible to designate more authorities.

- Member states create one or more CSIRTs (Computer Security Incident Response Team) responsible for monitoring incidents on their territory, and to provide early warnings with the aim of facilitating the circulation of information on risks and incidents, also at the international level (for example with other CSIRTs).
- Member states identify operators of essential services. These operators are all those companies that, for various reasons, have an important role for society and the economy of the country, for example, managers of power plants, managers of large transport networks, financial institutions (banks, stock exchange), large hospitals, telecommunication network managers, etc. In practice, the managers and/or managers of everything that can be considered "critical infrastructure."

Being a directive, the NIS directive requires Member States to transpose it via a national legislative act. Consequently, every member state has freedom to identify minimum security measures, methodologies for risk analysis and for governance in general.

The overall SATIE concept and its subsystems are aligned with the standards above and contribute to their advance and implementation. Indeed, SATIE works perfectly in line with NIS as it intends to provide additional levels of security for network and information systems in critical infrastructures (airports). The SATIE system provides technical measures to help airports deal with security incidents more efficiently, following the requirement of article 14 of the NIS directive:

Article 14:

1. **Member States shall ensure that operators of essential services take** appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems **which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.**
2. **Member States shall ensure that operators of essential services** take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems **used for the provision of such essential services, with a view to ensuring the continuity of those services.**

3.3.2 National implementation of the NIS directive

The three subsections below consist in the explanation of the implementation of the NIS directive in the three countries in which the end-users of the project are based, namely; Italy, Croatia and Greece.

3.3.2.1 Italy

Implementation:

The NIS directive was implemented through the legislative Decree 65/2018, on May the 16th, 2018.

National Strategy:

The national strategy is available at:

https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

DSP Summary:

For any data incidents, DSPs must report immediately to the Italian CSIRT.

Single point of contact:

Presidenza del Consiglio dei Ministri - DIS

National competent authority for DSPs:

Ministero dello Sviluppo Economico (http://www.isticom.it/) is one of the relevant authorities for DSPs, a second one, relevant for air transport is the Ministero delle Infrastrutture e dei Trasporti - Organo Centrale di Sicurezza.

Failure for non-compliance can result in an administrative fine of up to 150 000 EURO.

3.3.2.2 Croatia

Implementation:

The implementation act has been published in Croatia's Official Gazette no. 64/2018 and has been in force as of 26 June 2018.

The Act on the Cybersecurity of Essential Services Operators and Digital Services Providers (hereinafter referred to as "Cybersecurity Act") and bylaws have also been enacted on 4 August 2018 (the Decision on Essential Services Operators and Digital Services Providers, "the Decision").

National Strategy:

The national strategy is available at:

https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Single point of contact:

The Office of the National Security Council

National competent authorities for DSPs:

The Ministry of Economy, Entrepreneurship and Crafts is one, and the Ministry of the Sea, Transport and infrastructure is the other, relevant for air transport.

3.3.2.3 Greece

Implementation:

The NIS directive was implemented through the Decree (Ministerial) 1027/8.10.2019 and Law 4577/ 2018 (A΄ 199).

National Strategy:

The national strategy is available at:

https://diavgeia.gov.gr/doc/%CE%A84%CE%A17465%CE%A7%CE%980-%CE%966%CE%A9?inline=true

Single point of contact and competent authority for DSPs and OES:

National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)

3.3.3 The EU Cybersecurity Act

Within the frame of harmonization and standardization within EU, the Council and the European Commission have issued the Cybersecurity Act[3] which reinforces the mandate of the EU Agency for Cybersecurity, (European Union Agency for Network and Information and Security, ENISA) so as to better support Member States with tackling cybersecurity threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

According to a policy brief published by the European Commission ("The EU Cybersecurity Act - Digital Single Market - European Commission", n.d.), the EU Cybersecurity Act revamps and strengthens the EU Agency for cybersecurity (ENISA) and establishes an EU-wide cybersecurity certification framework for digital products, services and processes. The EU Cybersecurity Act grants a permanent mandate to the agency, more resources and new tasks.

In particular, ENISA will have a key role in setting up and maintaining the European cybersecurity **certification framework** by preparing the **technical ground for specific certification schemes** and informing the public on the certification schemes as well as the issued certificates through a dedicated website (Ibid.)

ENISA is also mandated to increase operational cooperation at the EU level, helping EU Member States who would request it to handle cybersecurity incidents, and supporting the coordination of the EU in case of large-scale cross borders cyber-attacks and crises. This task builds on ENISA's role as secretariat of the national Computer Security Incidents Response Teams (CSIRTs) Network, established by the Directive on security of network and information systems (NIS Directive).

Recitals 36, 37 and 38 of the NIS directive give more information on the role of ENISA:

Recital 36:

ENISA should assist the Member States and the Commission by providing expertise and advice and by facilitating the exchange of best practice. In particular, in the application of this Directive, the Commission should, and Member States should be able to, consult ENISA. To build capacity and

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

knowledge among Member States, the Cooperation Group should also serve as an instrument for the exchange of best practice, discussion of capabilities and preparedness of the Member States and, on a voluntary basis, to assist its members in evaluating national strategies on the security of network and information systems, building capacity and evaluating exercises relating to the security of network and information systems.

Recital 37:

Where appropriate, Member States should be able to use or adapt existing organisational structures or strategies when applying this Directive.

Recital 38:

The respective tasks of the Cooperation Group and of ENISA are interdependent and complementary. In general, ENISA should assist the Cooperation Group in the execution of its tasks, in line with the objective of ENISA set out in Regulation (EU) No 526/2013 of the European Parliament and the Council, namely to assist the Union institutions, bodies, offices and agencies and the Member States in implementing the policies necessary to meet the legal and regulatory requirements of network and information system security under existing and future legal acts of the Union. In particular, ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training. ENISA should also be involved in the development of guidelines for sector-specific criteria for determining the significance of the impact of an incident.

3.3.4 Standards and best practices

In an effort to harmonise practices across the EU, the European Union Agency for Cybersecurity published a report (2018) prepared to offer a collection of and comparison of all existing international standards on cybersecurity, within the various standards and regulations which exist in the various sectors to which the NIS directive applies.

The report also proposes a taxonomy of possible security checks and for the two most important documents (number 1 and number 5), a mapping is provided between this taxonomy and the controls identified by the document itself. It should be noted that this document offers different best practices and standards for the management of systems aimed at similar objectives than SATIE. This includes the security measure for “Identity and access management” at airports based on API STD 1164 and ONG-C2M2 standards. In this framework, protocols focus on **authentication and identification and access rights**, and include mechanisms such as user accounts, password controls, multi-factor authentication and biometrics (European Union Agency for Cybersecurity, 2018), which are already addressed or improved by the SATIE toolkit.

