



FP7-313161

*A holistic, scenario-independent, situation-awareness and guidance  
system for sustaining the Active Evacuation Route for large crowds*

## **ETHICAL AND LEGAL EVALUATION REPORT AND RECOMMENDATIONS**

**Deliverable Identifier:** D11.5 Ethical and legal evaluation report and recommendations

**Delivery Date:** 31 May 2017

**Classification:** Restricted

**Editor(s):** Ivo Emanuilov (KUL)

**Document version:** 1.0 – May 31, 2017

**Contract Start Date:** April 1<sup>st</sup>, 2013

**Duration:** 50 months

**Project coordinator:** EXODUS S.A. (Greece)

**Partners:** EXO (GR), IT INNOVATION (UK), ICCS (GR), HKV (NL), TEL (GR), TEK (ES), AIA (GR), VITRO (IT), CDI (UK), INDRA (ES), KUL (BE), DXT (FR), POLITO (IT), STX-FR (FR), TUD (DE), TUC (DE), ASRS (ES), METB (ES), TIM (IT)

**Project co-funded by the  
European Commission under the  
7<sup>th</sup> Framework Programme**



### Document Control Page

<b>Title</b>	Ethical and legal evaluation report and recommendations	
<b>Editors</b>	Ivo Emanuilov	KUL
<b>Contributors</b>		
<b>Peer Reviewers</b>	Hanneke Vreugdenhil	HKV Consultants
	Pedro Garibi	Indra
<b>Format</b>	Text - MS Word (docx)	
<b>Language</b>	en-UK	
<b>Work-Package</b>	WP11	
<b>Deliverable number</b>	D11.5	
<b>Due Date of Delivery</b>	31 May 2017	
<b>Actual Date of Delivery</b>	31 May 2017	
<b>Dissemination Level</b>	Restricted to other programme participants (including the Commission Services)	
<b>Rights</b>	eVACUATE Consortium	
<b>Audience</b>	<input type="checkbox"/> public <input checked="" type="checkbox"/> restricted <input type="checkbox"/> internal	
<b>Date</b>	May 31, 2017	
<b>Revision</b>	none	
<b>Version</b>	1.0	
<b>Edited by</b>	Ivo Emanuilov	
<b>Status</b>	<input type="checkbox"/> draft <input checked="" type="checkbox"/> Consortium reviewed <input checked="" type="checkbox"/> WP leader accepted <input checked="" type="checkbox"/> Project coordinator accepted	

### Revision History

Version	Date	Description and comments	Edited by
0.1	May 19, 2017	First draft	Ivo Emanuilov
0.2	May 22, 2017	Second draft with appendices	Ivo Emanuilov
0.3	May 23, 2017	Minor revisions	Ivo Emanuilov
0.4	May 23, 2017	Review with comments and suggestions	Pedro Garibi
0.5	May 30, 2017	Review with comments and suggestions	Hanneke Vreugdenhil
0.6	May 30, 2017	Minor revisions and additions	Ivo Emanuilov
1.0	May 31, 2017	Final version	Ivo Emanuilov

### List of Acronyms and abbreviations

Acronym	Meaning
AER	Active Evacuation Route
AP	Access Point
CIO	Chief Information Officer
CNIL	Commission nationale de l'informatique et des libertés
COP	Common Operational Picture
CSO	Chief Security Officer
DPIA	Data Protection Impact Assessment
EU	European Union
GDPR	General Data Protection Regulation
IMO	International Maritime Organisation
PDF	Portable Document Format
RFID	Radio Frequency Identification
SOLAS	International Convention for the Safety of Life at Sea
UNCLOS	United Nations Convention on the Law of the Sea
VPN	Virtual Private Network

## Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>7</b>
1.1	Purpose of this document.....	7
1.2	Structure of the Document.....	7
<b>2</b>	<b>Privacy and data protection compliance of eVACUATE .....</b>	<b>8</b>
2.1	Legal support during the validation demonstrations.....	8
2.2	Legal analysis of eVACUATE's compliance with the privacy and data protection requirements.....	10
<b>3</b>	<b>Overview of the impact of the General Data Protection Regulation on eVACUATE.....</b>	<b>35</b>
3.1	Territorial scope.....	35
3.2	The notion of 'personal data' .....	35
3.3	Accountability .....	35
3.4	Lawfulness of processing .....	36
3.5	Transparency .....	37
3.6	Rights of the data subjects .....	38
3.7	Data protection by design and by default.....	40
3.8	Data protection impact assessment.....	41
<b>4</b>	<b>Privacy and data protection compliance recommendations for end users of eVACUATE .....</b>	<b>44</b>
<b>5</b>	<b>Conclusions.....</b>	<b>47</b>
<b>6</b>	<b>Appendix I: Information and consent forms.....</b>	<b>49</b>
6.1	Information and consent form for Anoeta Stadium Real Sociedad (ASRS) validation demonstration.....	49
6.2	Information and consent form for Athens International Airport (AIA) validation demonstration.....	50
6.3	Information and consent form for STX France (STX) validation demonstration .....	52
6.4	Information and consent form for Metro Bilbao (METB) validation demonstration .....	54
<b>7</b>	<b>Appendix II: Data processing agreements .....</b>	<b>57</b>
7.1	Data processing agreements for Anoeta Stadium Real Sociedad (ASRS) validation demonstration.....	57
7.2	Data processing agreements for Athens International Airport (AIA) validation demonstration.....	91
7.3	Data processing agreements for STX France (STX) validation demonstration .....	122
7.4	Data processing agreements for Metro Bilbao (METB) validation demonstration .....	154
<b>8</b>	<b>Appendix III: Notifications to national data protection authorities ...</b>	<b>186</b>

8.1	Notification submitted by Anoeta Stadium Real Sociedad (ASRS) to the Spanish Data Protection Authority .....	186
8.2	Notification submitted by Athens International Airport (AIA) to the Hellenic Data Protection Authority .....	186
8.3	Notification submitted by STX France (STX) to the French Data Protection Authority .....	191
8.4	Notification submitted by Metro Bilbao (METB) to the Spanish Data Protection Authority .....	191

## Executive summary

This deliverable presents an assessment of the privacy and data protection compliance framework of the eVACUATE project, as evaluated in the previous tasks and during the four validation demonstrations. It contains analysis of the different elements of the eVACUATE solution from an ethical, privacy and data protection perspective and a summary of the insights on the impact of the technology on individuals' rights as observer during the demonstrations. The deliverable lays specific emphasis on the regulatory impact of the entry into force of the General Data Protection Regulation (GDPR) on the different elements of eVACUATE and pays attention to the data protection by design and by default measures considered in the context of eVACUATE. It formulates future-proof recommendations for end users when considering the implementation of eVACUATE in a production environment and also provides guidance on the new requirement of the GDPR of conducting a data protection impact assessment (DPIA).

The outcomes of the privacy and data protection analysis could be summarised as follows:

- **RFID** technology provides for detailed information for the data subjects, its use is entirely voluntary and sufficient safeguards respecting the data subjects' rights have been suggested; data minimisation techniques have been implemented such as non-individualisation of the chipless RFID tags and not using unique identification numbers; clear retention periods or criteria for determining such periods must be established in a production environment.
- **MobiMESH** technology has clearly defined purposes and processes proportionate amount of data to the defined purposes of processing; data security measures have been implemented; in a production environment, data controllers should elaborate a clear privacy policy and terms of use, taking into account the conditions for valid consent of Article 7 GDPR (if consent is relied upon); clear retention periods or criteria for determining such periods must be established in a production environment.
- **eVAMAPP** applications are used on a purely voluntary basis; compliance with the GDPR's intensified information and transparency obligations is essential; data protection by design and by default measures have been implemented: device's location is not tracked, GPS satellites and iBeacons are not used to identify or store the IDs of the terminal devices, applications do not store unnecessary identity attributes; the key moment for activation of identification functions is proportionately related to the moment of declaring an evacuation.
- **SoNeMa** technology provides for targeted content analysis but it should be performed in a limited timespan, eg, when an emergency is clearly present; the legal ground for processing must be carefully assessed by the controller in a production environment.
- **Crowd behaviour detection** technology has narrowly defined purposes and does not perform identification of natural persons; it has improved accuracy; facial images from optical cameras should not be processed to perform identification; data from behaviour detection algorithms should not be linked with data about identifiable persons; transparency obligations are key, especially when combining this technology with relatively known legacy technologies, such as CCTV; the technology should not be active at all times.
- **Counting** technology has clearly defined purposes and improved data accuracy; data minimisation includes video of low quality which does not allow for performing facial recognition operations and automatic deletion of frames shortly after their technical processing by the system.

## 1 Introduction

### 1.1 Purpose of this document

This deliverable presents an assessment of the privacy and data protection compliance framework of the eVACUATE project, as evaluated in the previous tasks and during the four validation demonstrations.

It contains analysis of the different elements of the eVACUATE solution from an ethical, privacy and data protection perspective and a summary of the insights on the impact of the technology on individuals' rights as observer during the demonstrations.

The deliverable lays specific emphasis on the regulatory impact of the entry into force of the General Data Protection Regulation on the different elements of eVACUATE. Furthermore, the analysis pays attention to the data protection by design and by default measures considered in the context of eVACUATE and formulates recommendations for end users when considering the implementation of eVACUATE in a production environment.

This document is the final deliverable of Work Package 11 focusing on the ethical and legal framework applicable to eVACUATE and it aims at providing useful guidelines and recommendations for ensuring future-proof compliance of the system in the long run.

### 1.2 Structure of the Document

The structure of this document is as follows:

In **chapter 2**, an evaluation of the project's compliance with the applicable data protection procedures for the validation demos and other research activities is provided. This evaluation summarises the outcomes of the analysis of the different technologies, their 'privacy by design' features and their impact on data protection and the implemented mitigation measures.

In **chapter 3**, an initial assessment of the regulatory impact of the General Data Protection Regulation on eVACUATE is provided. This analysis aims to familiarise potential end users considering the implementation of eVACUATE in a production environment with the new obligations they may have as data controllers. The purpose of this overview is to present some of the challenging aspects of the GDPR such as the data protection impact assessment, the various transparency obligations and new data subjects' rights.

In **chapter 4**, a concise set of recommendations for future users of (parts of) the eVACUATE system is provided in order to enhance their understanding of the privacy and data protection risks involved and to encourage them to consider the legal, technical and organisational measures prescribed by the GDPR in order to ensure their processing operations are fully compliant.

## **2 Privacy and data protection compliance of eVACUATE**

### **2.1 Legal support during the validation demonstrations**

In eVACUATE, four distinct validation demonstrations were carried out to evaluate the system's functionality and performance. In terms of ensuring the demonstrations' compliance with privacy and data protection regulations, two categories of issues had to be addressed, namely (1) determining the different partners' roles and responsibilities and (2) ensuring compliance with the legislation applicable in the demonstration's location.

As previously discussed in Deliverable D11.4, the individual research activities need to have a data controller as the party which defines the means and purposes of processing and assumes responsibility for ensuring compliance with the privacy and data protection requirements. Under the regime established with Directive 95/46/EC, the applicable law to the activities of a controller is the controller's national law.

Discussions with the technical partners at the stages of preparation of the validation demonstrations and analysis of their roles in the demonstrations were very helpful in determining the data controller. Thus, for each of the four demonstrations, our analysis determined that the partner responsible for determination of the purposes and means and provision of organisational resources, such as venue, access to facilities and ultimately exercising control over the resulting video recordings is to be designated as a data controller, with the rest of the partners acting on its behalf as data processors.

The final versions of the information and consent forms and the data processing agreements for each separate validation demonstration are provided in Appendix I and Appendix II to the present deliverable. Appendix III contains information on the submitted notifications to the respective national data protection authorities.

#### **A. Anoeta Real Sociedad Football Stadium**

In the first validation demonstration at Anoeta Real Sociedad Football Stadium in San Sebastian, the stadium, as a legal person, was determined to be a controller and the rest of the partners were designated data processors. Assistance was provided to the stadium's legal department in the preparation of data processing agreements governing the relationship between the controller and the processors. The templates of data processing agreements provided for in the annexes to Deliverable D11.4 were tailored to the context of the validation demonstrations, specifying the purposes and defining the parties' rights and obligations. The agreements were prepared by KU Leuven but the process of signing and execution of these agreements was under the control of the data controller. A separate data processing agreement was executed between the data controller and each data processor since the collection and processing operations carried out by the different partners were different in nature.

In addition to the data processing agreement, an information and consent form for obtaining the consent of the volunteers participating in the demonstration was drafted. The consent form was detailed enough to provide comprehensive information to the volunteers on the demonstration, the categories of data, the purposes, the means, the retention period, the policy for further processing for research purposes, and the contact details of the data controller's representative. Furthermore, the consent form provided for a visual separation of the scope of the data subject's consent from the rest of the information. On the back side



of the form, a list of the processors has been included and contact details of the persons responsible in case of requests from the data subjects.

The consent form was duly translated into Spanish language and relevant explanations were given to the volunteers before signing the consent form. A copy of the consent form has been provided to each data subject for them to retain for future reference and in case they may have any further questions on the data processing activities.

In the course of preparations for the demonstration, the controller was advised to consult the national data protection authority in order to inquire if a prior notification is required under national law. In addition, the controller was also advised to consult any activities with their internal legal department in order to ensure full compliance with any additional applicable national law. Finally, the controller was also advised that they should keep the signed consent forms and the video and image recordings in accordance with their internal policy.

## **B. Athens International Airport**

In the second validation demonstration at Athens International Airport in Athens, the airport, as a legal entity, was determined to be a controller and the rest of the partners were designated data processors. Assistance was provided to the airport's legal department in the preparation of data processing agreements governing the relationship between the controller and the processors. The templates of data processing agreements provided for in the annexes to Deliverable D11.4 were tailored to the context of the validation demonstrations, specifying the purposes and defining the parties' rights and obligations. The agreements were prepared by KU Leuven but the process of signing and execution of these agreements was under the control of the data controller. A separate data processing agreement was executed between the data controller and each data processor since the collection and processing operations carried out by the different partners were different in nature.

The airport's representatives confirmed the submission of a notification to the Hellenic Data Protection Authority regarding the data processing activities taking place during the demonstration. The original information and consent form was slightly modified to reflect the specifics of the demonstration and the venue but the purposes, the means, the retention period, and the policy for further processing for research purposes were kept intact.

The volunteers were invited to read the information and consent form before entering the demonstration's venue and they were provided with an opportunity to ask their questions in both Greek and English. Each volunteer was given a copy of the information and consent form to keep for future references.

After the demonstration, the controller prepared a promotional video for dissemination purposes. As some of the selected frames in the video contained images of faces and other attributes which might lead to identification of the natural persons involved, the controller applied blurring and other privacy-preserving techniques to ensure compliance with the consent obtained by the volunteers.

## **C. STX**

In the third validation demonstration, which took place on a ship at STX's premises in Saint-Nazaire, STX, as a legal entity, was determined to be a controller and the rest of the partners were designated data processors. Assistance was provided to the company's legal

department in the preparation of data processing agreements governing the relationship between the controller and the processors. The templates of data processing agreements provided for in the annexes to Deliverable D11.4 were tailored to the context of the validation demonstrations, specifying the purposes and defining the parties' rights and obligations. The agreements were prepared by KU Leuven but the process of signing and execution of these agreements was under the control of the data controller. A separate data processing agreement was executed between the data controller and each data processor since the collection and processing operations carried out by the different partners were different in nature.

STX's representatives were advised to consult CNIL, the national data protection authority in France, in order to make sure that all relevant national requirements are met prior to the demonstration. The information and consent form was modified to reflect the specifics of the demonstration and the applicable law in France but the essential elements were kept intact.

#### **D. Metro Bilbao**

In the fourth validation demonstration, which took place at a station of the underground in Bilbao, Metro Bilbao, as a legal entity, was determined to be a controller and the rest of the partners were designated data processors. Assistance was provided to the company's legal department in the preparation of data processing agreements governing the relationship between the controller and the processors. The templates of data processing agreements provided for in the annexes to Deliverable D11.4 were tailored to the context of the validation demonstrations, specifying the purposes and defining the parties' rights and obligations. The agreements were prepared by KU Leuven but the process of signing and execution of these agreements was under the control of the data controller. A separate data processing agreement was executed between the data controller and each data processor since the collection and processing operations carried out by the different partners were different in nature.

Metro Bilbao's representatives were advised to consult Agencia Española de Protección de Datos, the Spanish data protection authority, in order to make sure that all relevant national requirements are met prior to the demonstration. The information and consent form was modified to reflect the specifics of the demonstration and the applicable law in Spain but the essential elements were kept intact.

## **2.2 Legal analysis of eVACUATE's compliance with the privacy and data protection requirements**

In addition to the legal support provided to the controllers and processors prior and during the validation demonstrations, an assessment was carried out of the implementation of the requirements and recommendations provided by the legal analysis carried out in the previous deliverables in Work Package 11.

This assessment is based on the findings and recommendations of Deliverable D11.3 where an analysis of the individual elements of the eVACUATE solution was provided.

