D9.1 1st Stakeholder Workshop on ethical, privacy data protection and information

Project Acronym: FLYSEC
Project Title: Optimizing time-to-FLY and enhancing airport Security

Document Date: 12/06/2016

Work Package 9: Privacy, Ethics and Aviation Law

Grant Agreement No. 653879

Project Information

Project Name	Optimising time-to-FLY and enhancing airport SECurity
Project Acronym	FLYSEC
Project Coordinator	National Center for Scientific Research "Demokritos", EL
Project Funded by	European Commission
Under the Programme	Horizon 2020 Secure Societies
Subcall	Disaster-resilience: safeguarding and securing society, including adapting to climate change
Topic	DRS-16-2014 "Critical Infrastructure Protection topic 6: Improving the aviation security chain"
Funding Instrument	Research & Innovation Action
Grant Agreement No.	653879

Document Information

Document Reference	9.1
Document Title	Stakeholder Workshop on ethical, privacy data protection and information access issues
Work package reference	WPX – Privacy, Ethics and Aviation Law
Authored by	Olga E. Segou (NCSRD), Elmar Giemulla (ERAU), Hans-Joachim Ruff-Stahl (ERAU)
With contributions by	Dimitris M. Kyriazanos (NCSRD)
Dissemination Level	Confidential
Cover photo	Airport Crowd Simulation © Integrated Systems Laboratory 2015

Document Verification

Main author(s)	Elmar Giemulla (ERAU), Hans-Joachim Ruff-Stahl (ERAU), Olga E. Segou (NCSRD)
Internal Review and Verification	Dimitris M. Kyriazanos (NCSRD), Stelios C.A. Thomopoulos (NCSRD)

Document Submission

Document due date	30/04/2016
Document submission date	09/11/2016

Executive Summary

As presented by recent reports (IATA Checkpoint of the Future/Smart Security[1], COPRA[2], Flightpath 2050[3]) and following relevant FP7 research activities results, deployment and assessment of integrated, innovative concepts for airport security in an operational environment is a key challenge and a priority for the aviation security research roadmap. Following individual component testing, the Airports Council International (ACI) and the International Air Transport Association (IATA) are planning over the next years a series of pilot tests of multiple components interacting and working together.

Complementing the ACI/IATA efforts, FLYSEC project aims to develop and demonstrate an innovative, integrated and end-to-end airport security process for passengers, enabling a guided and streamlined procedure from the landside to airside and into the boarding gates, and offering for an operationally validated innovative concept for end-to-end aviation security.

FLYSEC is an ambitious 36 month Research and Innovation project, gathering excellence and expertise from Industry, SMEs, Research and Academia including stakeholders and end users such as major airport operator and international airports. FLYSEC ambition turns through a well-structured work plan into: (i) *innovative processes facilitating risk-based screening*, (ii) deployment and integration of *new technologies and repurposing existing solutions* towards a *risk-based Security paradigm shift*, (iii) improve passenger facilitation and customer service, bringing *security as a real service in the airport of tomorrow*, (iv) achieving *measurable throughput improvement and a whole new level of Quality of Service*.

On the technical side, FLYSEC achieves its ambitious goals by integrating new technologies on video surveillance, intelligent remote image processing and biometrics combined with big data analysis, open-source intelligence and crowdsourcing. Repurposing existing technologies is also in the FLYSEC objectives, such as mobile application technologies for improved passenger experience and positive boarding applications (i.e. services to facilitate boarding and landside/airside wayfinding) as well as RFID for carry-on luggage tracking and quick unattended luggage handling.

Besides more efficient background checks and passenger profiling, FLYSEC aims to implement a seamless risk-based security process within FLYSEC combining the aforementioned technologies with behavioural analysis and innovative cognitive algorithms. A key aspect in the design of FLYSEC risk-based security is applying ethical-by-design patterns, maximizing the efficiency of security controls through passenger differentiation ranging from “unknown” to “trusted”, while remaining ethical and fair in the process. Policy, regulatory and standardisation aspects will also be examined in the context of FLYSEC innovative security concept.

Keywords: Aviation Security, Checkpoint of the Future, FLYSEC.