The following standards and best practices were included in the report:

Standards:

- ICAO Aviation Security Manual - Document 8973 (Restricted Access)

- ARINC 811 Commercial aircraft information security concepts of operations and process framework
- EUROCAE ED-201 – 204 Aeronautical Information System Security (AISS) Framework
- RTCA DO-326 Airworthiness security process specifications

Best practices:

- AIAA (The American Institute of Aeronautics and Astronautics) The Connectivity Challenge: Protecting Critical Assets in a Networked World
- Information Security Certification and Accreditation (C&A) Handbook – FAA
- FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorized External Access
- FAA Aircraft systems information security protection overview

3.4 Airports management and security control

Besides the data protection regulation and the NIS Directive, there are a series of legal provisions on airport management and security controls that are directly applicable to SATIE objectives and governance. In particular, the norms and standards on the communication of passengers data among the involved stakeholders (carriers, airlines, airport operators and public authorities), those concerning security in baggage handling and around staff identify authentication must be considered.

3.4.1 Council Directive 2004/82/EC on the obligation of carriers to communicate passenger data

As part of T4.4, a system will be developed in order to transfer API data provided by airport carriers to the national authorities. Airport carriers have the obligation to send API to the authorities of where the aircraft land, it is thus in this sense that SATIE provides an innovative element: it enables national authorities on the departure side to verify that the passengers are not persons of interest.

The Council Directive 2004/82/EC aims at establishing an obligation for carriers to transfer advanced passenger data to the competent authorities as it is laid down in its Article 1.

Article 1:

This Directive aims at improving border controls and combating illegal immigration by the transmission of advance passenger data by carriers to the competent national authorities.

Article 3 of the directive establishes that member states shall be responsible for putting in place measures aimed towards guaranteeing that **air carriers[4] transmit information on passengers who are going to enter the territory of a member state**. It also accounts for the specific information that needs to be transmitted.

Article 3:

1. Member States shall take the necessary steps to establish an obligation for carriers to

[4] Air carriers are defined in Article 2 of the Directive as "any natural or legal person whose occupation it is to provide passenger transport by air"

transmit at the request of the authorities responsible for carrying out checks on persons at external borders, by the end of check-in, information concerning the passengers they will carry to an authorised border crossing point through which these persons will enter the territory of a Member State.

2. The information referred to above shall comprise:
    - 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.
3. In any case the transmission of the above mentioned data does not discharge the obligations and responsibilities laid down in the provisions of Article 26 of the Schengen Convention for carriers, as supplemented by Directive 2001/51/EC.

Article 6 of the Directive establishes the basis for the processing (combating illegal immigration more effectively and law enforcement purposes) and a **very brief data retention period that is in alignment with the principle of storage limitation** and that contributes to minimise data protection issues related to the storage of data.

Article 6:

1. The personal data referred to in Article 3(1) shall be communicated to the authorities responsible for carrying out checks on persons at external borders through which the passenger will enter the territory of a Member State, for the purpose of facilitating the performance of such checks with the objective of combating illegal immigration more effectively.

    Member States shall ensure that these data are collected by the carriers and transmitted electronically or, in case of failure, by any other appropriate means to the authorities responsible for carrying out border checks at the authorised border crossing point through which the passenger will enter the territory of a Member State. The authorities responsible for carrying out checks on persons at external borders shall save the data in a temporary file.

    After passengers have entered, these authorities shall delete the data, within 24 hours after transmission, unless the data are needed later for the purposes of exercising the statutory functions of the authorities responsible for carrying out checks on persons at external borders in accordance with national law and subject to data protection provisions under Directive 95/ 46/EC.

    Member States shall take the necessary measures to oblige carriers to delete, within 24 hours of the arrival of the means of transportation pursuant to Article 3(1), the personal data they have collected and transmitted to the border authorities for the purposes of this Directive.

    In accordance with their national law and subject to data protection provisions under Directive 95/46/EC, Member States may also use the personal data referred to in Article 3(1) for law enforcement purposes.

> 2. Member States shall take the necessary measures to oblige the carriers to inform the passengers in accordance with the provisions laid down in Directive 95/46/EC. This shall also comprise the information referred to in Article 10(c) and Article 11(1)(c) of Directive 95/46/EC.

Last, the implementation of this obligation is carried out within the European Union through the Advanced Passenger Information System (APIS), which is discussed in the next section.

3.4.2 Advance Passenger Information System (APIS)

The authorities of some countries require that the airlines communicate the personal data of the passengers, before they check in. Otherwise they will be unable to fly. The Advance Passenger Information System (APIS) is an **electronic data interchange system that allows commercial airlines, vessel operators and public administrations exchanging a set of passengers' data elements**. These include full name (last name, first name, middle name if applicable); gender; date of birth; nationality; country of residence; travel document type (normally passport) and travel document number (expiry date and country of issue for passport).[5] This information should be shared following the specifications for UN/EDIFACT Passenger List Message (PAXLST) formats.

Existing guidelines (WCO/IATA/ICAO, 2014) provide certain criteria to implement the API system which gives Border Control Agencies access to personal data belonging to passengers. These data had been collected by airlines in a swifter manner, as it said in point 9.1 of the guidelines:

> **9.1**
>
> Generally speaking, API provides Border Control Agencies with data they could otherwise access upon the passenger's arrival and presentation at an immigration inspection desk. API data simply provides data at an earlier time and through different means with the aim of expediting the passengers' clearance.

The guidelines account for the appearance of new privacy and data protection legislation around the globe, like the GDPR.

> **9.3**
>
> Privacy and data protection legislation has been enacted in many countries in recent years in order to protect the individual's right to privacy and to allow individuals to exercise their rights relating to the use of their personal data.

The guidelines do not establish any particular ways to comply with the regulation. Instead, they indicate that it is the responsibility of member states.

> **9.7**

[5] In addition to these data, the US authorities require that passengers traveling to / from or via the United States notify them the data of the "Green Card", if applicable, country of residence and to the people whose destination is the United States, the address in the country.

Because of the differences in the provisions and interpretation of privacy and data protection laws from country to country, carriers required to participate in API should enquire on a case-by-case basis whether the capture, storage and transmission of the passenger details mentioned in this Guideline is in contravention of applicable national law. Where such contravention is determined, the country requiring the API data should, to the best of its abilities, seek to address and resolve those legal concerns.