The following tables represent how the recommendations of Work Package 11 have been implemented in practice in the eVACUATE tools.

## A. Analysis of the RFID technology

#	Recommendation	What actions have been taken in order to implement the recommendations?
1.	<b>Define a purpose of the processing of personal data:</b> <ul style="list-style-type: none"> <li>• The purpose has to be specific and clearly defined</li> <li>• The purpose has to be defined before the actual processing</li> </ul>	<ul style="list-style-type: none"> <li>• The purpose of RFID tags developed within the eVACUATE project is to update and maintain the Active Evacuation Route (AER) by counting the number and type of individuals who pass through a specific place, where an appropriate chipless RFID reader is installed. For example, RFID reader could be installed at the entrance of a metro station or in a cruise ship.</li> <li>• During the validation demonstrations, no personal data of the volunteers have been collected or processed to test the operation of the RFID technology.</li> <li>• Potential end users will have to clearly define the purposes for which they intend to introduce and use the RFID technology but in any case, they should be specific and clearly defined, such as the ones described above.</li> </ul>
2.	<b>Define the legal basis for the processing:</b> <b>One of the following grounds could be selected:</b> <ul style="list-style-type: none"> <li>• Data subject's consent;</li> <li>• Necessary for the performance of a contractual obligation</li> <li>• Processing is necessary for compliance with a legal obligation to which the controller is subject;</li> <li>• Processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li>• 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;</li> <li>• Processing is necessary for the purposes of the legitimate interests pursued by the controller</li> </ul>	<ul style="list-style-type: none"> <li>• For the purpose of the validation demonstrations, a data subject's consent was requested from all participating volunteers</li> <li>• The legal basis for the data processing beyond the project (for a commercial tool based on chipless RFID technology) has also been considered in Deliverable D11.3</li> <li>• The recommendations to potential future end users include: <ul style="list-style-type: none"> <li>◦ individuals should be explicitly informed about the processing of their personal data via tickets containing RFID tags</li> <li>◦ individuals should consent to the usage of this technology</li> <li>◦ it should be ensured that the use of the technology is entirely voluntary and that no negative consequences will ensue if they do not wish to use it</li> <li>◦ if tickets are purchased from machines, individuals could be given the opportunity to press an "I agree button" after they have read the consent form and information notice in order to</li> </ul> </li> </ul>

		<p>proceed with the purchase of a tagged ticket</p> <ul style="list-style-type: none"> <li>provided the limited benefits of this technology, individuals should have a possibility whether to use tickets containing chipless RFID technology or not, which means that no one should be forced to purchase tickets or cards that contain the RFID tag.</li> </ul>
3.	<b>Ensure data accuracy and quality:</b> <ul style="list-style-type: none"> <li>Take measures to ensure that the collected data is adequate, relevant for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>The system is characterised in order to establish a figure of merit on the accuracy of the system. This parameter can be used to determine the tolerable error margin in the measurements</li> <li>An error in measurement could imply misleading information, eg, mistaking a disabled person with a first responder. The system is expected to have an accuracy higher than 90%</li> <li>The continuous development of the proposed technology will improve its accuracy to make sure that the collected data are adequate and relevant for the purposes of getting a reliable picture of the number of persons in a certain area</li> </ul>
4.	<b>Ensure data minimization:</b> <ul style="list-style-type: none"> <li>Take measures to ensure that the collected data is not excessive in relation to the purpose for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>To provide assistance in case of emergency situation, there is no need to have a detailed information about each RFID tag carrier. Therefore, the tags are not individualized, e.g. they do not contain names or other unique identifiers</li> <li>The chipless RFID tags do not have unique numbers</li> <li>In production environment, end users must adopt clear internal data access and usage policies specifying the individuals who have access to the data only for purposes of counting individuals and their categories and for identifying their approximate location</li> </ul>
5.	<b>Ensure data integrity and security:</b> <ul style="list-style-type: none"> <li>Take appropriate technical measures to prevent unauthorized disclosure or access to collected personal data</li> <li>Take appropriate organizational measures to prevent unauthorized disclosure or access to collected personal data</li> </ul>	<ul style="list-style-type: none"> <li>Even in the cases where a tag contains solely a number that is unique within a particular context, and no additional personal data can be extracted, care must be taken to address potential privacy and security issues if the tag is carried by persons</li> <li>The only information that can be taken out from the eVACUATE tag is a code (3 to 5 bits) which has no meaning until it is matched with a representation table. This table is stored into the eVACUATE framework and is secured with the</li> </ul>

		procedures developed for this purpose in WP6.
6.	<b>Attribute responsibilities for the parties involved in processing:</b> <ul style="list-style-type: none"> <li>• <b>Appoint the controller</b></li> <li>• <b>Define other parties involved (e.g., processors or third parties)</b></li> </ul>	<ul style="list-style-type: none"> <li>• During the validation demonstrations, TUD process personal data via the eVACUATE system provided by other project partners</li> <li>• During the technology development, data is stored at TUD. During the validation demonstrations, while the system is integrated to the whole eVACUATE system, TUD does not store any data</li> <li>• In the final product release, it is not contemplated that chipless RFID system can store or process any data</li> <li>• The acquired data are unique since they depend on the time when it has been collected and it is not possible to update them. Each new data captured represent new information</li> </ul>
7.	<b>Ensure respect of data subjects' rights</b> <ul style="list-style-type: none"> <li>• <b>Develop policies and procedures that would allow data subjects to request information about the collected data, to rectify, block or erase data</b></li> </ul>	<ul style="list-style-type: none"> <li>• Provided that the RFID tags are carried by individuals, they allow to establish a link with a particular person. Therefore, individuals should be explicitly informed that their usage of tickets containing RFID tags entail the processing of personal data.</li> <li>• As the tags used during the validation demonstrations were not personalised and linked to particular natural persons, their use did not lead to any negative consequences</li> </ul>
8.	<b>Ensure limited retention of the collected personal data</b> <ul style="list-style-type: none"> <li>• <b>Define the time period after which data will be deleted</b></li> <li>• <b>Establish practices, policies and procedures to delete data</b></li> </ul>	<ul style="list-style-type: none"> <li>• The data collected during the development of the project will be stored for 5 years after the finishing of the eVACUATE project for evaluation and review purposes</li> <li>• The data collected will be stored at TUD's servers and will be deleted according to the current procedures established at this institution</li> <li>• In a production environment, a retention and deletion policy would have to be established by the end users, such as automatic erasure at regular intervals determined in accordance with any specific national laws which may establish statutory periods of retention</li> </ul>
9.	<b>Limitations of the technology</b>	<ul style="list-style-type: none"> <li>• This technology, however, does not show the direction of movement of the individuals, i.e. it can only locate the proximity of a certain tag next to an RFID reader.</li> </ul>

		Therefore, the place where RFID technology is installed must be carefully considered.
--	--	---

## B. Analysis of the Wi-Fi - MobiMESH technology

#	Recommendation	What actions have been taken in order to implement the recommendations?
1.	<b>Define a purpose of the processing of personal data:</b> <ul style="list-style-type: none"> <li>• The purpose has to be specific and clearly defined</li> <li>• The purpose has to be defined before the actual processing</li> </ul>	<ul style="list-style-type: none"> <li>• MobiMESH is part of the eVACUATE system. The role of MobiMESH is to provide information about: <ul style="list-style-type: none"> <li>○ Access point (AP) online or offline</li> <li>○ For each AP: information and statistics (i.e., bytes and packets transmitted and received etc.)</li> <li>○ Probing: each AP probes the number of clients in its range</li> <li>○ Association: each AP gives information about the number of users associated to an AP</li> <li>○ Association and logging: each AP gives information about the number of users associated to an AP and authenticated from a captive portal</li> <li>○ Discover on which AP (and then where) the MAC address of a first responder is associated</li> <li>○ Sending SMS to first responders</li> </ul> </li> <li>• This platform is able to be configured to keep track of personal data such as: <ul style="list-style-type: none"> <li>○ name and surname of users</li> <li>○ mobile phone number (both for guest and first-responder)</li> <li>○ e-mail address of guests (only if provided by guest himself in registration phase).</li> </ul> </li> <li>• In the eVACUATE configuration during the validation demonstrations, this platform was used only for some functionalities already described above and the only information that can be stored is the mobile phone number that is collected</li> </ul>
2.	<b>Define the legal basis for the processing:</b> <b>One of the following grounds could be selected:</b> <ul style="list-style-type: none"> <li>• The data subject's consent;</li> <li>• Necessary for the performance of a contractual obligation</li> <li>• Processing is necessary for compliance with a legal obligation to which the</li> </ul>	<ul style="list-style-type: none"> <li>• Data subject's consent is relied on and it is obtained prior to any processing of personal data</li> <li>• The data are used to list the whole group of people involved in the first emergency response</li> <li>• In case of emergency, it is possible to use Wi-Fi instead of another way to connect to the first responder and send and receive</li> </ul>



	<p>controller is subject;</p> <ul style="list-style-type: none"> <li>• Processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li>• 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;</li> <li>• Processing is necessary for the purposes of the legitimate interests pursued by the controller</li> </ul>	<p>fundamental information for managing the emergency.</p> <ul style="list-style-type: none"> <li>• The whitelist of mobile phone numbers is used to provide the best performance to connect the control room with the first responder</li> <li>• In case of emergency, the EOC operator can: <ul style="list-style-type: none"> <li>○ Discover approximately how many people are involved in the emergency through the information provided by APs in the probing phase</li> <li>○ Discover exactly how many people are in the range of an AP through the information provided by APs in the associated phase</li> <li>○ Discover information about name, surname, mobile phone number of people associated and logged on the captive portal</li> <li>○ EOC can discover where a first responder is and then can send him SMS with information about the emergency</li> <li>○ First responder can use the Wi-Fi network to communicate with EOC</li> </ul> </li> </ul>
3.	<p><b>Ensure data accuracy and quality:</b></p> <ul style="list-style-type: none"> <li>• Take measures to ensure that the collected data is adequate, relevant for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>• The platform uses standard protocol to collect information that are subject to other type of certification (i.e., 802.11x etc.)</li> </ul>
4.	<p><b>Ensure data minimization:</b></p> <ul style="list-style-type: none"> <li>• Take measures to ensure that the collected data is not excessive in relation to the purpose for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>• The amount of the collected data is proportionate with the overall goal of a processing operation.</li> <li>• The data collected are only those indicated in the first point.</li> </ul>
5.	<p><b>Ensure data integrity and security:</b></p> <ul style="list-style-type: none"> <li>• Take appropriate technical measures to prevent unauthorised disclosure or access to collected personal data</li> </ul>	<ul style="list-style-type: none"> <li>• Data integrity and security is achieved, inter alia, by the following measures: <ul style="list-style-type: none"> <li>○ System must be periodically updated to the last release</li> <li>○ When the system start is powered on a VPN with the platform's support that make</li> </ul> </li> </ul>



	<ul style="list-style-type: none"> <li>• <b>Take appropriate organisational measures to prevent unauthorised disclosure or access to collected personal data</b></li> </ul>	<p>possible a remote connection for all the activities needed for support or maintenance scope. Automatic update is not possible.</p> <ul style="list-style-type: none"> <li>○ Development tools and compiler software must be removed from system. On the server, only the principal software is installed without the development environment.</li> <li>○ Passwords stored in the system are encrypted and salted (confidentiality)</li> <li>○ Passwords are not be hardcoded in software (shell scripts, JavaScript, Python scripting, etc.) and connection procedure</li> <li>○ Default passwords are changed</li> <li>○ Application passwords stored are be encrypted and salted (confidentiality).</li> <li>○ Passwords are not hardcoded in software (shell scripts, JavaScript, Python scripting, etc.)</li> </ul>
6.	<p><b>Attribute responsibilities for the parties involved in processing:</b></p> <ul style="list-style-type: none"> <li>• <b>Appoint the controller</b></li> <li>• <b>Define other parties involved (e.g., processors or third parties)</b></li> </ul>	<ul style="list-style-type: none"> <li>• In a production environment, the controller will likely be the end user who will determine the purposes and means of processing in the cases of private cellular network deployments. This will have to be examined on a case-by-case basis.</li> <li>• In the validation demonstrations, instead of public cellular networks, the Wi-Fi-based MobiMESH solution is used. <ul style="list-style-type: none"> <li>○ The mobile phone number is stored in MobiMESH appliance, in an internal database of Telecom Italia</li> <li>○ Information is kept up to date via internet for management activities, such as 'hardening' of the platform.</li> <li>○ To update the end-user information the operator have to use the captive portal UI.</li> </ul> </li> </ul>

		<ul style="list-style-type: none"> <li>○ The user information can be deleted through captive portal UI.</li> <li>○ A REST API is provided through which is possible to have evidence of the users associated and logged to the system. In this case the EOC operator have the possibility to discover also the mobile phone number of the user and in case can share it with first responders.</li> </ul>
7.	<b>Ensure respect of data subjects' rights</b> <ul style="list-style-type: none"> <li>• Develop policies and procedures that would allow data subjects to request information about the collected data, to rectify, block or erase data</li> </ul>	<ul style="list-style-type: none"> <li>• During the registration phase, the end user is asked to read and accept the privacy policy and terms of use</li> <li>• The policy and the terms of use must be tailored to the specific end user, must meet the transparency obligations imposed by the applicable data protection legislation and must provide for easy means for data subjects to exercise their rights</li> <li>• In the cases where the legal ground for data processing is consent, the specific conditions for consent of Article 7 GDPR must be observed: <ul style="list-style-type: none"> <li>○ controller must be able to demonstrate that the data subject has consented to processing of his or her personal data</li> <li>○ request for consent must 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</li> <li>○ data subject must be informed of his/her the right to withdraw his or her consent at any time</li> </ul> </li> </ul>
8.	<b>Ensure limited retention of the collected personal data</b> <ul style="list-style-type: none"> <li>• Define the time period after which data will be deleted</li> <li>• Establish practices, policies and procedures to delete data</li> </ul>	<ul style="list-style-type: none"> <li>• In a production environment, a retention and deletion policy would have to be established by the end users, such as automatic erasure at regular intervals determined in accordance with any specific national laws which may establish statutory periods of retention</li> </ul>

		<ul style="list-style-type: none"><li>• There is no automatic procedure to delete the collected data and this must be done via remote connection to the captive portal UI</li></ul>
<b>9.</b>	<b>Limitations of the technology</b>	<ul style="list-style-type: none"><li>• The application requires internet access.</li></ul>

### C. Analysis of eVAMAPP

#	Recommendation	What actions have been taken in order to implement the recommendations?
1.	<p><b>Define a purpose of the processing of personal data:</b></p> <ul style="list-style-type: none"> <li>• The purpose has to be specific and clearly defined</li> <li>• The purpose has to be defined before the actual processing</li> </ul>	<ul style="list-style-type: none"> <li>• The development of a mobile (smartphone) application in eVACUATE aims to offer the subscribers with valid, up-to-date information about the crisis, location-specific indications on how to get help and indicate the Active Evacuation Route.</li> <li>• Additional goal is to acquire more information about both the emergency scene and assess the safety of the individual as well as to support the individuals in identifying threatening situations.</li> <li>• In the <b><i>cruise ship passenger app</i></b>, the purpose of processing personal data concerns (1) provision of safety and evacuation information and Active Evacuation Route to passengers and (2) provision of help to first responders to find their location in the cases when someone has gone missing or is not moving</li> <li>• In the <b><i>first responders app</i></b>, the purpose of processing personal data concerns (1) efficient management of alerts and (2) enabling communication between first responders about the actions taken regarding a specific alert</li> <li>• In the <b><i>missing persons app</i></b>, the purpose of processing personal data concerns helping muster personnel to find cruise passengers who have not mustered and who might be assumed to be in a need of rescue</li> </ul>
2.	<p><b>Define the legal basis for the processing:</b> <b>One of the following grounds could be selected:</b></p> <ul style="list-style-type: none"> <li>• The data subject's consent;</li> <li>• Necessary for the performance of a contractual obligation</li> <li>• Processing is necessary for compliance with a legal obligation to which the controller is subject;</li> <li>• Processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li>• Processing is necessary for the performance of a task</li> </ul>	<ul style="list-style-type: none"> <li>• The very nature of the eVACUATE mobile application offers a number of guarantees to ensure it is offered on a voluntary basis only. The individual's consent to the collection of data that will assist in the evacuation process is explicitly asked in the following occasions: <ul style="list-style-type: none"> <li>○ Before he/she starts to download the application: the user is notified that the use of the application will lead to the activation of Bluetooth to allow for identification of nearby beacons.</li> <li>○ The application will not start by default. The user needs to activate the application. However once activated, the</li> </ul> </li> </ul>