[1] IATA’s checkpoint of the future Executive Summary (Accessed May 2015): http://www.iata.org/whatwedo/security/Documents/cof-executive-summary.pdf

[2] COPRA Project: Comprehensive European Approach to the Protection of Civil Aviation results (Accessed May 2015): http://www.copra-project.eu/Results.html

[3] Flightpath 2050, Europe’s vision for aviation (Accessed May 2015): http://ec.europa.eu/transport/modes/air/doc/flightpath2050.pdf

List of Acronyms and Abbreviations

ACRONYM	EXPLANATION
ACI	Airports Council International
EC	European Commission
EU	European Union
FLYSEC	Optimising time-to-FLY and enhancing airport SECurity
IATA	International Air Transport Association

Table of Contents

1 PROJECT AIMS

As presented by recent reports (IATA Checkpoint of the Future/Smart Security[4], COPRA[5], Flightpath 2050[6]) and following relevant FP7 research activities results, deployment and assessment of integrated, innovative concepts for airport security in an operational environment is a key challenge and a priority for the aviation security research roadmap. Following individual component testing, the Airports Council International (ACI) and the International Air Transport Association (IATA) are planning over the next years a series of pilot tests of multiple components interacting and working together.

Complementing the ACI/IATA efforts, FLYSEC project aims to develop and demonstrate an innovative, integrated and end-to-end airport security process for passengers, enabling a guided and streamlined procedure from the landside to airside and into the boarding gates, and offering for an operationally validated innovative concept for end-to-end aviation security.

FLYSEC is an ambitious 36 month Research and Innovation project, gathering excellence and expertise from Industry, SMEs, Research and Academia including stakeholders and end users such as major airport operator and international airports. FLYSEC ambition turns through a well-structured work plan into: (i) *innovative processes facilitating risk-based screening*, (ii) deployment and integration of *new technologies and repurposing existing solutions* towards a *risk-based Security paradigm shift*, (iii) improve passenger facilitation and customer service, bringing *security as a real service in the airport of tomorrow*, (iv) achieving *measurable throughput improvement and a whole new level of Quality of Service*.

On the technical side, FLYSEC achieves its ambitious goals by integrating new technologies on video surveillance, intelligent remote image processing and biometrics combined with big data analysis, open-source intelligence and crowdsourcing. Repurposing existing technologies is also in the FLYSEC objectives, such as mobile application technologies for improved passenger experience and positive boarding applications (i.e. services to facilitate boarding and landside/airside wayfinding) as well as RFID for carry-on luggage tracking and quick unattended luggage handling.

Besides more efficient background checks and passenger profiling, FLYSEC aims to implement a seamless risk-based security process within FLYSEC combining the aforementioned technologies with behavioural analysis and innovative cognitive algorithms. A key aspect in the design of FLYSEC risk-based security is applying ethical-by-design patterns, maximizing the efficiency of security controls through passenger differentiation ranging from “unknown” to “trusted”, while remaining ethical and fair in the process. Policy, regulatory and standardisation aspects will also be examined in the context of FLYSEC innovative security concept.

Keywords: Aviation Security, Checkpoint of the Future, FLYSEC.

[4] IATA’s checkpoint of the future Executive Summary (Accessed May 2015): http://www.iata.org/whatwedo/security/Documents/cof-executive-summary.pdf

[5] COPRA Project: Comprehensive European Approach to the Protection of Civil Aviation results (Accessed May 2015): http://www.copra-project.eu/Results.html

[6] Flightpath 2050, Europe’s vision for aviation (Accessed May 2015): http://ec.europa.eu/transport/modes/air/doc/flightpath2050.pdf

2 FUNCTION OF THE STAKEHOLDER ADVISORY GROUP

2.1 Scope of WP 9

FLYSEC devotes Work Package 9 "Privacy, Ethics and Aviation Law" entirely to the study of ethical and legal aspects linked with the project activities. WP9 dedicates effort to define the ethical requirements in terms of privacy, data protection and non-discrimination of the project R&D activities as well as the final FLYSEC solutions. It also forms an Ethics Monitoring Committee, which supervises the project activities and convenes when deemed necessary.

Furthermore, WP9 identifies any regulatory and aviation law gaps and constraints and will provide relevant recommendations that will facilitate the creation of an "Airport of the Future".

2.2 Function of the Stakeholders Advisory Group within the Scope of WP 9

WP9 will draw input from the Stakeholder Advisory Group through a dedicated workshop while it is also responsible for setting up and maintaining the Ethics Monitoring Committee. The FLYSEC Stakeholders Advisory Group (SAG) will be composed of experts or organisations that will provide additional expertise in airport security and optimisation of the passenger security control area, related to user requirements as well as impact creation and business models. The aim is to benefit from the practical field expertise and know-how of experts from additional countries, stakeholders, user organisations, without growing the consortium to a too large number of partners. The SAG allows getting an independent external view, whilst enabling for flexibility in the composition of the expert group. As a matter of fact, the FLYSEC partners will open the SAB to additional experts in the course of the project as suitable.