This means that, in any case, it falls out of the scope of the SATIE project to guarantee that the system meets the requirements and standards set out by the GDPR. It is thus understood that, if this system is in operation in the European Union it is because its level of compliance with the GDPR has been judged acceptable. **Nevertheless, the way in which API data could interact with the various innovative elements in SATIE will be the object of an analysis from a privacy standpoint in D8.4.**

3.4.3 Regulation (EC) No 300/2008

Regulation (EC) No 300/2008 of the European Parliament and the Council sets out rules concerning minimum security standards in civil aviation across Europe. The objectives of this regulation are established in its Article 1.1.

Article 1.1

This Regulation establishes common rules to protect civil aviation against acts of unlawful interference that jeopardise the security of civil aviation.

It also provides the basis for a common interpretation of Annex 17 to the Chicago Convention on International Civil Aviation.

The scope of the regulation includes airports as established in Article 2.1.

Article 2.1:

This Regulation shall apply to the following:

(a) <u>all airports</u> or parts of airports located in the territory of a Member State <u>that are not exclusively used for military purposes;</u>

(b) all operators, including air carriers, providing services at airports referred to in point (a);

(c) all entities applying aviation security standards that operate from premises located inside or outside airport premises and provide goods and/or services to or through airports referred to in point (a).

In this case, the regulation establishes specific security measures that are laid down in the Annex.

Article 4.1:

1. The common basic standards for safeguarding civil aviation against acts of unlawful interference that jeopardise the security of civil aviation shall be as laid down in the Annex.

As for who is responsible for ensuring compliance, Article 4.5 of the regulation establishes that the member states are the ones responsible for ensuring that the stakeholder mentioned in Article 2.1 of the regulation put in place the common basic standards laid down in the Annexes.

Article 4.5:

Member States shall ensure the application in their territory of the common basic standards referred to in paragraph 1. Where a Member State has reason to believe that the level of aviation security has been compromised through a security breach, it shall ensure that appropriate and prompt action is taken to rectify that breach and ensure the continuing security of civil aviation.

The main security measures that the regulation establishes in the Annex and that concern SATIE are those that have to do with the control of restricted areas and the management of hold baggage. The following sections of the Annex are relevant in this context:

Annex 1.2.2:

Access to security restricted areas shall be controlled in order to ensure that no unauthorised persons and vehicles enter these areas.

Annex 5.3:

1. Each item of hold baggage shall be identified as accompanied or unaccompanied.

2. Unaccompanied hold baggage shall not be transported, unless that baggage has been either separated due to factors beyond the passenger's control or subjected to appropriate security controls.

As for the control of restricted areas, it has been said that T3.3 will create a system aimed at controlling access into a restricted area, making automated decisions (allowing or denying entry into the restricted area) on the basis of a facial recognition system that matches the biometric features of the individuals attempting to get through with a database storing biometric information belonging to the authorised individuals. **The development of this innovative element constitutes an attempt to create a system that is able to allow airports to provide more effective ways of complying with this regulation**.

Regarding hold baggage management, T4.4 involves the creation of a system that links MRZ data of passengers with their baggage. This system allows for the classification of baggage into the two categories established in Annex 5.3, namely accompanied and unaccompanied. It also makes it more accurate and reliable. Therefore, T4.4 can also be seen as an attempt to improve security at airports.

4 National case studies

After a presentation of the various laws applicable to airports in terms of cybersecurity and data protection, the section below looks into individual case studies, to see the effects those regulations had on individual airports in different countries, and where a certain level of harmonization in terms of security levels and measures was reached. To this effect, the implementation of these laws in the Milan Malpensa Airport and Athens International Airport is delved into.

For all intended purposes, the roles SEA and AIA define are written with capital letters.

4.1 Milan Malpensa airport

4.1.1 GDPR

The EU regulation 2016/679 (GDPR), which repeals directive 95/46 / EC (general regulation on data protection) entered into force in Italy on 19 September 2018 and the regulation on privacy is governed by the Italian legislator with the Legislative Decree n. 51 of 18.05.18 and n. 101 of 10.08. 2018.

With specific reference to the SEA Group (SEA), it is useful here to remind some general information on the company policy and on corporate compliance in terms of discipline and data protection. It should be underlined that starting from the date of applicability of the GDPR, i.e.: starting from as early as 25 May 2018, SEA was already in line with the minimum principles and obligations required by the law that came into force on that date by developing an ad hoc project called “Europrivacy” (“Project ").

The Project was developed in three phases, namely, (i) a preliminary assessment phase, aimed at identifying the processing of existing personal data, the subjects and the company functions involved as well as the procedures for managing the different types of personal data processing, (ii) a gap analysis, aimed at identifying the existing criticalities in terms of compliance with the GDPR, finally, (iii) an action plan, aimed at defining the course of actions for the resolution of the identified problems.

During the Project the need to appoint a subject delegated by the data controller (SEA) for the management in the name and on behalf of the Owner of the obligations and obligations in this regard (the "Delegated Person"), has emerged. Otherwise, in fact, the management would have remained entirely in the hands of the Board of Directors, as SEA is the Data Controller.

4.1.1.1 Fulfilled actions

The activities carried out so far for the purposes of privacy compliance are listed below.

- Analysis of the existing relationships between SEA and the Supervisory Body / Ethics Committee and Anti-corruption Representative Body, definition of the privacy roles that the parties hold in the performance of their activities;
- Analysis of the processes related to the treatment of personal data as to the activity performed by SEA through the first aid services, available in SEA’s managed Airports (Malpensa Terminal 1 and Malpensa Terminal 2 + Linate Airport) and updating of the privacy documentation related to these services;

- Analysis of existing relationships with the occupational physician (“Medico competente”) and updating of the privacy documentation related to these relationships;
- Analysis of the commercial relationships between SEA and third parties to assess the privacy compliance with reference to the execution of contractual relationships;
- Implementation of new privacy policies dedicated to SEA’s employees: in particular, the SEA’s employees privacy policy and the privacy policy to be included in the procurement and subcontracting agreements and that the contractor / subcontractor must submit to its own personnel in the name of SEA;
- Implementation of different models of privacy clauses that can be employed in contracts subscribed by SEA with third parties;
- Analysis of privacy issues related to the video surveillance system (including the part relating to video cameras used by public authorities) and adoption of appropriate documentation in accordance with the GDPR;
- Adoption of a "privacy manual" containing the indication of the most appropriate practices and behaviors that SEA employees must adopt during the performance of their duties;
- Design of procedures to appropriately treat privacy issues, such as: data breach, impact assessment (DPIA), management of the requests of the interested parties for the exercise of their respective rights and identification of privacy qualifications (e.g.: Owner / Co-owner / Data Processors).