	<p>carried out in the public interest or in the exercise of official authority vested in the controller;</p> <ul style="list-style-type: none"> <li>• <b>Processing is necessary for the purposes of the legitimate interests pursued by the controller</b></li> </ul>	<p>application is ready to receive communication (notifications) about safety.</p> <ul style="list-style-type: none"> <li>• Even when the application is active, location is not tracked. This will only happen if an evacuation alert is issued by the relevant authorities when the app will receive a message that an emergency has been declared and that Bluetooth must be activated manually</li> <li>• Once location is approximated by the use of GPS (outdoors) or iBeacons (indoors), the infrastructure itself is totally passive, i.e. neither the GPS satellites, nor the iBeacons identify or store the IDs of the terminal devices receiving their signals.</li> </ul>
3.	<p><b>Ensure data accuracy and quality:</b></p> <ul style="list-style-type: none"> <li>• <b>Take measures to ensure that the collected data is adequate, relevant for which they are collected</b></li> </ul>	<ul style="list-style-type: none"> <li>• The data relevant to the visitor/passenger security are continuously updated by the application's back-end, which in turn communicates in real time with SOFIA.</li> <li>• As an example, a visitor/passenger is notified about a potentially dangerous situation using the push notification mechanism in iOS, even when the application is not active.</li> </ul>
4.	<p><b>Ensure data minimization:</b></p> <ul style="list-style-type: none"> <li>• <b>Take measures to ensure that the collected data is not excessive in relation to the purpose for which they are collected</b></li> </ul>	<ul style="list-style-type: none"> <li>• The data collected are the minimum required for the successful performance of the application role. The application does not keep unnecessary identity attributes. Data such as names and surnames, age, gender, etc. are not kept, only UserID.</li> <li>• The link between the UserID and the personal details is maintained by the central eVACUATE platform which adheres to the security and privacy measures explained in WP6.</li> <li>• In the scenario on a ship, only in the Missing Persons app, the Hospitality Information System is queried about the cabin number and personal information in case someone is missing.</li> <li>• In case of facial images, they will not be subjected to specific technical processing or be processed for unique identification of the natural person</li> <li>• It is recommended that in production environment, the 'push method' is used to inform the first responders on the necessary data for missing persons, ie information about them should be provided by, eg, the hotel, only upon receiving a list of missing persons (ie, without the app directly accessing the whole database)</li> </ul>

5.	<b>Ensure data integrity and security:</b> <ul style="list-style-type: none"> <li>• Take appropriate technical measures to prevent unauthorised disclosure or access to collected personal data</li> <li>• Take appropriate organisational measures to prevent unauthorised disclosure or access to collected personal data</li> </ul>	<ul style="list-style-type: none"> <li>• The application connects to the rest of the eVACUATE platform using the indicated protocols (HTTPS)</li> <li>• Personal data will be acquired by the eVACUATE system during registration of the user's smartphone application or, in the case of the cruise ship application, during the registration process at the ship's reception.</li> </ul>
6.	<b>Attribute responsibilities for the parties involved in processing:</b> <ul style="list-style-type: none"> <li>• Appoint the controller</li> <li>• Define other parties involved (e.g., processors or third parties)</li> </ul>	<ul style="list-style-type: none"> <li>• The personal information, as mentioned above, will be stored on the eVACUATE platform for reference only in case of an emergency. Any other personal information will be stored at the ship's Hospitality Information System (only in the case of cruise ships).</li> <li>• The facility's information officer (CIO) or the Chief Security Officer (CSO) are normally in charge of maintaining and deleting data stored in the database, according to the regulatory provisions of the industry (e.g. IMO, SOLAS regulations for ships).</li> <li>• The information from the eVACUATE Mobile App could be shared to first responders <b>only once an evacuation order is issued</b>.</li> <li>• Further recommendation is that the Emergency Operational Centre gains access to the identity and location data of the app's users only when there is a need to search for someone who has gone missing</li> <li>• Another data protection by design measure concerns storage of only the last known location in order to avoid continuous tracking of the app's users</li> </ul>
7.	<b>Ensure respect of data subjects' rights</b> <ul style="list-style-type: none"> <li>• Develop policies and procedures that would allow data subjects to request information about the collected data, to rectify, block or erase data</li> </ul>	<ul style="list-style-type: none"> <li>• It is technically feasible that a UserID is excluded from the use of the system. Once this UserID is revoked, the application stops to operate.</li> <li>• Data can be retained if required by the industry's regulatory provisions (e.g. IMO/SOLAS for cruise ships, the Spanish Football League safety regulations for the stadium, National Transport Safety authorities for Metro).</li> </ul>
8.	<b>Ensure limited retention of the collected personal data</b> <ul style="list-style-type: none"> <li>• Define the time period after which data will be deleted</li> </ul>	<ul style="list-style-type: none"> <li>• The time period after which the personal data are erased depends on either specific regulations or the facility operator's own security procedures.</li> </ul>

	<ul style="list-style-type: none"> <li>• Establish practices, policies and procedures to delete data</li> </ul>	
9.	<b>Limitations of the technology</b>	<ul style="list-style-type: none"> <li>• The application relies heavily on the ability of the smartphone to acquire a position estimated by either detecting a Bluetooth Beacon in its proximity or to receive GPS signals (mostly works in outdoors or open air facilities).</li> </ul>

#### D. Analysis of SoNeMa Platform

#	Recommendation	What actions have been taken in order to implement the recommendations?
1.	<b>Define a purpose of the processing of personal data:</b> <ul style="list-style-type: none"> <li>• The purpose has to be specific and clearly defined</li> <li>• The purpose has to be defined before the actual processing</li> </ul>	<ul style="list-style-type: none"> <li>• SoNeMa's purposes include: <ul style="list-style-type: none"> <li>○ Finding and evaluating conversations that take place in the social media and which relate to the validation demonstrations (purposes specifically for the validation demonstrations)</li> <li>○ Providing statistics on demographics, followers/fans, Klout score, sentiment analysis</li> </ul> </li> <li>• SoNeMa's purposes must be limited to identification of information on social networks that would inform the end user of an incident that is taking place or is about to take place on their premises</li> <li>• In a production environment, it must be proven that existing solutions used by end users are not sufficient to provide the information that SoNeMa will provide, ie it is required that SoNeMa is proved necessary response to safety and security issues experienced by the end users</li> <li>• In a production environment, end users are advised to assess whether SoNeMa will need to be permanently online so as to avoid disproportionate collection and further processing of user-generated content.</li> <li>• Particular measures to narrow the functionalities and operations of SoNeMa to the identified purposes could include: <ul style="list-style-type: none"> <li>○ Targeted content analysis, ie only content which has significance for an emergency situation</li> <li>○ Timespan of the content analysis, ie the analysis should be targeted at posts which happen in near real time and concern a present (emergency) situation</li> <li>○ Analytics on the collected data, ie they should not be extended to cover business purposes</li> <li>○ Prevention of incompatible processing, ie data should only be processed in the context of</li> </ul> </li> </ul>



		<p>emergency monitoring and not generally</p> <ul style="list-style-type: none"> <li>Retention and deletion policy must be adopted, especially regarding unnecessary or irrelevant content</li> </ul>
2.	<p><b>Define the legal basis for the processing:</b>  <b>One of the following grounds could be selected:</b></p> <ul style="list-style-type: none"> <li>The data subject's consent;</li> <li>Necessary for the performance of a contractual obligation</li> <li>Processing is necessary for compliance with a legal obligation to which the controller is subject;</li> <li>Processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li>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;</li> <li>Processing is necessary for the purposes of the legitimate interests pursued by the controller</li> </ul>	<ul style="list-style-type: none"> <li>SoNeMa offers the opportunity to search all types of content available on social networks which makes consent unsuitable legal ground since it cannot reasonably be obtained from everyone who is on social networks and who could potentially be targeted by SoNeMa.</li> <li>In the validation demonstrations, volunteers willing to participate in the testing of this technology were invited to post a hashtag #fp7evac on Twitter. Since this limited the scope of the search to this predefined hashtag, consent was an acceptable legal ground. As advised in Deliverable D11.3, another possible legal ground is necessity for the purposes of legitimate interests pursued by the controller, as established in Article 7 (f) Directive 95/46/EC. Since research is generally accepted as a legitimate interest but a balancing exercise with the interests and fundamental rights and freedoms of data subjects will still have to be carried out depending on the context.</li> <li>In a production environment, the impact of the General Data Protection Regulation should be taken into account. Pursuant to Article 6 (f) GDPR, processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party is not a valid legal ground in the context of processing carried out by public authorities in the performance of their tasks. Another possible legal ground to rely on could be processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6 (e) GDPR) but this is an assessment that will have to be carried out depending on the context within which the system is implemented.</li> </ul>
3.	<p><b>Ensure data accuracy and quality:</b></p> <ul style="list-style-type: none"> <li>Take measures to ensure that the collected data is adequate, relevant for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>The technical processing of the data is done by IBM's engine</li> <li>In order to make sure that the processed data are adequate and relevant, the keywords used in the search engine of the SoNeMa platform will have to be very</li> </ul>

		specific and precise. It will also contribute to meeting the data minimisation obligations.
4.	<b>Ensure data minimization:</b> <ul style="list-style-type: none"> <li>Take measures to ensure that the collected data is not excessive in relation to the purpose for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>SoNeMa will process data such as: <ul style="list-style-type: none"> <li>Profile name/alias</li> <li>Profile picture</li> <li>Content of social media posts</li> <li>Geographic location of the posts</li> <li>Statistical data such as demographic information, number of people checked in at the premises of the end user, sentiment of the posts collectively (ie, negative/positive)</li> <li>Followers of the end users</li> <li>Klout scores<sup>1</sup> of profiles that post content of interest</li> </ul> </li> <li>As long as the statistical data does not contain personally identifiable information, ie, it is fully anonymised, such data will not be considered personal data.</li> </ul>
5.	<b>Ensure data integrity and security:</b> <ul style="list-style-type: none"> <li>Take appropriate technical measures to prevent unauthorised disclosure or access to collected personal data</li> <li>Take appropriate organisational measures to prevent unauthorised disclosure or access to collected personal data</li> </ul>	<ul style="list-style-type: none"> <li>eVACUATE provides a secure communication architecture that enables different devices/users to access and share information in a secure and reliable manner protecting personal data against incidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access</li> <li>In a production environment, end users will also have to implement appropriate organisational measures to prevent unauthorised disclosure or access to personal data</li> </ul>
6.	<b>Attribute responsibilities for the parties involved in processing:</b> <ul style="list-style-type: none"> <li>Appoint the controller</li> <li>Define other parties involved (e.g., processors or third parties)</li> </ul>	<ul style="list-style-type: none"> <li>In the validation demonstrations, the controller was the end user. This will also be the case in a production environment where the controller decides to implement SoNeMa as part of an existing solutions or as a new solution</li> <li>The controller will have to observe the purpose limitation principles and not use the SoNeMa data for further processing extending beyond the scope of the purposes defined above</li> <li>The controller will have to collect only the minimum amount of data necessary to achieve the purposes and any additional data should be deleted</li> </ul>
7.	<b>Ensure respect of data subjects' rights</b>	<ul style="list-style-type: none"> <li>In the validation demonstrations, the data subjects were informed about data</li> </ul>

<sup>1</sup> Social media analytics ranking users according to online social influence

	<ul style="list-style-type: none"> <li>• <b>Develop policies and procedures that would allow data subjects to request information about the collected data, to rectify, block or erase data</b></li> </ul>	<p>processing through the information and consent form</p> <ul style="list-style-type: none"> <li>• In a production environment, data controllers will have to ensure compliance with the extended transparency obligations under the General Data Protection Regulation (Article 12-14 GDPR)</li> <li>• The information must be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (Article 12 GDPR)</li> <li>• An important exception from the obligation to provide information where personal data have not been obtained from the data subject, is contained in Article 14 (5) (b) GDPR which discharges the controller of its obligation if the provision of such information proves impossible or would involve a disproportionate effort. It is likely that a controller could rely on this in the case of collection of data from social networks. However, the data controller must still take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available</li> </ul>
8.	<b>Ensure limited retention of the collected personal data</b> <ul style="list-style-type: none"> <li>• <b>Define the time period after which data will be deleted</b></li> <li>• <b>Establish practices, policies and procedures to delete data</b></li> </ul>	<ul style="list-style-type: none"> <li>• Data retention and deletion policy should be adopted by the data controller in a production environment</li> <li>• eVACUATE is focused on providing real or near-real time response to events and the analysis of the user-generated content on social networks will be carried out in a limited time span. This circumstance should be reflected in the controller's policy and practices should be adopted at an organisational level to make sure that data are not further processed</li> </ul>
9.	<b>Limitations of the technology</b>	<ul style="list-style-type: none"> <li>• SoNeMa operates with public content only accessible via public channels</li> </ul>

## E. Analysis of crowd behaviour detection technology

#	Recommendation	What actions have been taken in order to implement the recommendations?
1.	<b>Define a purpose of the processing of personal data:</b> <ul style="list-style-type: none"> <li>• The purpose has to be specific and clearly defined</li> <li>• The purpose has to be defined before the actual processing</li> </ul>	<ul style="list-style-type: none"> <li>• In the validation demonstrations, the purpose was narrowly specified as studying crowd behaviour as part of designing the Active Evacuation Route (AER) and identifying potential threats in the venue</li> <li>• In a production environment, the purpose will likely be similar but it should be clear and specific enough to avoid illegal data processing and to make sure that each feature of the technology is indeed necessary and proportionate.</li> <li>• The purpose of the technology is not to identify individuals but rather to perform automated analysis of crowd behaviour and possibly the behaviour of specific individuals or small groups of individuals</li> <li>• Behavioural and psychological characteristics are considered 'soft' biometrics and they make certain features of the human body machine-readable and subject to further analysis and use. In eVACUATE, these characteristics are only used for categorisation (and not identification), that is to say, assigning individuals to a specific group of predefined characteristics and possible taking actions on the basis of this categorisation.</li> </ul>
2.	<b>Define the legal basis for the processing:</b> <b>One of the following grounds could be selected:</b> <ul style="list-style-type: none"> <li>• The data subject's consent;</li> <li>• Necessary for the performance of a contractual obligation</li> <li>• Processing is necessary for compliance with a legal obligation to which the controller is subject;</li> <li>• Processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li>• Processing is necessary for the performance of a task carried out in the public</li> </ul>	<ul style="list-style-type: none"> <li>• The legal basis for the processing will depend on the organisational context within which the behaviour monitoring software will be implemented: <ul style="list-style-type: none"> <li>◦ Directive 95/46/EC stipulates that processing of sound and image data, such as in cases of video surveillance, does not come within the scope of the directive if it is carried out for the purposes of public security (recital 16)<sup>2</sup></li> <li>◦ GDPR stipulates that it is not applicable to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the</li> </ul> </li> </ul>

<sup>2</sup> However, the notion of public security is subject to interpretation on a case-by-case basis.