The SAG is managed by the WP8 "Dissemination and Exploitation" Leader with support from the Coordinator and relevant networks and activities from all partners.

The SAG will support the FLYSEC consortium ensuring the compliance of the performed activities with the basic ethical principles that represent the shared values upon which the EU is founded and that are laid down in the European Charter of Fundamental Human Rights, and other applicable rules and regulations.

2.3 Organization of this document

This document will provide administrative notes, the meeting agenda, meeting minutes, and the questions posed by the SAG members.

3 SAG MEETING ADMINISTRATION

	FLYSEC 1st Stakeholders Advisory Group Workshop **19 February 2016** Embry-Riddle Aeronautical University – Europe, Berlin Campus, Kurfuerstenstr. 56, 10785 Berlin		
Meeting called by:	Stelios C.A. Thomopoulos (NCSRD)	**Type of meeting:**	Stakeholder Advisory Group workshop
Attendees:	**Consortium members** NCSRD: Stelios Thomopoulos, Dimitris Kyriazanos, Olga Segou, EMZA: Rami Krispin, ICTS: Shaike Rozanski, Guy Goron UNILU: David Naveh CG: Chanan Gabay, Keren Hananel, Oren Stoler EASC: Christoph Pilarek, Christian Janke, Wolfgang Rehak EXUS: Alex Bartzas, ELBIT: Ofir Rozenberg ERAU: Elmar Giemulla, Sandra Williams EPSILON: Marc Bonazountas, Anestis Trypitsidis **Stakeholder Advisory Group (SAG)** Office of MEP Gabrielle Preuss: Max Brandt Poznan Airport: Grzegorz Bykowski JRC IRMM: Japp de Ruiter Berlin University of Arts: Stephan G. Humer Ministry of Security and Justice of the Netherlands: Olivier Sander Rapiscan Systems: Imran Tahir German Federal Police: Steffen Richter		

4 MEETING AGENDA

Who	Program	Duration
	Arrivals & Coffee	09:00-10:00
NCSRD	Welcome by the FLYSEC Project Coordinator	10:00-10:15
NCSRD	• FLYSEC Project • Work done so far • Next steps	10:15-10:45
All participants	• Review of results already achieved • Involvement of the Stakeholder Advisory Group	10:45-11:30
	Coffee Break	11:30-12:00
CG Smartech	• The scenarios and FLYSEC CONOPS	12:00-12:30
UL	• Risk assessment and differentiation	12:30-13:00
	Lunch Break	13:00-14:00
ERAU & NCSRD	• Stakeholder Workshop on Ethical, privacy data protection and information access	14:00-15:00
All participants	• Round table discussion • Upcoming meetings and farewell	15:00-16:00
	End of Meeting	

5 MEETING MINUTES

5.1 General Remarks

During the SAG Workshop, SAG members were asked to give their unbiased opinion on the project activities and results.

- Stelios Thomopoulos (NCSRD) welcomed the SAG members and explained the current restrictions in terms of disseminating material.
- Dimitris Kyriazanos (NCSRD) gave a brief overview of the FLYSEC project and the tunnels concept.
- Oren Stoler (CG) presented the FLYSEC scenarios and CONOPS.
- David Naveh (UNILU) presented how risk assessment and passenger differentiation work within FLYSEC.
- Olga Segou (NCSRD) and Elmar Giemulla (ERAU) presented the ethical and legal considerations regarding the operational aspects of FLYSEC.

Following each presentation, the SAG members were asked to provide their opinion and ask any question that they might have. In order to have an unbiased opinion, free discussion among SAG members was encouraged with minimal contributions from the consortium. All questions posed by the SAG were then collected and answered by the consortium. The questions posed to the SAG members in the beginning of the session were the following:

- What would you like from FLYSEC?
- What are our strong/convincing points?
- Where to you locate weaknesses of your find objectives are too challenging?

5.2 Questions posed by the SAG members

1. **How is it possible to assign risk without discrimination?**

The screening procedure in FLYSEC is not based on specific characteristics of a person (e.g. their sex, age, ethnicity, etc.) but rather on suspicious behaviors that they might be showing. An example of such a behavior is leaving luggage unattended. The FLYSEC risk assessment is not based on any characteristic that is defined as a protected ground in the Treaty of Amsterdam.

2. **What is the role of manpower in airport security and in FLYSEC in particular?**

The MEP representative remarked that the role of manpower cannot be diminished. ICTS commented that security personnel are often required to handle very large crowds, therefore mistakes and oversights are bound to happen. FLYSEC can act complementarily to manpower.