With particular reference to the last point, in relation to the SATIE project, an impact assessment and an evaluation of risks (DPIA) related to the treatment of personal data will be carried out.

4.1.1.2 Training

In the first months of 2019 a training program was also started. The activities related to the training program are based on the criteria listed below:

- Classroom training for those categories of corporate subjects who, by role or function, hold an important position for privacy purposes;
- Specific technical-legal training for members of the Legal department who, in turn, will be required to provide internal legal consultancy advices;
- Massive training for the rest of the company population to be carried out using a specific IT tool or paper material.

In accordance with the above criteria, the following activities were carried out:

- Two specific training sessions for company directors, or in any case top managers, who had previously been identified as "Persons in Charge with Responsibility", and managing specifically assigned registers for the treatment of personal data;
- Two specific training sessions with the "Focal points", identified by each Person in Charge with Responsibility as subjects delegated to manage, manually and operationally, the updating of the Register and the treatment of personal data related to specific activities “Registro dei Trattamenti”, as well as other privacy issues and/or doubts that may arise within their area;
- Two specific training sessions for System Administrators;
- One specific training session for members of the Legal Affairs department.

The training program provides further training sessions for additional subjects that the various company departments will identify and report as deserving ad hoc courses.

4.1.1.3 IT Tool

The Data Protection Officer and the ICT Department are studying the implementation of a specific IT tool that, following market scouting, has been identified in PrivacyLab. This tool is being fine-tuned and, above all, tailored to the concrete needs of the companies.

This tool, once implemented, will be able to:

- Guarantee an efficient management of formal appointments for privacy purposes;
- Provide the automatic update of the privacy information to all employees, as well as request their consent when required by the law;
- Act as an archiving tool for all official documents as well as communications at a privacy level, even with third parties;
- Guarantee real-time management of the “Registro dei Trattamenti”;

SEA is considering using the tool for the extensive training of personnel in privacy matters, since the same is equipped with a customizable course that can be accessed by all employees.

4.1.2 Report on the compliance status of the NIS Directive (Legislative Decree 65/2018) inside SEA’s Group

On 6 July 2016, the European Union approved the EU Directive on network and information security known as the NIS Directive ("Network and Information Security").

Italy has implemented the Directive, incorporating it into national law with Legislative Decree n. 65 of May 18, 2018, published in the Official Journal n. 132 of June 9, 2018.

The implementing decree (with reference to Article 14 of the Directive) requires the adoption of technical-organizational measures functional to the management of risks and the prevention of IT incidents aimed at ensuring the continuity of the services provided.

More in detail, as to the risk management, organizations have to:

- Identify and analyze the risks on the ICT infrastructures / services;
- Adopt adequate technical and organizational measures to manage these risks.

As to incident management, organizations have to:

- Guarantee the continuity and resilience of essential services;
- Minimize the impact on IT systems supporting these services in the event of a security incident;
- Guarantee, without undue delay, adequate notification and communication mechanisms to the Computer Security Incident Response Team (CSIRT) in the event of IT incidents.

The Ministry of Transport guidelines are to be applied in a time range starting from September 2019 until April 2020.

Anyway, there are some actions to be completed almost immediately:

- Identification of the internal organizational structure responsible for implementing the NIS compliance requirements;

- Designation of NIS Referent and communication of its name and contacts;
- Adoption of organizational measures to ensure mandatory notification requirements;
- generation of a pair of keys (public / private) in accordance with the OpenPGP standard, with RSA encryption (4096 bits) and subsequent transmission of the public key to the NIS authority;
- Adoption of a minimum security organization suitable for the treatment of classified information at the RESTRICTED level, with the possibility of appointing the security representatives;
- Adoption of physical and CIS security measures and subsequent submission of the declaration for the use of the isolated CIS station;
- Provision of safety education for all those who need access to classified information (DPCM n.5 / 2015).

4.1.3 Security measures /Reference framework

The Department for Information and Security has adopted the National Framework for Cybersecurity and Data Protection. This provides an operational tool for the application of compliance obligations under the NIS Directive and GDPR Regulation. The Framework is visualized in Figure 4.1 and consists of the five elements:

Figure 4.1: National Security Framework

- IDENTIFY - Understanding of the business context, of the assets that support critical business processes and the associated risks. This understanding allows an organization to allocate resources and define investments in accordance with the risk management strategy and with company objectives.
- PROTECT - Definition and implementation of measures aimed at protecting business processes and company assets, regardless of their IT nature.
- DETECT - Definition and implementation of the appropriate activities aimed at identifying IT security incidents in a timely manner.
- RESPOND - Definition and implementation of the appropriate activities to be carried out when an IT security incident has been detected, in order to contain its potential impact
- RECOVER - Definition and implementation of the appropriate activities for the management of plans and actions to restore processes and services impacted by an IT incident. The objective is to guarantee the resilience of systems and infrastructures and support the timely recovery of business operations

4.1.4 ISO 27001 / ISRM (Information Security Risk Management)

For the purposes of the SATIE project, it should also be noted that SEA is in the process of obtaining ISO 27001 certification.

The scope of this certification is to apply a control framework for aspects related to physical security, logic and IT governance, designed to verify the state of exposure to harmful and significant risks to the confidentiality, availability and integrity of the company's information assets.

To cope with the complexity and dynamism of the threat scenario, the regulation in object (IT ISO 27001) requires the design of a single reference process, which must be supported by a set of global policies and procedures.

The model refers to the field of IT security risks, enabling the interception of emerging internal and external threats and supporting the growth of "proactive" behaviours, instead of "reactive" approaches, which are less and less effective and, on top of that, not sufficient.

To comply with the set objectives and with the ISO 27001 standards, the operational "roadmap" entails the following phases:

1. IT Security Risk Assessment (aimed at identifying the real level of risk exposure and the consequent identification of the controls necessary for its mitigation);
2. Business Impact Analysis (to ensure that the measures to protect the threats are in line with the mission, the objectives, the legal obligations specific for any given area. It allows the company to focus on the most critical business processes);
3. Risk Assessment and management (considering the results of the Business Impact Analysis, possible threats and appropriate controls to neutralize them, the gap between the necessary controls and the ones in use).