	<p>interest or in the exercise of official authority vested in the controller;</p> <ul style="list-style-type: none"> <li>• <b>Processing is necessary for the purposes of the legitimate interests pursued by the controller</b></li> </ul>	<p>execution of criminal penalties, including the safeguarding against and the prevention of threats to public security</p> <ul style="list-style-type: none"> <li>• Since the processing necessary for legitimate interests is not applicable under the GDPR to processing carried out by public authorities in the performance of their tasks, a likely possible legal ground seem to be necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</li> <li>• In the validation demonstrations, the controller relied on consent as a legal ground and this was deemed acceptable in the limited space and time of the demonstration</li> <li>• In a production environment, the legal ground will have to be given careful consideration depending on the private/public nature of the controller and their obligations</li> </ul>
3.	<p><b>Ensure data accuracy and quality:</b></p> <ul style="list-style-type: none"> <li>• <b>Take measures to ensure that the collected data is adequate, relevant for which they are collected</b></li> </ul>	<ul style="list-style-type: none"> <li>• In the validation demonstrations, the accuracy of the crowd detection algorithms seems to have improved significantly compared to the reported difficulties experienced in 2015 (D11.3, p. 31).</li> <li>• Algorithms proved to be versatile and sensitive so the enacted unusual behaviour in the loops was detected but also unusual behaviour appearing by chance was also correctly detected.<sup>3</sup></li> </ul>
4.	<p><b>Ensure data minimization:</b></p> <ul style="list-style-type: none"> <li>• <b>Take measures to ensure that the collected data is not excessive in relation to the purpose for which they are collected</b></li> </ul>	<ul style="list-style-type: none"> <li>• The crowd behaviour detection technology relies on data from optical cameras of which only the optical cameras potentially allow identification of individuals. However, the aggregated data from the three types of cameras (ie, optical, thermal and hyperspectral (infrared)) could reveal further information about crowds and individuals</li> <li>• Facial images of natural persons should not be used for identification since this entails the application of the stricter set of rules of the GDPR regarding the (special technical) processing of special categories of data (potentially, biometric data used for unique identification of natural persons)</li> <li>• Data from behaviour detection algorithms should not be linked to data about identifiable persons since this increases the</li> </ul>

<sup>3</sup> As reported by ITINNOV.

		risk of identification, singling out and categorisation of individuals
5.	<b>Ensure data integrity and security:</b> <ul style="list-style-type: none"> <li>• Take appropriate technical measures to prevent unauthorised disclosure or access to collected personal data</li> <li>• Take appropriate organisational measures to prevent unauthorised disclosure or access to collected personal data</li> </ul>	<ul style="list-style-type: none"> <li>• eVACUATE provides a secure communication architecture that enables different devices/users to access and share information in a secure and reliable manner protecting personal data against incidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access</li> <li>• In a production environment, end users will also have to implement appropriate organisational measures to prevent unauthorised disclosure or access to video recordings and other personal data</li> </ul>
6.	<b>Attribute responsibilities for the parties involved in processing:</b> <ul style="list-style-type: none"> <li>• Appoint the controller</li> <li>• Define other parties involved (e.g., processors or third parties)</li> </ul>	<ul style="list-style-type: none"> <li>• In the validation demonstrations, the controller was the end user. This will also be the case in a production environment where the controller decides to implement the crowd behaviour detection technology as part of an existing solutions or as a new solution</li> <li>• The controller will have to observe the purpose limitation principles and not use data for further processing extending beyond the scope of the purposes defined above</li> <li>• The controller will have to collect only the minimum amount of data necessary to achieve the purposes and any additional data should be deleted</li> </ul>
7.	<b>Ensure respect of data subjects' rights</b> <ul style="list-style-type: none"> <li>• Develop policies and procedures that would allow data subjects to request information about the collected data, to rectify, block or erase data</li> </ul>	<ul style="list-style-type: none"> <li>• In the validation demonstrations, the data subjects were informed about data processing through the information and consent form</li> <li>• In a production environment, data controllers will have to ensure compliance with the extended transparency obligations under the General Data Protection Regulation (Article 12-14 GDPR)</li> <li>• The information must be provided to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (Article 12 GDPR)</li> <li>• An important exception from the obligation to provide information where personal data have not been obtained from the data subject, is contained in Article 14 (5) (b) GDPR which discharges the controller of its obligation if the provision of such information proves impossible or would involve a</li> </ul>



		<p>disproportionate effort. However, the data controller must still take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available</p> <ul style="list-style-type: none"> <li>• A possible means of ensuring transparency could be the use of information notices explaining the new features of the technology compared to traditional CCTV. This will also be the case where the traditional (legacy) CCTV system is used but is combined with the crowd behaviour detection technology.</li> </ul>
8.	<b>Ensure limited retention of the collected personal data</b> <ul style="list-style-type: none"> <li>• Define the time period after which data will be deleted</li> <li>• Establish practices, policies and procedures to delete data</li> </ul>	<ul style="list-style-type: none"> <li>• Data retention and deletion policy should be adopted by the data controller in a production environment</li> <li>• eVACUATE is focused on providing real or near-real time response to events and the analysis of video streams may not always be required. However, it is within the end user's discretion to determine whether the technology will be operational at all times and whether it will meet the necessity criterion. In order to assess the impact of the system in these cases, a data protection impact assessment is recommended prior to implementation of this technology</li> </ul>
9.	<b>Limitations of the technology</b>	

## F. Analysis of the counting technology

#	Recommendation	What actions have been taken in order to implement the recommendations?
1.	<p><b>Define a purpose of the processing of personal data:</b></p> <ul style="list-style-type: none"> <li>• The purpose has to be specific and clearly defined</li> <li>• The purpose has to be defined before the actual processing</li> </ul>	<ul style="list-style-type: none"> <li>• The purpose of the processing, is to detect the number of people present in an area.</li> <li>• This is necessary in order to populate areas in the COP, with a specific and accurate number of people.</li> </ul>
2.	<p><b>Define the legal basis for the processing:</b></p> <p>One of the following grounds could be selected:</p> <ul style="list-style-type: none"> <li>• The data subject's consent;</li> <li>• Necessary for the performance of a contractual obligation</li> <li>• Processing is necessary for compliance with a legal obligation to which the controller is subject;</li> <li>• Processing is necessary in order to protect the vital interests of the data subject or of another natural person;</li> <li>• 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;</li> <li>• Processing is necessary for the purposes of the legitimate interests pursued by the controller</li> </ul>	<ul style="list-style-type: none"> <li>• The legal basis for the processing will depend on the organisational context: <ul style="list-style-type: none"> <li>◦ Directive 95/46/EC stipulates that processing of sound and image data, such as in cases of video surveillance, does not come within the scope of the directive if it is carried out for the purposes of public security (recital 16)<sup>4</sup></li> <li>◦ GDPR stipulates that it is not applicable 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, including the safeguarding against and the prevention of threats to public security</li> </ul> </li> <li>• Since the processing necessary for legitimate interests is not applicable under the GDPR to processing carried out by public authorities in the performance of their tasks, a likely possible legal ground seem to be necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller</li> <li>• In the validation demonstrations, the controller relied on consent as a legal ground and this was deemed acceptable in the limited space and time of the demonstration</li> <li>• In a production environment, the legal ground will have to be given careful consideration depending on the private/public nature of the controller and their obligations</li> </ul>

<sup>4</sup> However, the notion of public security is subject to interpretation on a case-by-case basis.



3.	<b>Ensure data accuracy and quality:</b> <ul style="list-style-type: none"> <li>Take measures to ensure that the collected data is adequate, relevant for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>The amount of true positives in relation to the few false positives and negatives resulted into significant high accuracy rates</li> </ul>
4.	<b>Ensure data minimization:</b> <ul style="list-style-type: none"> <li>Take measures to ensure that the collected data is not excessive in relation to the purpose for which they are collected</li> </ul>	<ul style="list-style-type: none"> <li>The video is of low resolution (at best 640x480) which is enough for this application but at the same time prohibits the data controller from perform facial recognition on the acquired imagery</li> </ul>
5.	<b>Ensure data integrity and security:</b> <ul style="list-style-type: none"> <li>Take appropriate technical measures to prevent unauthorised disclosure or access to collected personal data</li> <li>Take appropriate organisational measures to prevent unauthorised disclosure or access to collected personal data</li> </ul>	<ul style="list-style-type: none"> <li>In the validation demonstrations, training datasets are stored in secure locations on the processor's premises, protected physically (security doors, alarms) and digitally (password protection, encryption).</li> <li>In a production environment, data controllers are advised to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with Article 32 GDPR</li> </ul>
6.	<b>Attribute responsibilities for the parties involved in processing:</b> <ul style="list-style-type: none"> <li>Appoint the controller</li> <li>Define other parties involved (e.g., processors or third parties)</li> </ul>	<ul style="list-style-type: none"> <li>In the validation demonstrations, the respective end user was a data controller and ICCS was a data processor</li> <li>In a production environment, the controller will likely be the end user of the technology</li> </ul>
7.	<b>Ensure respect of data subjects' rights</b> <ul style="list-style-type: none"> <li>Develop policies and procedures that would allow data subjects to request information about the collected data, to rectify, block or erase data</li> </ul>	<ul style="list-style-type: none"> <li>In the validation demonstrations, the controller provided the data subjects with information about their rights and has also provided a list of the processors with respective contact details where data subjects could get more information and/or exercise their rights.</li> <li>No requests have been made by the controllers or any individuals for access to the thermal/hyperspectral videos.</li> </ul>
8.	<b>Ensure limited retention of the collected personal data</b> <ul style="list-style-type: none"> <li>Define the time period after which data will be deleted</li> </ul>	<ul style="list-style-type: none"> <li>All frames are automatically deleted shortly (1-2 sec) after they are technically processed by the system.</li> <li>In the validation demonstrations, training datasets are stored in secure locations, on the processor's premises, protected physically (security doors, alarms) and digitally</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Establish practices, policies and procedures to delete data</b></li> </ul>	<p>(password protection, encryption). They will be deleted in accordance with the retention period specified in the consent form and the data processing agreements executed between the data controller and the data processors.</p>
9.	<b>Limitations of the technology</b>	<ul style="list-style-type: none"> <li>• The algorithmic implementation supports detection of moving crowds, not stationary. In order to install the system at a different location, and have it operational, some procedures are required to calculate the geometry of the scene.</li> </ul>

### **3 Overview of the impact of the General Data Protection Regulation on eVACUATE**

This chapter provides an initial assessment of the regulatory impact of the General Data Protection Regulation on eVACUATE. This analysis aims to familiarise potential end users considering the implementation of eVACUATE in a production environment with the new obligations they may have as data controllers. The purpose of this overview is to present some of the challenging aspects of the GDPR such as the data protection impact assessment, transparency obligations and new data subjects' rights.

#### **3.1 Territorial scope**

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, regardless of whether the processing takes place in the Union or not. Furthermore, the provision of Article 3 (3) GDPR stipulates that the regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

A reasonable question in the context of eVACUATE could be whether the GDPR applies to processing of personal data on ships sailing on high seas, ie all parts of the sea that are not included in the territorial sea or in the internal waters of a state.

The general rule in international law is that a ship on the high seas is subject only to international law and the laws of the flag state. Thus, Article 92 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS III) stipulates that ships shall sail under the flag of one state only and, save in exceptional cases expressly provided for in international treaties or in this convention, shall be subject to its exclusive jurisdiction on the high seas. This means that, in the common case, the jurisdiction of an EU Member State shall be extended also to ships sailing under its flag which means that the GDPR will also be applicable in this case, regardless of whether the controller has establishment in the EU or not.

#### **3.2 The notion of 'personal data'**

The GDPR provides a slightly modified definition of 'personal data' in Article 4 (1) so as to reflect the developments of the last decade. Thus, references to how a natural person could be identified include identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

This implies that, to the extent identification numbers or location data processed in eVACUATE allow for the identification of a natural person, these data should in all cases be treated as personal data and their processing shall be subject to the provisions of the GDPR.

#### **3.3 Accountability**

It is noteworthy that the GDPR introduced among the principles relating to processing of personal data in Article 5 the principle of accountability. In the context of eVACUATE, this principle implies that data controllers are responsible and must be able to demonstrate compliance with the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.

The principle of accountability was elaborated by Article 29 Working Party in Opinion 3/2010 on the principle of accountability. The principle of accountability encourages data controllers to apply measures that “deliver the outcomes of the data protection principles”.<sup>5</sup> Examples of such measures include, more specifically, identification of data processing operations<sup>6</sup>, response to access requests, allocation of resources, designation of individuals responsible for the organisation of data protection compliance, such as data protection officers etc.

A reflection of the principle of accountability could be seen in the conditions for consent established by Article 7 GDPR. This provision stipulates that when 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.

Thus, for eVACUATE end users it would be very important to observe and comply with the principle of accountability by not only implementing the principles of processing of personal data but also by being able to demonstrate compliance with them, eg, by maintaining sufficiently well documented records.

### **3.4 Lawfulness of processing**

#### **A. Legitimate interests and public authorities**

It has already been mentioned above that necessity for the purposes of the legitimate interests pursued by the controller or by a third party will no longer be a valid legal ground when it comes to processing carried out by public authorities in the performance of their tasks. This should be carefully observed by data controllers and they should always check if the legal ground they are relying on to process personal data is indeed valid.

Also, it is worth mentioning that the GDPR provides guidance to data controllers who wish to process personal data for a purpose other than that for which the personal data have been collected. Article 6 (4) stipulates that where such processing is not based on the data subject's consent or on a EU 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: (1) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; (2) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; (3) 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; (4) the possible consequences of the intended further processing for data subjects; (5) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

#### **B. Consent**

---

<sup>5</sup> Article 29 Working Party, Opinion 3/2010 on the principle of accountability, p. 19.

<sup>6</sup> This is also an explicit requirement imposed by Article 30 GDPR which requires that a controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

The GDPR introduces some conditions for consent in Article 7. Thus, it prescribes that 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. The consequence of non-compliance with this provision is that any part of such a declaration which constitutes an infringement of the GDPR shall not be binding.

Additionally, data subjects have the right to withdraw their consent at any time. In order to protect data controllers, the GDPR provides that the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. The GDPR requires that data controllers inform the data subject about their right to withdraw prior to giving consent. Furthermore, it must be as easy to withdraw as to give consent.

The provision of Article 7 also provides guidance on assessing whether consent is freely given. It stipulates that some of the criteria for this assessment include whether 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.

Thus, in cases where the end user of eVACUATE relies on consent for some of the data processing activities, they should demonstrate compliance with this requirement and they should always provide the data subject with the opportunity to withdraw their consent.

### **C. Processing which does not require identification**

The GDPR also provides in Article 11 that if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR.

The provision further specifies that where in these cases the controller is able to demonstrate it is not in a position to identify the data subject, the data subject must be informed accordingly, if possible. In these case the rights to access, rectification, erasure, restriction of processing and data portability are not applicable unless the data subject provides additional information for the purpose of exercising these rights and this information enables his or her identification.

This impact of provision is particularly important in the cases where personal data are processed but they do not require the identification of a data subject as it relaxes some of the controller's obligations.

## **3.5 Transparency**

The GDPR tightens the transparency obligations of data controllers in obliging them to provide particular information to data subjects in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (Article 12 GDPR). The information must be provided in writing, including by electronic means and when requested by the data subject, it may also be provided orally if the identity of the data subject is proven by other means.

The controller is obliged to provide the information on actions taken on requests for exercising the data subjects' rights to the data subjects within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Information should be provided free of charge except where the requests are "manifestly unfounded or excessive ... repetitive" but

only with reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested.

The information that has to be provided to the data subjects for personal data collected from the data subjects must contain at least the elements outlined in Article 13 GDPR and it must be provided at the time when personal data are obtained. In the case where the personal data have not been obtained from the data subject, the controller must provide the information (1) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed or (2) at the latest at the time of the first communication to that data subject (if the personal data are to be used for communication with the data subject) or (3) at the latest when the personal data are disclosed (if a disclosure to another recipient is envisaged).

In the context of eVACUATE, data controllers should take care of ensuring full compliance with the enhanced transparency obligations under the GDPR, especially where personal data has not been obtained from the data subjects.

### **3.6 Rights of the data subjects**

The GDPR codified some new rights of the data subjects explicitly, such as the right to erasure and the right to data portability. This analysis will only focus on these three rights and their possible impact on eVACUATE's end users.

#### **A. Right to be forgotten**

The right to be forgotten concerns the data subject's right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller's obligation to erase personal data without undue delay. It is noteworthy that the right to erasure, colloquially 'right to be forgotten', applies where one of six specific grounds outlined in Article 17 (1) GDPR is present. These grounds include:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

There are five exceptions where the controller may refuse to comply with the data subject's request for exercising the right to erasure (Article 17 (3) GDPR). These exceptions are applicable where the processing is necessary for:

- exercising the right of freedom of expression and information;
- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to



- in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- the establishment, exercise or defence of legal claims

In the case of eVACUATE, it is reasonable to assume that in many cases the controller might be required by national law to process the data or it may be necessary for the performance of a task carried out in the public interest or exercise of official authority vested in the controller. The notion of public interest is also a very broad one and will have to be interpreted in the context of the specific processing activity. In any case, controllers should aim at observing this right of the data subjects and comply with it unless one of the exceptions apply.

### **B. Right to data portability**

The right to data portability essentially refers to the right of the data subject to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided (Article 20 GDPR). This right may only be exercised where:

- processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
- the processing is carried out by automated means

The right to data portability does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. It is unlikely that this right will be applicable in the context of eVACUATE since it is aimed at preventing vendor lock-in for data subjects and it is hard to find a situation within the scope of eVACUATE where the data subject might want to exercise this right.

### **C. Right to object**

The right to object is not new as it was already present in Directive 95/46/EC. However, in the GDPR its scope was extended to cover profiling (Article 21 GDPR). The GDPR defines 'profiling' as any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4 (4) GDPR).

Thus, in the context of eVACUATE, the evaluation of behaviour and location or movements of individuals could potentially fall within the ambit of this definition. Article 21 (1), first sentence *in fine* prescribes that the data subject has the right to object at any time to processing of personal data concerning him or her which is based on (1) processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or (2) processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party, including profiling based on these provisions.

The principle is that upon receiving such as request, the controller must no longer process the personal data. An exception is foreseen for the cases where the controller can demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

### 3.7 Data protection by design and by default

Data protection by design, also known as ‘privacy by design’, is now explicitly mandated as an obligation of the controller. Article 25 GDPR prescribes that the controller is obliged, both at the time of the determination of the means for processing and at the time of the processing itself, to implement appropriate technical and organisational measures 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 the GDPR and protect the rights of data subjects.

In line with the traditional notion of privacy enhancing technologies, the GDPR seems to require from data controllers to implement technical measures which ‘enforce’ the main data protection principles. In choosing such measures, the controller must take into account:

- the state of the art
- the cost of implementation
- the nature, scope, context and purposes of processing
- the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Furthermore, the controller is also obliged to implement “appropriate technical and organisational measures” to ensure that *by default* only personal data necessary for each specific purpose of the processing are processed and that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons. The obligation extends to cover:

- the amount of personal data collected
- the extent of their processing
- the period of their storage
- the data's accessibility

It is noteworthy that this obligation does not extend to producers of the products, services and applications that are based on the processing of personal data or process personal data to fulfil their task. Recital 78 of the GDPR only “encourages” them to consider the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. While market-driven mechanisms will ensure *de facto* compliance with this recommendation, it is regrettable that this stipulation did not find a place in the provisions of the GDPR as a legal obligation.