3. **How extensive is FLYSEC's reliance on technical means with respect to personnel?**

FLYSEC proposes a set of technical means that complement security personnel. Security personnel are still required at the checkpoints.

4. **How does FLYSEC differentiate among passengers?**

NCSRD explained that the profiling is based not on a person's characteristics but rather on suspicious behaviors. UNILU provided an extensive presentation on how behavior-based risk assessment is implemented within FLYSEC.

5. **What are the monitoring system components used in FLYSEC?**

NCSRD provided an extensive description of the FLYSEC applications, while EMZA provided a description of the Visual Sensor.

6. **Does each checkpoint utilize the same equipment or are there different checkpoints?**

It is not within the scope of FLYSEC to make improvements to the screening equipment, although it would be optimal to have screening equipment that can seamlessly adapt to heightened security procedures. FLYSEC does not require the airport operators to increase the resources used in checkpoints or have different lanes and the separation is virtual. FLYSEC tries to optimize the flow of passengers to each lane, taking into account their behavioral characteristics and randomized checks. Furthermore, ICTS commented that different lanes are implemented successfully in UK airports (like Belfast and Bristol).

7. **What is the FLYSEC benchmarking and validation process?**

FLYSEC uses an in-vitro crowd behavior simulator and 3D reconstruction of an airport terminal to test crowd behavior in a large scale, during the initial stages of the project. The main benefit of this approach is that the simulation can provide benchmark results early on, before the field-testing. In addition, simulation is a closed environment avoiding the bias that could result by a crowd that is aware of the testing activity. The first results of the simulated environment will be used as a testing benchmark that the results from the field-testing can be compared to.

8. **Does FLYSEC include airports in this research?**

The Luxembourg International Airport and the Schoenhagen Berlin Airport are part of FLYSEC and will be hosting the FLYSEC pilot tests.

9. Does FLYSEC include analysis of microexpressions?

No, FLYSEC currently does not implement microexpression face recognition.

10. Can a camera outsmart trained security personnel?

A camera complements the security personnel, especially in rush hour where there are large crowds to screen.

11. How does FLYSEC demonstrate and validate its results?

FLYSEC uses an in-vitro crowd behavior simulator and 3D reconstruction of an airport terminal to test crowd behavior in a large scale, during the initial stages of the project. The first results of the simulated environment will be used as a testing benchmark that the results from pilot testing can be compared to. The results will be validated in the operational environments of the Schoenhagen and Luxembourg airports. It was commented that validation with actors is not as accurate as having real passengers and threats, but UNILU argues that it is the only ethical and practical solution.

12. How does FLYSEC achieve constant optimization?

FLYSEC will redirect travellers to their lanes based on the behavioral risk analysis and randomized checks in order to achieve near-optimal efficiency. The main criteria used in FLYSEC are behavioral analytics with QoS criteria and passenger satisfaction.

13. Is FLYSEC an opt-in programme?

Yes, using the FLYSEC applications is an opt-in. FLYSEC advocates an application that offers incentive to the passengers in order to facilitate the process and use the system. Furthermore, the passenger will be aware of the measures we take for data protection in order to improve their trust to the FLYSEC applications and the social acceptance of the solution. Passengers have the right to decline to use the system and go through an enhanced checkpoint.

14. What threats does FLYSEC detect? (terrorism, smuggling etc.)

FLYSEC detects suspicious behavior that could be linked with any type of crime. CBRNE or drug detection is not within the scope of FLYSEC.

15. **What is the period of data retention for FLYSEC applications?**

As small as possible, while the passenger will have the right to ask for their data to be removed at all times. The exact data retention period remains to be seen, as soon as the new Data Protection Directive is finalized, taking into account the Right to Forget. Furthermore, real time behavior for people opting-out won't be stored except in case of arrest, for registered there might be some data retention.

16. **What if a particular behavior is linked to a sensitive data case?**

It is difficult to assume that a particular behavior is only linked to a very specific case. An example would be someone who is having a health problem and is crouching, that could look like they are trying to conceal an item.

17. **How can we "quantify" human behavior and assign "trustworthiness" to specific indicators of suspicious behavior?**

FLYSEC can't quantify the whole spectrum of human behavior, but will produce a set of rules that will also be used for the project's final validation. We value the simulation platform for early validation through the simulation of behavioral analysis since it's unaffected by observation and is unbiased. Simulation, quantification and risk indicators, combining operational validation during our field tests, will help up plan for the final testing and validation of FLYSEC.

18. **What kind of data does FLYSEC use and how do we handle the massive amount of information? What is the level of data protection we apply?**

FLYSEC adheres to the current data protection directive and takes into account the current plan for reform (especially regarding the right to forget). The FLYSEC application can collect personal and tracking data, the visual sensor with record video data but no sensitive data will be collected from the travellers.