Below is a list of the controls subject to assessment in SEA’s "IT Securization" plan, organized according to the ISO 27001 model, to be included in the "information security management system" (ISMS):

- Security Program
- Organization of security
- Security Policy
- Risk Management
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Business Continuity Management
- Security Incident Management
- Compliance and improvements
- Malicious software protection
- Cryptography & Key Management
- Capacity Management
- Software control
- Host Access Control
- Network Architecture
- Firewall
- Specific network services

- Data transmission security
- Wireless security
- Network Access Control
- Periodic verification of the policies and procedures application
- Verification of the access policies and of the compliance with Segregation of Duties (SOD) principles
- Annual Vulnerability Assessment Plan
- Penetration periodic and spot tests

4.2 Athens International Airport

AIA has taken into account the following laws, to the extent that those are applicable to its operations:

- The EU Directive 2016/1148 (NIS Directive) as transposed into the Hellenic legal system by law 4577/2018 and accompanying Ministerial Decisions;
- General Data Protection Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, including its national adaptation Law 4624/2019;
- Directive EU 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data
- EU Directive 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime
- E-Privacy EU Directive of 2009 on the processing of personal data in publicly available public e-communications networks and EC legislative proposal for the new e-Privacy Regulation
- The Airport Development Agreement (ADA) signed on July 31st, 1995, as ratified by the Hellenic Republic by Law 2338/1995 (Government Gazette A’ 202/14.9.1995)
- Opinions and Guidelines, as issued by the European Data Protection Board (formerly “WP 29”) or the Hellenic data Protection Authority
- ISO / IEC 29100 on Information Technology – Security Techniques – Privacy Framework.

On August 27th 2018, the Greek Parliament passed a national legislation supplementing the EU General Data Protection Regulation. Under Law 4624/2019, the Greek Supervisory Authority has been re-established, provisions of the GDPR were supplemented by additional measures and provisions of Directive (EU) 2016/680 were transposed into Greek law. The law repeals the prior Law 2472/1997 excluding certain provisions regarding the public disclosure of a suspect’s data by law enforcement authorities in case of specific offenses, the use of closed-circuit TV material from public gatherings and the opt-out register for commercial communications by mail.

The development of the required roadmap to achieve compliance for GDPR was approved by AIA’s Board of Executives and Board of Directors in Q3 2017. For this process AIA has employed subject matter experts and the assistance of contracted external consultancy firms, to provide the required guidance for the development of a comprehensive program that spans through many organizational units within AIA.

Athens International Airport S.A. (AIA) GDPR Compliance Facts:

- AIA, prior to the GDPR effective May 25th 2018, implemented the appropriate technical, organizational measures and controls, as well as fulfilled accompanying legal requirements to demonstrate its compliance with GDPR.
- Our compliance maturity was assessed by an independent auditing firm within the period of September - October 2018, validating an adequate level of privacy compliance in AIA's data governance model.
- As regulatory compliance is an ongoing process, AIA reviews and enhances its personal data protection framework, adapting to new processes and guidelines issued on the subject matter by the European Data Protection Board, the Hellenic Data Protection Authority, or other competent bodies.

4.2.1 Organizational controls

In brief, AIA's organizational controls comprise a Personal Data Protection Management System (PDPMS), which is rational and proportional to its activities and to the nature of aviation industry and was formally adopted prior to the enforcement date of the General Data Protection Regulation in 2018. This system includes:

- Corporate policy, manual and procedures, with assigned accountabilities for Management and employees, duly integrated into the corporate business process management;
- Corporate data registry and privacy impact assessment methodology and performance (risk assessment) aiming to protect the rights and freedoms of individuals;
- Employee training and awareness, guidelines to Airport stakeholders and information bulletins to the other business partners
- Proper information provision to the public and mechanism for supporting data subjects in the exercise of their respective GDPR rights
- Incorporation of data processing requirements within all processes, as well as all new and existing contracts with other Data Controllers, or Data Processors respectively;
- The implementation of appropriate technical security controls, ensuring data availability, integrity and confidentiality.

The documents serve AIA's purposes for demonstrating accountability and compliance with GDPR provisions within the entire lifecycle of personal data, while enhancing confidence and fostering high-trust relationships with all stakeholders.

Major concluded actions within AIA:

- Updated Procedural Documentation,
- Issuance of Privacy Notices available to the public for all processing activities,
- Around 70 Data Privacy Impact Assessments (DPIAs), consisting of remediation actions to mitigate inherent privacy risk,
- Contract templates consisting privacy clauses - GDPR terms in AIA's existing contracts – Data Processing Agreements for related partnerships and AIA's Joint Controllers and/ or Data Processors,
- New documents for Cross-Border Data Transfer Management and Third-Party Partnerships Assessment Criteria
- Data Subjects Rights Handling
- GDPR training & awareness courses within AIA and Guidelines to Airport Stakeholders through corporate extranet
- Information security awareness session

- Inclusion of data privacy incidents in the information security incidents registry
- Technical security measures for corporate databases (data masking, encryption, USB blocking)

Next steps:

- Issuance of a Self-Assessment Review Plan for 2020
- Distribution of Third–Party processors compliance Questionnaire
- Review Information Security Policies and Procedures under the light of NIS compliance and ISO 27000 certification

4.2.2 Readiness review

Following the 6-month enforcement period of the Regulation, AIA's Management decided to assess the corporate compliance status. The Readiness Review was performed against GDPR provisions, as well as the guidelines of Article 29 Data Protection Working Party (currently European Data Protection Board), so as to evaluate the compliance level of AIA concerning the protection of natural persons in the context of personal data processing. More specifically, the evaluation included the review of the following areas of personal data protection:

1. Privacy Management and Governance Model (organizational structure, data protection strategy)
2. Data Protection Framework (data protection policy and supporting procedures)
3. Data Governance (data architecture, data classification, data retention and secure disposal)
4. GDPR Operations (record of processing activities maintenance, conduction of DPIAs, data breach incident handling, compliance assessment mechanisms)
5. Training and Awareness (data protection training program and supporting awareness material for data subjects and third parties)
6. Legal Processes (contract templates, consent statements, data privacy notices)
7. Third Party Management (contract templates with data processors, joint controllers and vendors, third party data protection assessment mechanisms)
8. Data Transfer (cross-border data transfer handling and related safeguards)
9. GDPR IT and Information Security Controls (implemented information security measures, access management, back-up, information security risk assessment)

4.2.3 IT Infrastructure (technical and security controls)

Through the gap analysis process the areas for the implementation of technical controls for AIA's IT&T where identified and the assessment of the most applicable IT controls was evaluated. The outcome of this process led to the implementation of several IT controls through the use of necessary technologies.