Recital 78 also provides an indicative list of measures which meet the principles of data protection by design and by default. These could include, for example, minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features.

In the context of eVACUATE, several successfully implemented data protection by design and by default measures could be pointed out.

- The **RFID technology** only counts the number and type of individuals but does not show the direction of their movement; the tags are not individualised and do not contain names or other unique identifiers; interlinkage with other data can only be made once an evacuation is declared; recommendations have been made to the end users, as data controllers, to adopt clear and strict policies to meet their transparency, security, data retention and access control obligations;
- The **MobiMESH Wi-Fi** technology requires only a minimum amount of data necessary to provide its core functionality and to meet the identified purpose; recommendations have been made to data controllers in a production environment



on how to strengthen further their compliance by ‘soft’ measures such as adoption of internal policies.

- The **eVAMAPP applications** obtain devices’ location data only when an evacuation is declared and Bluetooth connection has to be manually activated; identity and location of a person are only available to the responsible personnel if someone has been declared missing and they need to be located in order to be rescued; a recommendation has been made that only the last known location of the data subject should be stored to avoid permanent tracking; a recommendation has been made that passengers’ database (for example, in the case of a ship) and the missing persons application should only communicate via ‘push method’, ie only the data about the missing persons is sent to the application by the server.
- The **SoNeMa platform** has been recommended to consider anonymization techniques, narrowing of the purposes, avoiding data mining if security or safety-related events can be identified without accessing social network data; the platform must avoid applying business analytics on the collected data; SoNeMa does not perform searches for the present location of a data subject; recommendations have been made to data controllers to consider and define strict and clear policy for deletion of unnecessary data and limiting the scope of the key words used to query the search engine.
- Regarding the **(crowd) behaviour detection** technology, data controllers are advised to consider whether this technology should be operational at all times in order to mitigate the risks of singling out and behavioural analysis of individuals.
- Regarding the **counting technology**, the quality of the video does not allow the performing of facial recognition by data controllers and the frames are deleted immediately after the technical processing has completed.

Further data protection by design and by default measures could be implemented by the data controllers when a full-scale data protection impact assessment has been carried out and the complete set of risks has been established.

### 3.8 Data protection impact assessment

The GDPR introduced for the first time in the EU legislation on data protection the requirement for data protection impact assessment. The more widely known term ‘privacy impact assessment’ is used interchangeably in literature and practice.

The Article 29 Working Party recognised data protection impact assessment as an “important tool for accountability” and an enabler for data controllers to both comply with the regulation’s requirements and demonstrate that appropriate measures have been taken.<sup>7</sup>

In the GDPR, the provisions of Article 35 and 36 set the main principles of data protection impact assessment. Article 35 (1) provides that the controller is obliged to carry out “an assessment of the impact of the envisaged processing operations on the protection of personal data” prior to the processing. Provided the notion of ‘processing’ employed by the data protection legislation is extremely broad, this means that the exercise must in practice be carried out prior to any collection of data.

Keeping in line with the ‘risk-based approach’, the GDPR does not mandate a data protection impact assessment in all cases. It is only required for types of processing

---

<sup>7</sup> WP29 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017, WP 248, p. 4, available at: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44137](http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

which are “likely to result in a high risk to the rights and freedoms of natural persons”. Criteria for evaluation of likelihood of a high risk are provided by both the GDPR and the Article 29 Working Party in its Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, adopted on 4 April 2017, WP 248. The controller must take into account the nature, scope, context and purposes of the processing.

The texts of recitals 89, 91 and Article 35 (1) and (3) GDPR seem to imply that whenever a new data processing technology is being introduced, a data protection impact assessment is likely to be necessary.

Article 35 (3) GDPR provides an indicative but non-exhaustive list of processing activities which are “likely to result in high risks”. In these cases a data protection impact assessment is deemed mandatory. These cases include:

- 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.
- 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.

The provision of recital 75 indicates that at least the following types of activities may give rise to risks to the rights and freedoms of natural persons:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
  - where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
  - where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures (emphasis added);
  - where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
  - where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.
- Systematic monitoring of a publicly accessible area on a large scale

In line with the principles of data protection by design and by default, the GDPR mandates that a data protection impact assessment must be carried out prior to the processing. The

party responsible for ensuring that a data protection impact assessment has been carried out is the controller who is also the ultimately accountable party. The controller is obliged to seek the advice of the data protection officer and of the data subjects or their representatives.

A typical data protection impact assessment must contain at least the elements outlined in Article 35 (7) and recitals 84 and 90. These elements include:

- Description of the envisaged processing operations and the purposes of processing
- Assessment of the necessity and proportionality of the processing
- Assessment of the risks to the rights and freedoms of data subjects
- Measures envisaged to address the risks and demonstrate compliance with the regulation

In the context of eVACUATE, it is reasonable to assume that a data protection impact assessment will be required prior to any implementation of the system in a production environment. Whether the system falls within the ambit of the any of the situations described in the indicative list in the GDPR, depends on the particular scenario. For example, will the implementation of the eVACUATE solution in the system of a city underground be considered as a ‘systematic monitoring of a publicly accessible area on a large scale’?

The GDPR does not specifically define the notions of ‘systematic monitoring’ or ‘large scale’. Some guidance could be found in recital 91. According to the recital’s text, large-scale processing operations “aim to process a considerable amount of personal data at regional, national or supranational level ... which could affect a large number of data subjects and which are likely to result in a high risk, for example, on account of their sensitivity, where in accordance with the achieved state of technological knowledge a new technology is used on a large scale as well as to other processing operations which result in a high risk to the rights and freedoms of data subjects, in particular where those operations render it more difficult for data subjects to exercise their rights”. Particularly, a data protection impact assessment is necessary when monitoring publicly accessible areas using optic-electronic devices or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale.

Thus, end users considering eVACUATE in a production environment will also have to check local compliance with decisions and other acts of the supervisory authorities concerned which might classify certain operations as posing ‘high risks’ per se.

## 4 Privacy and data protection compliance recommendations for end users of eVACUATE

While it is almost impossible to provide a complete list of recommendations for each possible use of eVACUATE in a production environment, the following list of recommendations aims to help potential end users of the eVACUATE solution in meeting their compliance obligations. Each of these recommendations should be further consulted with the data protection officer (if applicable) and with the legal department of the data controller. In many cases, national specifics will nuance the compliance with one recommendation or another, but in any case these recommendations are aimed at facilitating the controller's task in ensuring full compliance with the applicable privacy and data protection legislation.

These general recommendations are aimed more specifically at ensuring compliance with the novel elements introduced by the General Data Protection Regulation and should be read in light of the recommendations and findings of all deliverables in Work Package 11.

- The **purposes** of processing for each component of the eVACUATE solution should be clearly identified, specific, explicit and legitimate; the indicated purposes of the technology could be further specified by the end user.
- The appropriate **legal ground for lawful processing** should be elaborated; consent is not always applicable and it is incumbent on the data controller to identify the proper legal basis for the processing activity. It should be borne in mind that processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party under the GDPR can no longer be applied by public authorities in the performance of their tasks. Whenever consent is relied upon, the controller must take care to ensure full compliance with the GDPR's conditions for obtaining of a valid consent.
- **Information** about: the processing activity, the controller, the purposes, the recipients, the storage period or the criteria used for calculation of this period, the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, the right to lodge a complaint with a supervisory authority, whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data, and the existence of automated decision-making, including profiling, must be provided to the data subject in a **concise, transparent, intelligible and easily accessible form**, using **clear and plain language**. Information notices should reflect the novel features of technologies that are relatively known amongst data subjects, such as video surveillance.

- **Data protection by design and by default** measures should be taken in accordance with the prescriptions for each particular technology by implementing data minimisation techniques, including through providing for very specific purposes, transparency with regard to the functions and processing of personal data (see previous recommendation), enabling effective control of the data subject over the processed personal data about him or her, and enabling the controller to create and improve security features. Whenever identification of a data subject is not required, it should in all cases be avoided and personal data should be kept to a minimum and only for the purposes for which they have been initially collected.
- Data subjects should be provided with sufficiently elaborated mechanisms for **control and access** to the personal data concerning them. Controllers must provide a **copy** of the personal data undergoing processing and where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form, such as PDF.
- Personal data must be 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. Whenever facial images are processed, especially using data mining and matching algorithms, unique identification of natural persons should not be performed since this entails a stricter set of rules concerning special categories of data ('sensitive data').
- Personal data must be processed in a manner that ensures **appropriate security** of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, in accordance with the data security measures applied in eVACUATE. In particular, data controllers could envisage measures such as pseudonymisation and encryption of personal data, 'hardening' of processing systems and services, ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, schedule for regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures.
- End users should carry out a **data protection impact assessment** prior to the implementation of eVACUATE's technologies in order to identify the risks to the fundamental rights and freedoms of data subjects resulting from the envisaged data processing activities and ensure compliance with the General Data Protection Regulation. Where appropriate, such as, for example, in large-scale processing in public places, the controller must seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. The controller must consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

- End users should appoint a **data protection officer**, if they have not done so already, even if their activity does not fall within the mandatory scope of activities which necessitate the designation of a data protection officer. End users should involve the data protection officer properly and in a timely manner in all issues which relate to the protection of personal data, including the data protection impact assessment.



## 5 Conclusions

This deliverable presented an assessment of the privacy and data protection compliance framework of the eVACUATE project, as evaluated in the previous tasks and during the four validation demonstrations.

It analysed the different elements of the eVACUATE solution from an ethical, privacy and data protection perspective and provided a summary of the insights on the impact of the technology on individuals' rights as observer during the demonstrations. The deliverable laid specific emphasis on the regulatory impact of the entry into force of the General Data Protection Regulation (GDPR) on the different elements of eVACUATE and paid attention to the data protection by design and by default measures considered in the context of eVACUATE.

Finally, it provided future-proof recommendations for end users when considering the implementation of eVACUATE in a production environment and also provides guidance on the new requirement of the GDPR of conducting a data protection impact assessment (DPIA).

The outcomes of the privacy and data protection analysis could be summarised as follows:

- **RFID** technology provides for detailed information for the data subjects, its use is entirely voluntary and sufficient safeguards respecting the data subjects' rights have been suggested; data minimisation techniques have been implemented such as non-individualisation of the chipless RFID tags and not using unique identification numbers; clear retention periods or criteria for determining such periods must be established in a production environment.
- **MobiMESH** technology has clearly defined purposes and processes proportionate amount of data to the defined purposes of processing; data security measures have been implemented; in a production environment, data controllers should elaborate a clear privacy policy and terms of use, taking into account the conditions for valid consent of Article 7 GDPR (if consent is relied upon); clear retention periods or criteria for determining such periods must be established in a production environment.
- **eVAMAPP** applications are used on a purely voluntary basis; compliance with the GDPR's intensified information and transparency obligations is essential; data protection by design and by default measures have been implemented: device's location is not tracked, GPS satellites and iBeacons are not used to identify or store the IDs of the terminal devices, applications do not store unnecessary identity attributes; the key moment for activation of identification functions is proportionately related to the moment of declaring an evacuation.
- **SoNeMa** technology provides for targeted content analysis but it should be performed in a limited timespan, eg, when an emergency is clearly present; the legal ground for processing must be carefully assessed by the controller in a production environment.
- **Crowd behaviour detection** technology has narrowly defined purposes and does not perform identification of natural persons; it has improved accuracy; facial images from optical cameras should not be processed to perform identification; data from behaviour detection algorithms should not be linked with data about identifiable persons; transparency obligations are key, especially when combining this technology with relatively known legacy technologies, such as CCTV; the technology should not be active at all times.



- **Counting** technology has clearly defined purposes and improved data accuracy; data minimisation includes video of low quality which does not allow for performing facial recognition operations and automatic deletion of frames shortly after their technical processing by the system

These findings should be taken into the broader framework of the legal and ethical analysis carried out in the framework of Work Package 11. The implementation of parts of the eVACUATE solution in a production environment will require a case-by-case assessment of these recommendations by the respective data controller(s). Data controllers should keep in mind the new requirements of the General Data Protection Regulation, particularly with respect to the conditions for obtaining valid consent, the legal grounds for personal data processing, the enhanced transparency obligations, the rights of data subjects and the new requirements for designation of data protection officers and carrying out of a data protection impact assessment. This will ensure not only legal and ethical compliance of the practical implementation of a system relying on (parts of) the eVACUATE solution with the existing regulatory landscape but will also make it future-proof in the context of the GDPR and the developments at Member States level associated with its application from 25 May 2018.

## 6 Appendix I: Information and consent forms

### 6.1 Information and consent form for Anoeta Stadium Real Sociedad (ASRS) validation demonstration

<p style="text-align: center;"><b>CONSENT FORM</b></p> <p>In the context of the European Union's Seventh Framework Programme for Research, Technological Development and Demonstration (FP7), the project eVACUATE has received funding under Grant Agreement No. 313161. The project aims to address the needs of the safety of citizens during complex evacuation processes following normal and abnormal events (crises) towards the creation of a comprehensive system that will be able to identify, designate and sustain a dynamic Active Evacuation Route (AER) under any circumstances.</p> <p>The performance and scalability of the eVACUATE system will be validated in four distinct scenarios involving incidents with large crowds at various venues with the requirements of evacuation time reduction and increase of safety and security (evacuation demonstrations). In the context of these scenarios, REAL SOCIEDAD DE FÚTBOL, S.A.D., an enterprise registered at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, has joined forces with universities and research institutes (the "eVACUATE consortium") for the carrying out of one of the evacuation demonstrations.</p> <p>Your participation in the REAL SOCIEDAD DE FÚTBOL, S.A.D. evacuation demonstration involves your physical presence at the stadium and your participation in the evacuation activities. You will receive detailed instructions and guidance during the demonstration.</p> <p>The demonstration will be recorded on different types of video cameras. Still images (photographs) and moving images (videos/video recordings) of the participants will be captured and stored during the demonstration. These still and moving images will contain personal data about you, such as your image, but they will not be used to identify you. These personal data will be processed by REAL SOCIEDAD DE FÚTBOL, S.A.D. and will be made available to other partners of the eVACUATE consortium for the following purposes in line with the research objectives of the eVACUATE project:</p> <ul style="list-style-type: none"><li>• to test tools to detect unusual behaviour in moving crowds;</li><li>• to model different evacuation routes that will enable decision makers to choose the safest route in case of an evacuation;</li><li>• to communicate customised evacuation information to supporters and crew during an evacuation test;</li><li>• to promote the project and the outcomes of the demonstration internally within the companies/organisations of the eVACUATE consortium partners and also to the European Commission for the purposes of demonstration, reporting and evaluation of the work carried out.</li></ul> <p>For these purposes the recordings may be shared only with the following research institutions within the eVACUATE consortium: ITInnovation, INDRA, EXODUS, DIGINEXT, Technical University Chemnitz, Technical University Dresden, Telecom Italia TIM, CDI and ICCS. Contact details of each eVACUATE consortium partner are provided in addendum on the back side of this consent form. The images and recordings are under the custody and control of REAL SOCIEDAD DE FÚTBOL, S.A.D. and will be processed only by the aforementioned eVACUATE consortium partners. The still and moving images will be kept for a maximum period of up to five (5) years after the end of the eVACUATE project.</p> <div style="border: 1px solid black; padding: 5px;"><p><b>BY SIGNING AND RETURNING THE PRESENT CONSENT FORM, YOU AGREE THAT:</b></p><ul style="list-style-type: none"><li>• you have been informed of and understand the purposes of the evacuation demonstration,</li><li>• you have been given the opportunity to ask questions,</li><li>• your participation in the evacuation demonstration is voluntary,</li><li>• you understand you can withdraw your participation and consent at any time without prejudice and</li><li>• you consent to the collection and processing for the abovementioned purposes, during and after the evacuation demonstration, of the still and moving images containing personal data about you captured and stored during the evacuation demonstration, controlled by REAL SOCIEDAD DE FÚTBOL, S.A.D., Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain.</li></ul></div> <p>You will receive a copy of this consent form.</p> <p>For more information about the project, please visit the project's website at: <a href="http://www.evacuate.eu/">http://www.evacuate.eu/</a>.</p> <p>For further information about the processing of your data and your rights of access, rectification, restriction and withdrawal, please contact REAL SOCIEDAD DE FÚTBOL, S.A.D. by sending an email to Vicente Serrulla at <a href="mailto:vicente.serrulla@realsociedad.es">vicente.serrulla@realsociedad.es</a>.</p> <div style="border: 1px solid black; padding: 5px;"><p><b>Name of volunteer:</b></p><p><b>Signature:</b></p><p><b>Place and date:</b> San Sebastián, 22 October 2016</p></div>
--

## 6.2 Information and consent form for Athens International Airport (AIA) validation demonstration

### INFORMATION AND CONSENT FORM

In the context of the European Union's Seventh Framework Programme for Research, Technological Development and Demonstration (FP7), the project eVACUATE has received funding under Grant Agreement No. 313161. The project aims to address the needs of the safety of citizens during complex evacuation processes following normal and abnormal events (crises) towards the creation of a comprehensive system that will be able to identify, designate and sustain a dynamic Active Evacuation Route (AER) under any circumstances.