6 COMMENTS BY THE SAG MEMBERS

6.1 General Remarks

These statements do not represent the official opinion of the organisations.

6.2 Comments

MEP representative (Head of Office):

- The process must be compliant to EU law and also adaptable to account for new legislation
- Passengers usually complain about the screening procedure, not the waiting time. FLYSEC focuses a lot on optimizing flow and waiting time.
- Criticism might rise due to preferential treatment, travel must be regarded as a basic need. We should not create “first class” and “second class” passengers.
- Currently smuggling is a bigger concern than terrorist attacks

JRC (XP-Dite project technical officer):

- FLYSEC needs to clarify if the main focus is in flow optimization, security or screening processes.
- EXPEDITE uses fingerprints as a biometric tag, but is only used through checkpoints and is not used to identify the person in another basis. The fingerprint is removed from the database when the passenger exits the checkpoint. There must not be a link to any external database with identities.
- Suggests connection with frequent flyer programme.
- Clarify how we can “quantify” human behavior and assign some “trustworthiness” to indicators of human behavior.
- The upside is that there is no visual difference in three different lanes but the checkpoint needs to be able to cope with different settings
- Study the overhead of false alarms
- Different checkpoints could be optimized to their security settings, are we addressing this issue in the project?
- Security searches for forbidden objects that are regulation, specific and identifiable, FLYSEC adds a different dimension by trying to quantify the intent
- Differentiation would be more efficient with advanced equipment that can adapt to level of risk

Berlin U of Arts:

- FLYSEC introduces an innovative new concept and not additional security measures on top of existing
- Suggests we implement a “positive discrimination” process where travellers who follow the rules are “rewarded”

German Federal Police:

- Do not include PNR in FLYSEC
- In order to interface a system like FLYSEC with police databases, we would have to check for identification. The problem is that there is no ID check before check-in.
- How would we handle passengers asking to change lane or asking why there is a difference in screening procedures, what happens when passengers change lanes on their own or change their behavior.

Poznan Airport:

- Increase efficiency
- Focus on one location at the airport, as operators don’t spare resources for differentiation
- Work near the capacity levels of the screening equipment
- Link FLYSEC to loyalty programmes, frequent flyer programmes etc.
- More clarity on how we differentiate between normal and enhanced security passengers
- Speed up the process for travellers carrying only cabin luggage
- It is not generally considered good for an airport operator to mix standardized and non-standardized equipment (must be standardized and compliant to EU an member state legislation)
- 100% accuracy cannot be achieved but at the end of the day, it is a matter of the judgement of the individual providing a check
- Clarify how we can align the novel technology with commercial drivers
- Be smarter and friendlier than what is available on the market

Netherlands Ministry of Security and Justice:

- Clarify the difference between virtual and actual checkpoints
- In the Netherlands, airports find it difficult to have different checkpoints, since they wouldn’t know how many people they would have for each checkpoint

- The concept has a deterrence effect, on the other hand some security measures would be lower and a potential terrorist could prepare for it
- There is a need for a passenger-friendly way to screen for explosives
- Find a way to easily integrate sniffing/detection technology into the checkpoint
- We can try to apply a “point system” for rewarding a passenger

Rapiscan:

- Airport checks are essentially looking into what you have on your luggage, and not if you might have malicious intent.
- One of the current demands in the screening equipment market is the risk based protocol and how to increase the scanning speed of the equipment.

7 SUMMARY AND PROPOSED WAY FORWARD BY THE SAG

7.1 Summary

SAG members commented that PNR data should not be used within FLYSEC, although ICTS commented that using PNR data for security systems is a common practice in UK airports. There was a lot of focus on the behavioral analysis and how we apply the ethical principle of non-discrimination. FLYSEC should also take into account the capacity and the technological improvement of screening equipment and the role of personnel performing the security checks. FLYSEC also needs to take into account the passenger perspective in terms of their acceptance of differentiated screening procedures and how to reduce complaints. FLYSEC also needs to take into consideration standardization and compliance.

7.2 Proposed Scenarios to be Included in FLYSEC

- Insider threats (partially within scope, since there might be pre-existing data on an employee, there are connections between an insider threat and FLYSEC although the scenario would be implemented differently)
- Stolen or falsified passports
- Security breaches when a person does not go through a specified checkpoint
- A (trusted) passenger unknowingly carrying suspicious items that were placed in their luggage by another person
- There needs to be a mechanism that allows flexibility in changing scenarios and changing environments