More respectively the following controls are implemented or are in a completion phase:

- Encryption of data – Encryption of Data at rest and Data in motion for all systems that have been identified through DPIA's to contain and exchange personal data, has taken place. File storages and databases that contain such data have been encrypted and the network access and interchange of data takes place only in encrypted format.
- Encrypt Laptops – As many of the data leakages occur through the loss or theft of employee laptops, we have encrypted all company so as to minimize the possibility of a personal data leakage.

- USB Blocking – In order to prevent the uncontrolled sharing of data through USB sharing, AIA has imposed a strict policy towards the use of USBs on corporate desktops and laptops. USB usage is prevented from AIA personnel apart from a small number of authorized and appointed users. For those appointed users', special encryption and PIN enabled high security USB dongles have been allocated. In the event of loss of such a USB dongle, the information contained in it are not accessible.
- Filesharing Blocking – Access to filesharing internet sites such as Gmail, Dropbox etc. has been blocked through the corporate firewall, in an effort to minimize the risk of uncontrolled data sharing from the corporate file servers or desktop and laptop equipment.
- Corporate Mobile Device Management – Similar to the case of laptops, the loss or theft of corporate mobile phones and tablets can lead to the leakage of personal data. Through Mobile Device Management the corporate data on these mobile devices are wiped and the access to corporate emails and files is blocked, in the event of a loss or theft of the respective device.
- Office 365 GDPR Advanced Threat Protection Controls – AIA's Information Technology and Telecommunication has activated Office 365 Advanced Threat Protection, with a focus on mitigating content phishing, domain spoofing, and impersonation campaigns to AIA's email service, network, users and file storages. Office 365 Advanced Threat Protection is also expanded to help secure SharePoint Online, OneDrive for business, and Teams that is used as AIA's official files sharing tools.
- Airport Passenger Internet Access – Technical modifications to the internet access mechanism for airport users so as not to collect personal information anymore and provide access in a GDPR compliant manner
- Corporate Website – technical modification to minimize the required use of personal data to only the absolute necessary cases such as passenger complaint handling etc.

As the compliance to the GDPR directive is an ongoing process, additional initiatives such as the evaluation of supplementary IT infrastructure tools and controls, such as Holistic Corporate Encryption Solutions and Security Information Event Management software suites, is currently in progress.

4.2.4 NIS Framework

The NIS Directive (EU 2016/1148) defines critical infrastructures and services that if disrupted it is expected to have a significant impact on the proper functioning of the state apparatus and on the lives of citizens. Airports have been classified under the NIS framework form ENISA as critical infrastructures - under the transportation sector - and appropriate information security measures, tools and processes need to be introduced so at to protect them from information security incidents. Greece has recently (Oct. 2019) provided the Ministerial decision to proceed to the definition of critical cyber security infrastructures and services. This decision authorizes the National Cyber Security Authority to design and define the requirements for implementing a Single Security Policy.

The Directive and, consequently, the Ministerial Decision concern the declaration of the essential security requirements of network and information systems and the process of providing information and reporting security incidents to the competent Authorities. The essential security requirements, as defined by the Ministerial Decision, are divided into the categories of Identification, Prevention and Mitigation. The first category requirements are necessary to understand the business context, the resources that support key services, and the relative risk to the security of network and information systems and allow the Agency to focus its efforts and manage its resources, by effective and efficient way. In the Prevention category, measures must be defined to ensure that all the involved resources (people, processes and technologies) that support the core services of the Organization are met. The measures selected to meet the requirements of this category should take into account the risk management strategy. The third category refers to Mitigation, thus, to measures required for the detection, response, and overall management of a security event that may affect the provision of key airport services. At the same time, this category promotes the reduction of the impact of a security incident, by ensuring the continuity and restoration of the provision of basic Airports services at an acceptable and predetermined level.

Currently AIA is in coordination with the National Cyber Security Authority to formally proceed with the announcement of the airport as a critical infrastructure and proceed to the definition of expected actions towards achieving compliance with the NIS Directive. One of the actions anticipated is the adoption of an ISO 27001 certification initiative for the airport among other measures. As this is currently an ongoing process a definitive program is expected to be officially presented by AIA within the year 2020.

5 Summary analysis and recommendations

This deliverable establishes the legal state of the art for the SATIE toolkit. This legal framing and analysis is focused on the two main domains addressed by the SATIE toolkit: 1) the identification and authentication of airports' staff and passengers, and 2) threat detection. These tasks are mainly based on three different functionalities of the SATIE toolkit, which allow the system to assess the stress level of ATCOs as they carry out their duties, authenticate the identity of airports' staff so access to restricted areas can be monitored, and link passengers' baggage with their identity, in the case the baggage has lost its tag. The SATIE project is aimed at developing these and other subsystems in a way that they can be deployed and administered by the airport -public or private- operators. When doing this, these organizations will act as data controllers and establish collaboration with other stakeholders, for instance, by exchanging data with air companies or notifying local police authorities about identified threats or anomalies.

Taking the above into account, four legal frameworks have been addressed in this document: human rights, data protection, cybersecurity, and airport management regulations. Concerning human rights, SATIE does not pose significant issues, as it is not a personal data heavy project, nor is it intrusive for the members of the staff or passengers involved. Still, the SATIE subsystems will need to process special categories of data, including facial and voice identifiers of staff members. In terms of the rights to integrity and no discrimination, the main issues in this context relate to the potentiality of some of the SATIE functionalities for producing false positives or biased automated decisions. Still, the impact that alerts or anomalies detected by the system may have over the integrity of airport's staff or passengers is low, since related notifications work only as support for the airports security management. Moreover, the classification of a piece of baggage as a security risk must be supported by the identification of its owner, which can only conduct to a secondary assessment by using MRZ data. Concerning the use of verifying ATCOs as speakers and identity authentication for airport staff, these procedures also entail minor risks in terms of human rights, since they will be an added element to the set of identification systems already implemented at airports with the same purpose. In brief, beyond the potential misuse of collected data, the system does not involve major risks for human rights. In fact, if managed following the security standards reflected in the documents below, it will contribute to the safety of passengers and airport staff by detecting threats and anomalies at airports.