The performance and scalability of the eVACUATE system will be validated in four distinct scenarios involving incidents with large crowds at various venues with the requirements of evacuation time reduction and increase of safety and security (evacuation demonstrations). In the context of these scenarios, STX France (AIA), located at Spata, 19019, Greece, has joined forces with universities and research institutes (the "eVACUATE consortium") for the carrying out of one of the evacuation demonstrations.

Your participation in the AIA evacuation demonstration, to which you agreed to participate on a voluntary basis, involves your physical presence at the airport and your participation in the evacuation activities. You will receive detailed instructions and guidance during the demonstration.

The demonstration will be recorded on different types of video cameras. Still images (photographs) and moving images (videos/video recordings) of the participants will be captured and stored during the demonstration. These still and moving images will contain personal data about you, such as your image, but they will not be used to identify you. These personal data will be processed by AIA as identified above and will be made available only to other partners of the eVACUATE consortium for the following purposes in line with the research objectives of the eVACUATE project:

- to test tools to detect unusual behaviour in moving crowds;
- to model different evacuation routes that will enable decision makers to choose the safest route in case of an evacuation;
- to communicate customised evacuation information to supporters and crew during an evacuation test;
- to promote the project and the outcomes of the demonstration internally within the companies/organisations of the eVACUATE consortium partners and also to the European Commission for the purposes of demonstration, reporting and evaluation of the work carried out.

For these purposes, the recordings may be shared only with the following research institutions within the eVACUATE consortium: ITInnovation, INDRA, EXODUS, DIGINEXT, Technical University Chemnitz, Technical University Dresden, Telecom Italia TIM, CDI and ICCS. Contact details of each eVACUATE consortium partner are provided in addendum on the back side of this consent form. The images and recordings are under the custody and control of AIA and will be processed only by the aforementioned eVACUATE consortium partners. The still and moving images will be kept for a maximum period of up to five (5) years after the end of the eVACUATE project.

#### BY SIGNING AND RETURNING THE PRESENT CONSENT FORM, YOU AGREE THAT:

- you have been informed of and understand the purposes of the evacuation demonstration,
- you have been given the opportunity to ask questions,
- your participation in the evacuation demonstration is voluntary,
- you understand you can withdraw your participation and consent at any time without prejudice and
- you consent to the collection and processing for the abovementioned purposes, during and after the evacuation demonstration, of the still and moving images containing personal data about you captured and stored during the evacuation demonstration, controlled by Athens International Airport, 19019 Spata, Greece, for the purposes described above.

You will receive a copy of this consent form.

For more information about the project, please visit the project's website at: <http://www.evacuate.eu/>.

For further information about the processing of your data and your rights of access, rectification, restriction and withdrawal, please contact AIA by sending an email to Papagiannopoulos Nikolaos at [PapagiannopoulosN@aiagr.gr](mailto:PapagiannopoulosN@aiagr.gr) or Felaneri Chrysoula at [FelanerisC@aiagr.gr](mailto:FelanerisC@aiagr.gr).

Name of volunteer:

Signature:

Place and date: Athens, 27 January 2016

**ΕΝΤΥΠΟ ΕΝΗΜΕΡΩΣΗΣ ΚΑΙ ΣΥΝΑΙΝΕΣΗΣ**

Στα πλαίσια του Προγράμματος-Πλαίσιο 7 (FP7) της Ευρωπαϊκής Ένωσης για την Έρευνα, την Τεχνολογική Ανάπτυξη και την Επίδειξη, έχει χρηματοδοτηθεί το έργο eVACUATE (Συμφωνία Επιχορήγησης Νο 313161). Το έργο στοχεύει στην αντιμετώπιση των αναγκών για την ασφάλεια των πολιτών κατά τη διάρκεια των πολύπλοκων διαδικασιών εκκένωσης μετά από κανονικά και μη γεγονότα (κρίσεις), προς την κατεύθυνση της δημιουργίας ενός ολοκληρωμένου συστήματος που θα είναι σε θέση να εντοπίζει, να καθορίζει και να διατηρεί μια δυναμική Ενεργή Διαδρομή Εκκένωσης κάτω από οποιοδήποτε συνθήκες.

Η απόδοση και η επεκτασιμότητα του συστήματος eVACUATE θα επικυρωθούν σε τέσσερα διακριτά σενάρια (ασκήσεις εκκένωσης), που αφορούν περιστατικά με μεγάλα πλήθη σε διάφορους χώρους, με τις απαιτήσεις της μείωσης του χρόνου εκκένωσης και αύξησης της ασφάλειας και της υγείας (security & safety). Στο πλαίσιο αυτών των σεναρίων, ο Διεθνής Αερολιμένας Αθηνών Α.Ε. (ΔΑΑ), που βρίσκεται στα Σπάτα, 19019, ένωσε τις δυνάμεις του με πανεπιστήμια και ερευνητικά ιδρύματα (την "Κοινοπραξία eVACUATE") για την πραγματοποίηση μιας από τις ασκήσεις εκκένωσης.

Η συμμετοχή σας στην άσκηση εκκένωσης του ΔΑΑ, στην οποία συμφωνήσατε να συμμετάσχετε σε εθελοντική βάση, περιλαμβάνει τη φυσική παρουσία σας στο αεροδρόμιο και τη συμμετοχή σας στις δραστηριότητες εκκένωσης. Θα λάβετε λεπτομερείς οδηγίες και κατευθύνσεις κατά τη διάρκεια της άσκησης.

Η άσκηση θα καταγραφεί σε διαφορετικούς τύπους βιντεοκάμερας. Ακίνητες εικόνες (φωτογραφίες) και κινούμενες εικόνες (βίντεο/βίντεο εγγραφές) από τους συμμετέχοντες θα ληφθούν και θα αποθηκευτούν κατά τη διάρκεια της άσκησης. Αυτές οι σταθερές και κινούμενες εικόνες θα περιέχουν προσωπικά σας δεδομένα, όπως την εικόνα σας, αλλά δεν θα χρησιμοποιηθούν για την αναγνώριση σας. Τα προσωπικά αυτά δεδομένα θα υποβληθούν σε επεξεργασία από το ΔΑΑ, όπως περιγράφεται ως άνω και θα διατεθούν μόνο στους άλλους εταίρους της κοινοπραξίας eVACUATE για τους ακόλουθους σκοπούς σύμφωνα με τους ερευνητικούς στόχους του έργου eVACUATE:

- να δοκιμαστούν εργαλεία για τον εντοπισμό ασυνήθιστης συμπεριφοράς σε κινούμενα πλήθη,
- να μοντελοποιηθούν διαφορετικές διαδρομές εκκένωσης που θα επιτρέπουν σε φορείς λήψης αποφάσεων να επάξουν την ασφαλέστερη διαδρομή σε περίπτωση εκκένωσης,
- να επικυρωθούν εξατομικευμένες πληροφορίες εκκένωσης σε υποστηρικτές και το πλήρωμα κατά τη διάρκεια της άσκησης εκκένωσης,
- να προβληθούν τόσο το έργο όσο και τα αποτελέσματα της άσκησης στο εσωτερικό των εταιρειών/ οργανισμών της κοινοπραξίας eVACUATE, αλλά και προς την Ευρωπαϊκή Επιτροπή για τους σκοπούς της επίδειξης, της υποβολής εκθέσεων και της αξιολόγησης των διεξαγόμενων εργασιών.

Για τους σκοπούς αυτούς, οι εγγραφές μπορούν να κοινοποιηθούν μόνο στα ακόλουθα ερευνητικά ιδρύματα της κοινοπραξίας eVACUATE: ITIpponadion, INDRA, EXODUS, DIGIMEXT, Τεχνικό Πανεπιστήμιο Chemnitz, Τεχνικό Πανεπιστήμιο της Δρέσδης, η Telecom Italia TIM, CDI και EPISY. Τα στοιχεία επικοινωνίας του κάθε εταίρου της κοινοπραξίας eVACUATE παρέχονται στο προσάρτημα στο πίσω μέρος αυτού του εντύπου συναίνεσης. Οι εικόνες και οι εγγραφές είναι κάτω από την φύλαξη και τον έλεγχο του ΔΑΑ και θα υποβληθούν σε επεξεργασία μόνο από τους προαναφερθέντες εταίρους της κοινοπραξίας eVACUATE. Οι σταθερές και κινούμενες εικόνες θα διατηρηθούν για το μέγιστο χρονικό διάστημα των πέντε (5) χρόνων μετά το τέλος του έργου eVACUATE.

**Υπογράφοντας και επιστρέφοντας το παρόν έντυπο ΣΥΝΑΙΝΕΣΗΣ, συμφωνείτε ότι:**

- έχετε ενημερωθεί και κατανοήσατε τους σκοπούς της άσκησης εκκένωσης,
- σας έχει δοθεί η ευκαιρία να υποβάλετε ερωτήσεις,
- η συμμετοχή σας στην άσκηση εκκένωσης είναι εθελοντική,
- καταλαβαίνετε ότι μπορείτε να αποσύρετε τη συμμετοχή και τη συγκατάθεσή σας ανά πάσα στιγμή χωρίς επιφυλάξεις και
- συναινείτε στη συλλογή και την επεξεργασία για τους ανωτέρω σκοπούς, κατά τη διάρκεια και μετά την άσκηση εκκένωσης, των ακίνητων και κινούμενων εικόνων που περιέχουν προσωπικά σας δεδομένα ληφθέντα και αποθηκευμένα κατά τη διάρκεια της άσκησης εκκένωσης, που ελέγχεται από το Διεθνές Αεροδρόμιο Αθηνών, 19019 Σπάτα, Ελλάδα, για τους ως άνω περιγραφόμενους σκοπούς.

Θα λάβετε ένα αντίγραφο αυτού του εντύπου συναίνεσης.

Για περισσότερες πληροφορίες σχετικά με το πρόγραμμα, παρακαλούμε επισκεφθείτε την ιστοσελίδα του έργου στο: <http://www.evacuate.eu/>.

Για περισσότερες πληροφορίες σχετικά με την επεξεργασία των δεδομένων σας και τα δικαιώματά σας σχετικά με την πρόσβαση, τη διόρθωση, τον περιορισμό και την απόσυρση, παρακαλούμε επικοινωνήστε με τον ΔΑΑ, στέλνοντας ένα email στον Νίκο Παπαγιαννόπουλο στο [forac@pponadion.gr](mailto:forac@pponadion.gr) ή τη Χρυσούλα Φαλαγγάρη στο [forac@tim.it](mailto:forac@tim.it).

**Ονοματεπώνυμο εθελοντή:**

**Υπογραφή:**

**Τόπος και ημερομηνία: Αθήνα, 27 Ιανουαρίου 2016**

## 6.3 Information and consent form for STX France (STX) validation demonstration

### INFORMATION AND CONSENT FORM

In the context of the European Union's Seventh Framework Programme for Research, Technological Development and Demonstration, the project eVACUATE aims to address the needs of the safety of citizens during complex evacuation processes following normal and abnormal events (crises). The project's objective is to develop a comprehensive system that will be able to identify, designate and sustain a dynamic Active Evacuation Route (AER) under any circumstances. The project has received funding under Grant Agreement No. 313161.

The performance and scalability of the eVACUATE system will be validated in four distinct scenarios simulating incidents with large crowds at various venues with the requirements of evacuation time reduction and increase of safety and security (the "evacuation demonstrations"). In the context of these scenarios, STX France SA, siren n°43906761200036 with registered seat at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France ("STX") has joined forces with universities and research institutes (the "eVACUATE consortium") for the carrying out of one of the evacuation demonstrations. For more information about the project, please visit the project's website at: <http://www.evacuate.eu/>.

Your participation in the STX evacuation demonstration is voluntary. It involves your physical presence on board a ship owned and operated by STX and your participation in the evacuation activities. You will receive detailed boarding, safety and practical instructions and guidance during the demonstration.

The demonstration will be recorded on different types of video cameras by the partners in the eVACUATE consortium acting on behalf of STX. Still images (photographs) and moving images (videos/video recordings) of the participants will be captured and stored during the demonstration. These still and moving images will contain personal data about you, such as your image, but they will not be used to identify you. These personal data will be collected and processed by STX and will be made available only to other partners in the eVACUATE consortium for the following purposes in line with the research objectives of the eVACUATE project:

- to test the integration and operation of the eVACUATE system's software and hardware tools used for modelling and detection of unusual behaviour in moving crowds;
- to create models of different evacuation routes enabling decision makers to choose the safest route in case of an evacuation;
- to communicate customised evacuation information to supporters and crew during an evacuation test;
- to present the project's results and the outcomes of the demonstration internally within the companies/organisations of the partners in the eVACUATE consortium and also to the European Commission for the purposes of demonstration, reporting and evaluation of the work carried out;
- to conduct further research in a manner compatible with the abovementioned purposes.

For these purposes, the recordings may be shared only with the following research institutions, which are partners in the eVACUATE consortium: ITInnovation, INDRA, EXODUS, DIGINEXT, Technical University Dresden, Telecom Italia TIM, CDI and ICCS. Contact details of each eVACUATE consortium partner are provided in addendum on the back side of this information and consent form.

The images and recordings are under the custody and control of STX and will be processed only by the aforementioned eVACUATE consortium partners. The still and moving images will be kept for a maximum period of up to five (5) years after the end of the eVACUATE project.

#### BY SIGNING AND RETURNING THE PRESENT INFORMATION AND CONSENT FORM, YOU CONFIRM THAT:

- you have been informed of and understand the purposes of the evacuation demonstration of the eVACUATE project,
- you have been given the opportunity to ask questions,
- you understand you can withdraw your participation at any time without prejudice and
- you consent voluntarily to the collection and processing for the purposes describe above, during and after the evacuation demonstration, of the still and moving images and your names containing personal data about you, captured and stored during the evacuation demonstration and controlled by STX France SA (STX), siren n°43906761200036 with registered seat at Avenue Antoine BOURDELLE, CS 90180, 44613 Saint Nazaire Cedex, France.

You will receive a copy of this consent form.

For further information about the processing of your data by the partners in the eVACUATE consortium and your rights of access, rectification, and restriction, in accordance with the applicable legislation, please contact STX by sending an email to: (to be specified).

Name of volunteer:

Signature:

Place and date: Saint Nazaire, France, 17 March 2016

**NOTE D'INFORMATION ET ACCORD DE CONSENTEMENT**

Dans le cadre du 7ème programme d'infrastructure pour la recherche le développement technique de la CEE, le projet eVACUATE a pour but de répondre au besoin de sécurité des personnes lors de processus d'évacuation complexe à la suite d'événements programmés ou imprévus (crise). Les objectifs du projet sont de développer un système global en mesure d'identifier, désigner et mettre en œuvre de manière dynamique une Route Active d'Evacuation (RAE). Le projet a reçu un financement par l'agrément n°313161.

Les performances et la modularité du système eVACUATE seront validées au cours de quatre scénarios distincts simulant des incidents avec des foules importantes dans des lieux divers avec nécessité de réduction de la durée d'évacuation et augmentation de la sécurité. Dans le cadre de ces scénarios, STX France SA siren n°43906761200036 dont le siège est situé à Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France a rejoint le consortium des universités et centres de recherche pour héberger l'un des exercices d'évacuation. Pour plus d'information, voir le site web du projet : <http://www.evacuate.eu/>.

Votre participation à cet exercice d'évacuation chez STX est volontaire. Elle suppose votre présence physique à bord d'un navire propriété de STX et votre participation aux activités de l'exercice d'évacuation. Vous serez informés des conditions pratiques, de sécurité et des détails de l'exercice pendant la manifestation.

Cette démonstration sera enregistrée par une vidéo réalisée pour le compte de STX. Des images fixes (photo) et en mouvement (film) des participants seront prises et conservées pendant l'exercice. Ces images contiendront ainsi des données personnelles vous appartenant, comme votre image, mais ne seront pas utilisées pour vous identifier. Ces données personnelles seront collectées et traitées par STX et ne seront mises à disposition des autres partenaires du consortium eVACUATE que pour répondre aux objectifs suivants, en ligne avec les objectifs de recherche du projet eVACUATE:

- Tester l'intégration et la mise en œuvre du système eVACUATE, ses outils matériels et logiciels utilisés pour la modélisation de foule en mouvement et détection de comportement inhabituel;
- Créer des modèles pour les différentes routes d'évacuation permettant aux preneurs de décisions de choisir la route la plus sûre en cas d'évacuation;
- Communiquer des informations d'évacuation personnalisées aux passagers ou membres d'équipages pendant le test d'évacuation;
- Présenter les résultats du projet et de l'exercice en interne, aux sociétés et organisations partenaires du consortium eVACUATE et également à la Commission Européenne afin que celle-ci en prenne connaissance et puisse évaluer le travail réalisé;
- Approfondir les travaux de recherche de manière compatible avec les objectifs mentionnés ci-avant.

Dans ces objectifs, les enregistrements ne peuvent être partagés que par les organismes de recherche suivants, qui sont membres du consortium eVACUATE: ITInnovation, INDRA, EXODUS, DIGINEXT, Technical University Dresden, Telecom Italia TIM, CDI and ICCS. Les coordonnées de chaque partenaire sont disponibles en annexe au verso de cette note d'information et de consentement.

Les images et enregistrements sont sous la responsabilité et contrôle de STX et seront traités seulement par les membres du consortium eVACUATE pré-cités. Ces images seront conservées au maximum 3 (cinq) ans après la fin du projet eVACUATE.

**EN SIGNANT ET RETOURNANT LE PRESENT FORMULAIRE D'INFORMATION ET DE CONSENTEMENT, VOUS RECONNAISSEZ QUE:**

- Vous avez été informé(e) et vous avez compris les objectifs de l'exercice d'évacuation du projet eVACUATE
- Vous avez eu la possibilité de poser des questions
- Vous avez compris pouvoir annuler votre participation à tout moment sans préjudice.
- Vous donnez votre accord volontairement à la prise d'images (fixes ou en mouvement) pouvant contenir des données personnelles vous appartenant et à leur montage et exploitation selon les objectifs décrits ci-avant, pendant et après l'exercice. Ces images sont sous contrôle de STX France SA (STX), siren n°43906761200036 dont le siège est situé: Avenue Antoine BOURDELLE, CS 90180, 44613 Saint Nazaire Cedex, France.

Vous recevrez une copie de cet accord de consentement.

Pour de plus amples informations sur le traitement de vos données par les partenaires du consortium eVACUATE et vos droits d'accès, de rectifications, de restrictions, en accord avec la législation applicables, vous pouvez contacter STX par mail à l'adresse suivante: **contact à préciser.**

Name of volunteer:

Signature:

Place and date: Saint Nazaire, France, 17 March 2016



## 6.4 Information and consent form for Metro Bilbao (METB) validation demonstration

### INFORMATION AND CONSENT FORM

In the context of the European Union's Seventh Framework Programme for Research, Technological Development and Demonstration, the project eVACUATE aims to address the needs of the safety of citizens during complex evacuation processes following normal and abnormal events (crises). The project's objective is to develop a comprehensive system that will be able to identify, designate and sustain a dynamic Active Evacuation Route (AER) under any circumstances. The project has received funding under Grant Agreement No. 313161.

The performance and scalability of the eVACUATE system will be validated in four distinct scenarios simulating incidents with large crowds at various venues with the requirements of evacuation time reduction and increase of safety and security (the "evacuation demonstrations"). In the context of these scenarios, Metro Bilbao S.A., with registered seat at Calle Navarra, 2, 48001 Bilbao, Bizkaia, España (hereinafter referred to as "METB") has joined forces with universities and research institutes (the "eVACUATE consortium") for the carrying out of one of the evacuation demonstrations. For more information about the project, please visit the project's website at: <http://www.evacuate.eu/>.

Your participation in the METB evacuation demonstration is voluntary. It involves your physical presence at the San Mames Metro Station in Bilbao and your participation in the evacuation activities. You will receive detailed instructions and guidance during the demonstration.

The demonstration will be recorded on different types of video cameras by the partners in the eVACUATE consortium acting on behalf of METB. Still images (photographs) and moving images (videos/video recordings) of the participants will be captured and stored during the demonstration. These still and moving images will contain personal data about you, such as your facial image, but they will not be used to identify you. These personal data will be collected and processed by METB and will be made available only to other partners in the eVACUATE consortium for the following purposes in line with the research objectives of the eVACUATE project:

- to test the integration and operation of the eVACUATE system's software and hardware tools used for modelling and detection of unusual behaviour in moving crowds;
- to create models of different evacuation routes enabling decision makers to choose the safest route in case of an evacuation;
- to communicate customised evacuation information to supporters and crew during an evacuation test;
- to present the project's results and the outcomes of the demonstration internally within the companies/organisations of the partners in the eVACUATE consortium and also to the European Commission for the purposes of demonstration, reporting and evaluation of the work carried out;
- to conduct further research in a manner compatible with the abovementioned purposes.

For these purposes, the recordings may be shared only with the following research institutions, which are partners in the eVACUATE consortium: ITInnovation, INDRA, EXODUS, DIGINEXT, Technical University Dresden, Telecom Italia TIM, CDI and ICCS. Contact details of each eVACUATE consortium partner are provided in addendum on the back side of this information and consent form.

The images and recordings are under the custody and control of METB and will be processed only by the aforementioned eVACUATE consortium partners. The still and moving images will be kept for a maximum period of up to five (5) years after the end of the eVACUATE project.

#### BY SIGNING AND RETURNING THE PRESENT INFORMATION AND CONSENT FORM, YOU CONFIRM THAT:

- you have been informed of and understand the purposes of the evacuation demonstration of the eVACUATE project,
- you have been given the opportunity to ask questions,
- you understand you can withdraw your participation at any time without prejudice and
- you consent voluntarily to the collection and processing for the purposes describe above, during and after the evacuation demonstration, of the still and moving images and your names containing personal data about you, captured and stored during the evacuation demonstration and controlled by Metro Bilbao SA (METB), with registered seat at Calle Navarra, 2, 48001 Bilbao, Bizkaia, España.

You will receive a copy of this consent form. For further information about the processing of your data by the partners in the eVACUATE consortium and your rights of access, rectification, and restriction, in accordance with the applicable legislation, please contact METB by sending an email to: [info-iod3@metrobilbao.euz](mailto:info-iod3@metrobilbao.euz).

Name of volunteer:

Signature:

Place and date: Bilbao, Spain, 05 May 2017



#### HOJA DE CONSENTIMIENTO

El proyecto eVACUATE ha recibido financiación en el contexto del Séptimo Programa Marco de la Unión Europea para la Investigación, Desarrollo Tecnológico y Demostración (FP7), bajo el Acuerdo de Subvención Nº 313161. El proyecto tiene como objetivo asegurar la seguridad de la ciudadanía durante los procesos de evacuación generados por situaciones habituales y/o situaciones no controladas (crisis) a través del desarrollo de un sistema integral que será capaz de identificar, designar y mantener una ruta de evacuación activa dinámica (AER) bajo cualquier circunstancia.

El rendimiento y la escalabilidad del sistema eVACUATE serán validados en cuatro escenarios diferentes, se realizarán simulaciones de incidencias con aglomeraciones de personas en diferentes situaciones, y con la finalidad de reducir el tiempo de evacuación y de aumentar la seguridad (demostraciones de evacuación). En el contexto de estos escenarios, METRO BILBAO, S.A., empresa registrada en la Calle Navarra, 2, 48001 Bilbao, Bizkaia, España, colabora con las universidades y los institutos de investigación miembros del "consorcio eVACUATE" para recrear una de las demostraciones de evacuación. Para más información sobre el Proyecto, se puede visitar la página web del Proyecto a la dirección siguiente: <http://www.evacuate.eu/>

Su participación en la demostración de evacuación en las instalaciones de METRO BILBAO, S.A. requiere su presencia física en la estación de San Mamés, así como en la realización de los ejercicios de simulación de evacuación. Ud. recibirá instrucciones detalladas e Indicaciones durante la demostración.

La demostración se grabará en diferentes tipos de cámaras de vídeo. Las imágenes fijas (fotografías) y las imágenes en movimiento (vídeo / grabaciones de vídeo) de las personas participantes serán capturadas y almacenadas durante los ejercicios. Estas imágenes fijas y en movimiento contendrán datos personales sobre Ud., como su imagen, pero no serán utilizadas para identificarle. Estos datos de carácter personal serán tratados por METRO BILBAO, S.A. y serán compartidos con los otros miembros del consorcio eVACUATE única y exclusivamente para fines compatibles con los objetivos de investigación del proyecto eVACUATE:

- Probar las herramientas desarrolladas para detectar comportamientos inusuales en Aglomeraciones.
- Modelar distintas rutas de evacuación que permitirán elegir la ruta más segura en caso de evacuación.
- Proporcionar a las personas usuarias, al personal de la estación y al de seguridad, la información necesaria para realizar una correcta evacuación.
- Exposición del proyecto y análisis de los resultados de la demostración con las empresas/ organizaciones (miembros del consorcio eVACUATE) y con la Comisión Europea para los fines de la demostración, presentación de informes y evaluación del trabajo realizado.

Las grabaciones realizadas pueden ser compartidas únicamente con los institutos de investigación siguientes: ITInnovation, INDRA, EXODUS, DIGINEXT, Technical University Dresden, Telecom Italia TIM, CDI and ICCS (miembros del consorcio eVACUATE). La información de contacto de estas entidades está en el anexo de esta hoja de consentimiento. Las imágenes y grabaciones están bajo la custodia y control de METRO BILBAO, S.A. y serán tratadas únicamente por las entidades del consorcio eVACUATE antes mencionadas. Las imágenes fijas y en movimiento serán conservadas para un máximo de cinco (5) años después del final del proyecto eVACUATE.

#### FIRMANDO EL PRESENTE FORMULARIO DE CONSENTIMIENTO, USTED CONFIRMA QUE:

- Ha sido informado y comprende los propósitos de estos ejercicios de evacuación.
- Se le ha dado la oportunidad de realizar preguntas.
- Su participación en este ejercicio de evacuación es voluntaria.
- Entiende que puede retractarse de su participación y su consentimiento en cualquier momento sin perjuicio.
- Permite la adquisición y el procesamiento para los objetivos mencionados, durante y después de los ejercicios de evacuación, de las imágenes y vídeos capturados y almacenados durante este ejercicio de evacuación y que contiene información personal sobre usted, controlados por METRO BILBAO, S.A., Calle Navarra, 2, 48001 Bilbao, Bizkaia, España.

Conforme a la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal y en el Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999, le informamos de la existencia de un fichero con los datos que se recaban y del que es responsable Metro Bilbao, con sede en la calle Navarra nº2 48001 Bilbao (Bizkaia). Si desea, podrá ejercitar los derechos de Acceso, Rectificación, Cancelación y Oposición, diríjase a [dblo-icod3@metrobilbao.eus](mailto:dblo-icod3@metrobilbao.eus) o a una de nuestras Oficinas Atención a Clientes de Metro Bilbao.

Nombre del voluntario:

Firma:

Lugar y fecha: Bilbao, de de 2017

For each information and consent form, on the back side of the paper an addendum was printed with information and contact details of the data processors.

#### ADDENDUM

List of eVACUATE consortium partners with whom still and moving images containing personal data collected during the evacuation demonstration may be shared

PARTNER	ADDRESS	CONTACT PERSON AND DETAILS
Crowd Dynamics International Limited (CDI)	21 Station Road West, Oxted Surrey, RH8 9EE, United Kingdom	Paul Townsend, Associate Director Email: paul.townsend@crowddynamics.com
DIGINEXT	5 Rue Brindejonc des Moulinais 31506 Toulouse Cedex 5 France	Romain Charbit, Technical Project Leader Email : romain.charbit@diginext.fr
EXODUS S.A. (EXODUS)	73-75 Mesogeion Av & Estias Str 1, Postal Code 115 26, Athens, Greece	Dimitris Petrantonakis, Project Coordinator Email: dpetr@exus.co.uk
INDRA	Ctra. de Loeches, 9, Edificio Principal, 28850 Torrejón de Ardoz, Madrid	Pedro Garibi Pérez, Safety & Security Engineer Email: pgaribi@indra.es
Institute of Communication and Computer Systems (ICCS)	Iroon Polytechniou, 9, 15773 Zografou, Attiki, Greece	Konstantinos Karantzas Email: konstantinos.karantzas@gmail.com
Technische Universität Dresden, Faculty of Electrical and Computer Engineering, Institute of Principles of Electrical and Electronic Engineering; Chair of Circuit Design and Network Theory (Technical University Dresden)	Helmholtzstrasse 10, Dresden, 01069, Germany	Sven Kreigenfeld, Head of Unit "Research and Innovation Promotion" Email: sven.kreigenfeld@tu-dresden.de
Telecom Italia TIM	Viale Parco de Medici, 61 – 00148 - Roma	Marco Mancini, Projects ICT - R&D Funding Email: marco.mancini@telecomitalia.it
University of Southampton IT Innovation Centre (ITInnovation)	Gamma House, Enterprise Road, Southampton SO16 7NS, UK	Dr Zoheir A. Sabeur, Science Director Email: zas@it-innovation.soton.ac.uk

All original signed information and consent forms are kept by the controller in the respective validation demonstration in compliance with their internal procedures and with the obligations assumed as data controllers for the specific validation demonstration.

## 7 Appendix II: Data processing agreements

### 7.1 Data processing agreements for Anoeta Stadium Real Sociedad (ASRS) validation demonstration

Template only  
**Real Sociedad-EXODUS**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise domiciled at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

##### **And:**

**EXODUS S.A.**, 73-75 Mesogeion Av & Estias Str 1, Postal Code 115 26, Athens, Greece, duly represented by Dimitris Skliros, CEO

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used for these research purposes within eVACUATE project;

The Processor, i.e. **EXODUS**, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis

of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of monitoring and control of the evacuation mode and for dissemination and promotion of the project and the outcomes of the pilot exercises internally within the Processor's company and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the project partners in the context of a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

**Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in San Sebastian, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dimitris Skliros, CEO

For the Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)



Template only  
**Real Sociedad-ICCS**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

#### **Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise domiciled at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

#### **And:**

**INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)**, Iroon Polytechniou, 9, 15773 Zografou, Attiki, Greece, duly represented by Konstantinos Karantzalos, ICCS,

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in **a research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as the acquisition of video data at certain spectral regions by means of thermal and hyperspectral sensors enabling the measurement of crowd density, velocity and direction estimation, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as the subsequent activities enabling the measurement of crowd density, velocity and direction estimation, as explained above and used for research purposes within eVACUATE project;

The Processor, i.e. **ICCS**, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**



- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of measuring crowd density, velocity and direction estimation.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the project partners in the context of a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read,

copied, altered or removed without authorization during processing, use and after recording (access control),

- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the Controller of any cases of violation by the Processor or its employees of provisions relating to personal data protection or any breaches of the terms specified by the Controller.

4.10. The Processor commits not to enter into subcontracts.

**Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the period specified in Article 5.1 above with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due written notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the competent courts in the Kingdom of Spain.

Done in \_\_\_\_\_, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Konstantinos Karantzalos, ICCS

For the Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only  
**Anoeta Stadium-CDI**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement**

**Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise domiciled at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

**And:**

**Crown Dynamics International Limited (CDI)**, 21 Station Road West, Oxted Surrey, RH8 9EE, United Kingdom, duly represented by Paul Townsend, Associate Director

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in **a research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as the subsequent activities enabling the measurement of crowd density, velocity and direction estimation, as explained above and used for research purposes within eVACUATE project;

The Processor, i.e. CDI, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of counting the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen.

- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under Article 1.2 above.
- 1.4. The categories of personal data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of personal data undertaken by the Processor in the context of a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),

- to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the Controller of any cases of violation by the Processor or its employees of provisions relating to personal data protection or any breaches of the terms specified by the Controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the period specified in Article 5.1 above with a notice period of one (1) month in case the other party does not

comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due written notice.

- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Kingdom of Spain shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the competent courts in the Kingdom of Spain.

Done in San Sebastian, Spain, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Paul Townsend, Associate Director

For the Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only  
**Real Sociedad-ITInnovation Centre**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise registered at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

##### **And:**

**University of Southampton IT Innovation Centre (IT Innovation)**, Gamma House, Enterprise Road, Southampton SO16 7NS, UK, duly represented by Dr Zoheir Sabeur, Science Director,

Hereinafter: the Processor,



**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings), as explained above and used for these research purposes within eVACUATE project;

The Processor, i.e. **IT Innovation**, agrees to process the still images (photographs) and moving images (video recordings) containing Personal Data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean recording, transforming, processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) in order to perform crowd analysis and algorithm calibration.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

**Article 2 - Subject**

- 2.1. The Agreement governs the processing of personal data undertaken by the project partners in the context of recording, transforming, processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) in order to perform crowd analysis and algorithm calibration in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC

– 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any

advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in \_\_\_\_\_, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dr Zoheir Sabeur, Science Director

For the Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only  
**Real Sociedad-TUD**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

**Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise registered at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the “Controller”,

**And:**

**Technische Universität Dresden**, HELMHOLTZSTRASSE 10, DRESDEN, 01069, Germany represented by Sven KREIGENFELD, Head of Unit or his authorized representative

Acting Side: Faculty of Electrical and Computer Engineering, Institute of Principles of Electrical and Electronic Engineering; Chair of Circuit Design and Network Theory

Hereinafter: the “Recipient”,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in **a research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the

compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of the Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as the subsequent activities on analysing the operation of the chipless RFID system, as explained above and used for research purposes within eVACUATE project;

The Recipient agrees to receive the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons from the Controller or from subjects working on behalf of the Controller and collect Personal Data on behalf of the Controller. The Recipient will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Recipient', and 'Processing' shall have the same meaning as in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter "Directive 95/46/EC").
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of studying the operation of the chipless RFID system and providing the eVACUATE system with the number and type of persons who have crossed through a particular position that is used to maintain and keep up to date the Active Evacuation Route for a specific venue.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the project partners in the context of a **research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Recipient shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants
- that Personal Data will be processed in accordance with applicable data protection law and they are fit for their intended purpose herein,
  - that throughout the duration of the Processing it will issue instructions to the Recipient in accordance with applicable laws,
  - to inform Recipient without undue delay about relevant errors or irregularity.