Regarding data protection, the systems which require the use of personal data are the access control (T3.3 and T6.5), the Advanced Passenger Identity (T4.4 and T6.3) and the TraMICS (T4.2 and T6.2) systems. The legal analysis on data protection for each of these systems is summarized below:

- Firstly, as already mentioned, the access control system uses face recognition to authenticate staff seeking to enter restricted areas, and essentially works in the same way as staff access cards. The facial recognition ensures a higher level of security than the access cards, as these can be lost or stolen, and mean staff need not worry about having forgotten or misplaced their card. TraMICS purports to use biometrics to verify that the speaker is authorized, or vise versa, detect an unauthorized speaker.
- Secondly, the stress detection within TraMICS is not meant to evaluate the ATCO's performance at work, but to detect a potential security issue, implying that this person would not be coerced and its privacy not affected in a significant manner. Voice identifiers used for threat detection by analysing stress level do not have a high enough precision to ensure personal identification and can be framed under the concept of public interest in the GDPR (Art. 6) and backed up by other legal provisions, including the NIS or the Police Directives.

The above two cases are covered by Art. 6 (b) GDPR, which allows airports to collect and process personal data based on the performance of a contract. As already explained in this document, this use of biometrics is allowed by Art. 9 of the GDPR under consent and public interest basis and by implementing special safeguards in its treatment. In this way there are many legal bases on which SATIE can process airport staff's personal information

- Thirdly, the main privacy risks relate to the processing of passengers' personal data. MRZ data will be matched with baggage identifications. The Advanced Passenger Identity includes an innovative solution which transfers the API data to national authorities of the departure airport, which is similar to a requirement imposed by the Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data[6] to destination airports. Even though this use of personal data with identity verification and security purposes may be framed in public interest (Art 6 GDPR), the management of such functionality by airport operators must follow the security standards for data protection posed by the GDPR and the NIS directive. In this line, the MRZ data will only be processed with the photo taken of the baggage during check-in for those cases when a baggage has lost its tag. Both the MRZ data and API data are stored temporarily in databases subject to access control and deleted after a short period of time (this time-frame has not been determined yet, but the idea is until the plane lands at the destination airport). These security mechanisms, jointly with the Privacy Impact Assessment carried out in D9.10 ensures a sufficient level of data protection.

Overall, the system is compliant with the requirements posed by the GDPR on purpose limitation, data minimization and security. In particular, the anonymization techniques reflected in D9.7 will play a key role in minimizing such risks. Moreover, SATIE does not pose major threats concerning data protection even though some of its subsystems use biometric data. Still, the issue of consent, analysed in the context of the identification of the legal basis for processing in D9.8, requires special attention. In this sense, in order to implement SATIE, airport operators acting as data controllers will also have to ensure that personal data processed by those processors processing the data on their behalf apply the security and data protection standards established in a contract or legal act. These documents must clearly reflect the duties of the data processor towards the data controller, which must be aligned with the GDPR requirements and reflected in the consent form/ contract signed by data subjects or other binding documents such as Privacy Policies.

Concerning the cybersecurity regulations, SATIE provides further mechanisms and technologies to ensure compliance with the NIS directive and the cybersecurity standards applied by airport operators. Actually, it seeks to advance in the implementation of the cybersecurity regulation and existing security standards. Along these lines, the NIS directive fosters the assessment of risk management systems and the adoption of adequate technical and organizational measures to manage these risks. Moreover, one of the functionalities of these systems must be the efficient notification and communication of possible incidents occurred at airports. As reflected in the described case studies, airports have already adopted data protection measures and protocols to respond to the legal requirements posed by the GDPR and the NIS Directive. Compliance with these standards already represents a baseline for the integration of the SATIE toolkit which, jointly with its privacy by design approach, should facilitate the alignment of airports with the above discussed legal provisions. Measures or actions conducted in this framework include the establishment of security mechanisms for data communication (such as encryption in the Milan airport), general data governance activities (such as the new identity verification systems proposed by SATIE) or the

[6] It should be noted that these data is processed by the Smart API data analysis system to query the passengers against the Government watch lists ("screening"), prior to the arrival of the plane.

establishment of technological and procedural basis for reaching ISO 27001 concerning cyber security.

Lastly, concerning those legal provisions regulating airport security and management which have concrete implications for SATIE, two main aspects need to be considered. On the one hand, API standards imply that data processed by this system in the European Union must follow the GDPR, which we have considered it does. On the other hand, SATIE also favours the enhancing of security mechanisms for monitoring airports' restricted areas, ensuring compliance with the Regulation (EC) No 300/2008 on security standards in civil aviation across Europe as well as the ISO standards in the field. In fact, SATIE will provide new functionalities for ensuring a secure baggage handling at airports ensuring the correct classification of baggage into the two categories established in Annex 5.3 of Regulation (EC) No 300/2008, namely accompanied and unaccompanied.

5.1 Legal recommendation for the SATIE systems

The following table sets the legal requirements detailed above into relevant recommendations for the design and deployment of the SATIE toolkit.

Table 5.1: Summary of the legal recommendation for the SATIE systems

Field	Regulation/Guidelines	Recommendations
Human rights	Various: • Charter of Fundamental Rights of the European Union. • European Convention on Human Rights. • Universal Declaration of Human Rights.	• Ensure that machine learning systems and database interoperability do not have discriminatory effects . • Ensure that the speaker verification system does not affect the right to integrity. • Prevent false positives. • Conduct an analysis of proportionality and trade-offs between privacy rights of passengers and airport staff and their rights to security.
Data protection	General Data Protection Regulation	• Anonymise or pseudonymise data whenever possible. • Clearly identify where sensitive personal data will be processed and to put in place special security measures for their processing. • Avoid collecting biometrics as far as possible (data minimization). • Clearly establish who are the controllers and processors in order to ensure accountability, especially in the context of research. • Determine the instruments through which controllers and processors are to establish their relationship. • Keep records of data processing activities. • Adopt a storage period that is reasonable

Field	Regulation/Guidelines	Recommendations
		in relation to the purposes of the processing. • Embed the principle of privacy by design into the development of the SATIE outcomes. • Establish safeguards directed at protecting the rights and freedoms of those employees who will undergo facial recognition (like including human intervention). • Respect the anonymization techniques and processes reflected in D9.7. This will allow the system to comply with the GDPR principles detailed above, including the principle of purpose limitation. • Develop matching systems which allow the removal of personal data from databases as soon as possible. • Conducting an Algorithmic Impact Assessment if algorithms with the potential to produce discriminatory outcomes will be developed within SATIE. • Integrating a protocol for personal data breaches, be it into the SATIE system or into the internal guidelines of airports. • Carry out training activities on data protection and security activities around the SATIE system (as implemented in Milan airport). • Update security systems to be GDPR compliant. • Delete data that is no longer relevant. • Revise contracts with third parties to make sure they are GDPR compliant, if need be, ask them to complete an audit. • Make sure there are processes in place to notify both public authorities and data subjects in case of data breach. • Set up a register of data breaches. • Update privacy policies.
Airports management and security control	Council Directive 2004/82/EC	No direct legal implications for the project.
	Guidelines on Advance Passenger Information (API)	No direct legal implications for the project. The societal impact of interoperability will be examined in D8.4..
	Directive EU 2016/681 of the European Parliament and of	No direct legal implications for the project. The societal impact of interoperability will be

Field	Regulation/Guidelines	Recommendations
	the Council	examined in D8.4.
Other	Regulation (EC) 300/2008	SATIE can be seen as an attempt to better comply with these standards.

5.2 Recommendations for the SATIE validation activities

WP6 consists in validating the various elements developed in the other WPs and validating those at airports during demonstrations. WP6 consists in the following tasks:

- T6.1: Integration on the simulation platform of the partners' solutions.
- T6.2: Test, verification and validation of the SATIE solution with every threat scenario. DLR will test and validate TraMICS in that task.
- T6.3: Integration and demonstration in Zagreb airport. This demonstration puts in operational conditions the baggage handling system.
- T6.4: Integration and demonstration in Athens airport. The focus of this demonstration are cyber-physical scenarios. Idemia will perform the anomaly detection on passenger database in this task.
- T6.5: Integration and demonstration in Milan airport. Cyber-physical scenarios are also focused on in this task. Access control is validated within this scenario.

All of the participants involved in the activities of WP6 will be staff of consortium partners, apart from ATCOs which DLR will recruit to validate TraMICS. No real passengers or passenger data shall be recruited and collected during the demonstrations. **Participation to all activities is voluntary**, and all participants are made aware of what the demonstrations entail through an information sheet and consent form. More information on recruitment is provided in D9.1, while consent is gone over in D9.2 and D9.8.

Furthermore, all partners processing personal data have organizational and technical measures in place to ensure adequate data protection according to the GDPR. These measures are detailed in D9.7.

In this context, the processing of the personal data is based first of all on the participants consent, but also on the basis of public interest; that put forward by the NIS directive and Regulation No 300/2008.

Taking the above into consideration, the following table lists the main issues to be accounted for during the development of the SATIE project research activities.

Table 5.2: Summary of the legal recommendation for the SATIE validation activities

Field	Regulation/Guidelines	Recommendations
Human rights	Various: • Charter of Fundamental Rights of the European Union.	• Ensure participation is voluntary. • Ensure all participants are informed about the nature of the activity in which they are about to take part. • Ensure participants are aware of their rights (through an information sheet and

Field	Regulation/Guidelines	Recommendations
	• European Convention on Human Rights. • Universal Declaration of Human Rights.	consent form). • Ensure no participants are turned down for discriminatory reasons.
Data protection	General Data Protection Regulation	• Same as the above. • Ensure informed consent for data processing has been obtained.
Airports management and security control	Council Directive 2004/82/EC	No direct legal implications for the project.
	Guidelines on Advance Passenger Information (API)	No direct legal implications for the project. The societal impact of interoperability will be examined in D8.4.
	Directive EU 2016/681 of the European Parliament and of the Council	No direct legal implications for the project. The societal impact of interoperability will be examined in D8.4.
Other	Regulation (EC) 300/2008	SATIE can be seen as an attempt to better comply with these standards.

6 Summary analysis and recommendations

This deliverable has sought to establish the legal framework for SATIE, taking into account human rights, the GDPR, cybersecurity regulations and international standards. Each of these frameworks were set out and linked to SATIE.

In a second part, the implementation of these various frameworks in national contexts was analyzed for the three airports in which SATIE will be demonstrated.

Based on the analysis of the legal framework, recommendations were set out both for the SATIE system as a whole, and for the validation activities.

7 References

Article 29 Data protection Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies*. Retrieved from https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

Boutin, N.; Fechtel, A.; Ho Loh, H; Tan, M. (2016). The Connected Airport: The Time Is Now [Blog]. Retrieved from https://www.bcg.com/publications/2016/technology-digital-transformation-connected-airport-the-time-is-now.aspx

Council Regulation (EEC) No 3925/91 of 19 December 1991 concerning the abolition of controls and formalities applicable to the cabin and checked baggage of persons taking an intra-Community flight and the baggage of persons making an intra-Community sea-crossing

Davis Michels, J., & Walden, I. (2018). *How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive.*

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges.

European Union (2012). Charter of Fundamental Rights of the European Union.

European Union Agency for Cybersecurity. (2018). *Mapping of OES Security Requirements to Specific Sectors*. Retrieved from https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors

Lee, S. and Kleiner, B. (2003), "Electronic surveillance in the workplace", Management Research News, Vol. 26 No. 2/3/4, pp. 72-81. https://doi.org/10.1108/01409170310784014

Michels, J. D., & Walden, I. (2018). How Safe is Safe Enough? Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive. *Improving Cybersecurity in Europe's Critical Infrastructure Under the NIS Directive (December 7, 2018). Queen Mary School of Law Legal Studies Research Paper*, (291).

Narayanan, A., & Shmatikov, V. (2008). Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset). *University of Texas at Austin*.

Public task. Retrieved 15 October 2019, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/public-task/

Regulation (EC) No 300/2008 of the European parliament and of the council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (Text with EEA relevance)

Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky

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) (2016).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. (n.d.).

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)

SATIE consortium. (2019). *D9.1-H-Requirement No.1.*

SATIE consortium. (2019). *Grant Agreement.*

The EU Cybersecurity Act - Digital Single Market - European Commission. Retrieved 29 October 2019, from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

UN General Assembly. (1948). *Universal Declaration of Human Rights.*

WCO/IATA/ICAO. (2014). *Guidelines on Advance Passenger Information (API)*. Retrieved from https://polis.osce.org/wco-iata-and-icao-guidelines-api-including-appendices-guidelines

WCO/IATA/ICAO. (2014). *Guidelines on Advance Passenger Information (API)*. Retrieved from https://www.iata.org/publications/api-pnr-toolkit/Documents/FAL/API/API-Guidelines-Main-Text_2014.pdf

West, J. P., & Bowman, J. S. (2016). Electronic Surveillance at Work: An Ethical Analysis. *Administration & Society*, *48*(5), 628–651.

WP29. (2014). Article 29 data protection working party. *Opinion 05/2014 on Anonymisation Techniques*. Adopted on 10 April 2014. Available at https://www.pdpjournals.com/docs/88197.pdf