### **Article 4 – Warranties and obligations of the Recipient**

- 4.1. The Recipient agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Recipient agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Recipient also undertakes to take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

- 4.3. The Recipient further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

- 4.4. The Recipient undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any



advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Recipient shall also comply with the current and future applicable data protection legislation to the extent applicable to the Recipient.

- 4.5. The Recipient agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Recipient shall not respond to such request without prior consultation and the express authorization to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the Recipient accepts their obligation to accept and cooperate.
- 4.8. The Recipient shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the Data Subject as well as after the processing has been carried out.
- 4.9. The Recipient shall notify the Controller of any cases of violation by the Recipient or its employees of provisions relating to personal data protection or any breaches of the terms specified by the Controller.
- 4.10. The Recipient commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The parties shall be liable to each other for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Recipient for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the period specified in Article 5.1 above with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due written notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Recipient shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Recipient prevents him from returning or destroying such data. In that case, the Recipient warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.



6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the applicable competent court plaintiff.

Done in \_\_\_\_\_, on \_\_\_\_\_ (date), in two copies, each party having received one.

The Recipient

[name]

The Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only  
**Real Sociedad-DXT**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### Agreement

**Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise registered at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

**And:**

**Diginext**, 5 Rue BrindeJonc des Moulinais 31506 Toulouse Cedex 5 France, duly represented by Romain Charbit, Technical Project Leader (DXT)

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in **a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to directly see what is happening in a crisis environment, which form part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016, and to store them for later replay in debriefings or training sessions in the framework of the eVACUATE project.**

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to integrate the video

recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to directly see what is happening in a crisis environment, and to store them for later replay in debriefings or training sessions, as explained above and used for these research purposes within the eVACUATE project;

The Processor, i.e. DXT, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs), moving images (video recordings) for the purpose of integrating the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to directly see what is happening in a crisis environment, and for storing them for later replay in debriefings or training sessions.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of personal data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of personal data undertaken by the project partners in the context of a **research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to directly see what is happening in a crisis environment, and to store them for later replay in debriefings or training sessions in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

**Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the **Spanish Data Protection Act**, and any other applicable laws.

**Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request

received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.

- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the Controller of any cases of violation by the Processor or its employees of provisions relating to personal data protection or any breaches of the terms specified by the Controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the period specified in Article 5.1 above with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due written notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the competent courts in the Kingdom of Spain.

Done in San Sebastian, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Romain Charbit, Technical Project Leader

For the Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only  
**Real Sociedad-INDRA**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

#### **Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise domiciled at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

#### **And:**

**INDRA**, 73-75 CTRA. DE LOECHES, 9, Edificio Principal, 28850 Torrejón de Ardoz, Madrid, duly represented by Pedro Garibi Pérez, Safety & Security Engineer

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used for these research purposes within eVACUATE project;

The Processor, i.e. **INDRA**, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of dissemination and promotion of the project and the outcomes of the pilot exercises internally within the Processor's company and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the project partners in the context of a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies/organisations and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**



- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.
- These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.
- The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.
- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.
- The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.
- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.



- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

**Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in San Sebastian, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Pedro Garibi Pérez, Safety & Security Engineer

For the Controller

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only

**Real Sociedad-TIM**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement****Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise domiciled at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively

Hereinafter: the Controller,

**And:**

**TELECOM ITALIA TIM, Viale Parco de Medici, 61 – 00148 - Roma**, duly represented by Marco Mancini, B.OG.D, Projects ICT - R&D Funding

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in **a research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastián, Spain on the 22<sup>nd</sup> of October, 2016, and the promotion of the project internally within the parties' organisations as well as the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and used for research purposes within the eVACUATE project;

The Processor, i.e. **FUNDACIÓN TEKNIKER**, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).

- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of promotion of the project internally within the Processor's organisation as well as for the compilation of subsequent reports and related research in the framework of the eVACUATE project.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the project partners in the context of **a research activity involving** the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to promote the project internally within the Processor's organisation as well as to compile subsequent reports and related research in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data

storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),

- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any employees of his who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

## **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in \_\_\_\_\_, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor:

Marco Mancini, B.OG.D, Projects ICT - R&D Funding

For the Controller:

Jokin Aperribay Bedialauneta (President)      Ángel Oyarzun Narváez (Vicepresident)

Template only  
**Real Sociedad-TUC**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement****Between:**

**REAL SOCIEDAD DE FÚTBOL, S.A.D.**, an enterprise domiciled at Paseo de Anoeta, 1, 20014 Donostia, Gipuzkoa, Spain, duly represented by Mr. Jokin Aperribay and Mr. Ángel Oyarzun, acting as its President and Vicepresident, respectively,

Hereinafter: the Controller,

**And:**

**CHEMNITZ UNIVERSITY OF TECHNOLOGY (TUC)**, Institute for Print and Media Technology, Reichenhainer Str. 70, 09126 Chemnitz, Germany, duly represented by Dr.-Ing. Georg Schmidt, Wissenschaftlicher Mitarbeiter,

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and organisations and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Anoeta Stadium in San Sebastian, Spain on 22 October 2016 and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

**REAL SOCIEDAD** is a Controller within the meaning of article 3.d of Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC, for the personal data collected and processed in relation to making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and organisations and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used for these research purposes within eVACUATE project;

The Processor, i.e. **CHEMNITZ UNIVERSITY OF TECHNOLOGY (TUC)**, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of dissemination and promotion of the project and the outcomes of the pilot exercises internally within the Processor's organisation and also to the European Commission for the purposes of demonstration and evaluation of the work.

- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and video processing activities as described under 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Anoeta Stadium in San Sebastian on 22 October 2016.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the project partners in the context of a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and organisations and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Spanish Data Protection Act (Ley Orgánica 15/1990, de 13 de diciembre, de Protección de Datos de Carácter Personal), and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),



- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorization by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of this Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects with regard to the processing of this Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual damage suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with

its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.

- 5.4. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Kingdom of Spain shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in San Sebastian, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dr.-Ing. Georg Schmidt, Wissenschaftlicher Mitarbeiter

For the Controller

Jokin Aperribay Bedialauneta (President) Ángel Oyarzun Narváez (Vicepresident)

## **7.2 Data processing agreements for Athens International Airport (AIA) validation demonstration**

**AIA-CDI**

### **Agreement**

**Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

**And:**

**CROWN DYNAMICS INTERNATIONAL LIMITED (CDI)**, 21 Station Road West, Oxted Surrey, RH8 9EE, United Kingdom, duly represented by Paul Townsend, Associate Director,

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161); They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**CDI**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of counting the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.

- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),

- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with

its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.

- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Hellenic Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Paul Townsend, Associate Director

For the Controller

Demetriades George, Director, IT&T Business Unit

**AIA-DIGINEXT**

#### **Agreement**

##### **Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

##### **And:**

**DIGINEXT**, 5 Rue Brindejone des Moulinais 31506 Toulouse Cedex 5 France, duly represented by Romain Charbit, Technical Project Leader (DXT),

Hereinafter: the Processor,

##### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);



They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to directly see what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**DIGINEXT**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of integrating the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.



**Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

**Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

**Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.

5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal

Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Hellenic Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Romain Charbit, Technical Project Leader

For the Controller

Demetriades George, Director, IT&T Business Unit

**AIA-EXODUS****Agreement****Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

**And:**

**EXODUS S.A.**, 73-75 Mesogeion Av & Estias Str 1, Postal Code 115 26, Athens, Greece, duly represented by Dimitris Skliros, CEO,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot

exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**EXODUS**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of monitoring and control of the evacuation mode and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring, to monitor

and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.
- The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.
- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Hellenic Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dimitris Skliros, CEO

For the Controller

Demetriades George, Director, IT&T Business Unit

**AIA-ICCS**

### **Agreement**

**Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

**And:**

**INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)**, Iroon Polytechniou, 9, 15773 Zografou, Attiki, Greece, duly represented by Konstantinos Karantzalos,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as the acquisition of video data at certain spectral regions by means of thermal and hyperspectral sensors enabling the measurement of crowd density, velocity and direction estimation, as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the



making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as the subsequent activities enabling the measurement of crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**ICCS**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of measuring crowd density, velocity and direction estimation and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Hellenic Republic shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Konstantinos Karantzalos, ICCS

For the Controller

Demetriades George, Director, IT&T Business Unit

**AIA-INDRA**

### **Agreement**

**Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

**And:**

**INDRA**, 73-75 CTRA. DE LOECHES, 9, Edificio Principal, 28850 Torrejón de Ardoz, Madrid, duly represented by Pedro Garibi Pérez, Safety & Security Engineer,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**INDRA**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in

accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of studying crowd behaviour and training algorithms for crowd behaviour monitoring and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

**Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Hellenic Republic shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Pedro Garibi Pérez, Safety & Security Engineer

For the Controller

Demetriades George, Director, IT&T Business Unit



### **Agreement**

**Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, IT&T Business Unit,

Hereinafter: the Controller,

**And:**

**UNIVERSITY OF SOUTHAMPTON IT INNOVATION CENTRE (IT INNOVATION)**, Gamma House, Enterprise Road, Southampton SO16 7NS, UK, duly represented by Dr Zoheir Sabeur, Science Director,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**IT INNOVATION**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).

- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean recording, transforming, processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of performing crowd analysis and algorithm calibration and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),

- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.

5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Hellenic Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dr Zoheir Sabeur, Science Director

For the Controller

Demetriades George, Director, IT&T Business Unit

**AIA-TIM**

**Agreement**

**Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

**And:**

**TELECOM ITALIA (TIM)**, Viale Parco de Medici, 61 – 00148 - Roma, duly represented by Marco Mancini, B.OG.D, Projects ICT - R&D Funding,

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161); They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally within their companies and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**TIM**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of studying crowd behaviour and training algorithms for crowd behaviour monitoring and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.

- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

**Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

**Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with the Greek Data Protection Law 2472/97, and any other applicable laws.

**Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),

- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the Processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.



- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Hellenic Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Hellenic Republic.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Marco Mancini, B.OG.D, Projects ICT - R&D Funding

For the Controller

Demetriades George, Director, IT&T Business Unit

**AIA-TUD**

#### **Agreement**

##### **Between:**

**ATHENS INTERNATIONAL AIRPORT S.A. (AIA)**, located at Spata, 19019, Greece, duly represented by Demetriades George, Director, IT&T Business Unit,

Hereinafter: the Controller,

##### **And:**

**TECHNISCHE UNIVERSITÄT DRESDEN (TUD)**, Helmholtzstrasse 10, Dresden, 01069, Germany represented by Sven Kreigenfeld, Head of Unit or his authorised representative

Acting Side: Faculty of Electrical and Computer Engineering, Institute of Principles of Electrical and Electronic Engineering; Chair of Circuit Design and Network Theory

Hereinafter: the Recipient,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at Athens International Airport in Athens, Greece on 27 January 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**ATHENS INTERNATIONAL AIRPORT** is a Controller within the meaning of Law 2472/97, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as the subsequent activities on analysing the operation of the chipless RFID system and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**TUD**, i.e. the Recipient, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons from the Controller or from subjects working on behalf of the Controller and collect Personal Data on behalf of the Controller. The Recipient will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws.

**Therefore, it has been agreed, as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Recipient' shall have the same meaning as in Law 2472/97, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of the operation of the chipless RFID system and providing the eVACUATE system with the number and type of persons who have crossed through a particular position that is used to maintain and keep up to date the Active Evacuation Route for a specific venue and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Recipient's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.

- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at Athens International Airport in Athens, Greece on 27 January 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Recipient shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants:
- that Personal Data will be processed in accordance with applicable data protection law and they are fit for their intended purpose herein;
  - that throughout the duration of the processing it will issue instructions to the Recipient in accordance with the applicable laws;
  - to inform Recipient without undue delay about relevant errors or irregularity.

#### **Article 4 – Warranties and obligations of the Recipient**

- 4.1. The Recipient agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Recipient agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),

- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Recipient also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Recipient further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Recipient undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Recipient shall also comply with the current and future applicable data protection legislation to the extent applicable to the Recipient.

4.5. The Recipient agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Recipient shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the Recipient accepts their obligation to accept and cooperate.

4.8. The Recipient shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Recipient shall notify the controller the cases of violation by the Recipient or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Recipient commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The parties shall be liable to each other for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual harm suffered.

Punitive damages (i.e. damages intended to punish the Recipient for its outrageous conduct) are specifically excluded.

- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Recipient shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Recipient prevents him from returning or destroying such data. In the latter case, the Recipient warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Hellenic Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the applicable competent court plaintiff.

Done in Athens, on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Recipient

.....

For the Controller

Demetriades George, Director, IT&T Business Unit

### **7.3 Data processing agreements for STX France (STX) validation demonstration**

Template only  
**STX-CDI**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

**And:**

**CROWN DYNAMICS INTERNATIONAL LIMITED (CDI)**, 21 Station Road West, Oxted Surrey, RH8 9EE, United Kingdom, duly represented by Paul Townsend, Associate Director,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**CDI**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of counting the crowd flow over time exiting the stands in the live demonstration in order to



validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.

- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

## **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

## **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and any other applicable laws.

## **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data



storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),

- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

## **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the French Republic shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Paul Townsend, Associate Director

For the Controller

[name], [position]

Template only  
**STX-DIGINEXT**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement****Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

**And:**

**DIGINEXT**, 5 Rue Brindejont des Moulinais 31506 Toulouse Cedex 5 France, duly represented by Romain Charbit, Technical Project Leader (DXT),

Hereinafter: the Processor,

#### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161); They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**DIGINEXT**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of integrating the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also

to the European Commission for the purposes of demonstration and evaluation of the work.

- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

## **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

## **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and any other applicable laws.

## **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),

- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm

suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the French Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Romain Charbit, Technical Project Leader

For the Controller

[name], [position]

Template only  
**STX-EXODUS**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

##### **And:**

**EXODUS S.A.**, 73-75 Mesogeion Av & Estias Str 1, Postal Code 115 26, Athens, Greece, duly represented by Dimitris Skliros, CEO,



Hereinafter: the Processor,

### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**EXODUS**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of monitoring and control of the evacuation mode and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.



- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),

- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.

- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the French Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dimitris Skliros, CEO

For the Controller

[name], [position]

Template only  
**STX-ICCS**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

##### **And:**

**INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)**, Iroon Polytechniou, 9, 15773 Zografou, Attiki, Greece, duly represented by Konstantinos Karantzalos,

Hereinafter: the Processor,

##### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as the acquisition of video data at certain spectral regions by means of thermal and hyperspectral sensors enabling the measurement of crowd density, velocity and direction estimation, as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**ICCS**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor. The Processor will also acquire and process thermal and hyperspectral data at a spatial resolution that does not allow the identification of natural persons.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of measuring crowd density, velocity and direction estimation and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons,

captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

#### **Article 2 – Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.

- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the French Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor  
Konstantinos Karantzalos, ICCS

For the Controller  
[name], [position]

Template only  
**STX-INDRA**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

##### **And:**

**INDRA**, 73-75 CTRA. DE LOECHES, 9, Edificio Principal, 28850 Torrejón de Ardoz, Madrid, duly represented by Pedro Garibi Pérez, Safety & Security Engineer,

Hereinafter: the Processor,

##### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study



crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**INDRA**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of studying crowd behaviour and training algorithms for crowd behaviour monitoring and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and

analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.
- The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.
- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the French Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Pedro Garibi Pérez, Safety & Security Engineer

For the Controller

[name], [position]

Template only  
**STX-ITInnovation**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement****Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

And:

**UNIVERSITY OF SOUTHAMPTON IT INNOVATION CENTRE (IT INNOVATION)**, Gamma House, Enterprise Road, Southampton SO16 7NS, UK, duly represented by Dr Zoheir Sabeur, Science Director,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of

subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**IT INNOVATION**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean recording, transforming, processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of performing crowd analysis and algorithm calibration and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and

promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.



- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.
- The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.
- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**



6.1. The laws of the French Republic shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dr Zoheir Sabeur, Science Director

For the Controller

[name], [position]

Template only  
**STX-TIM**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

**Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

**And:**

**TELECOM ITALIA (TIM)**, Viale Parco de Medici, 61 – 00148 - Roma, duly represented by Marco Mancini, B.OG.D, Projects ICT - R&D Funding,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161); They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd

behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**TIM**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of studying crowd behaviour and training algorithms for crowd behaviour monitoring and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the Processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the French Republic shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the French Republic.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Marco Mancini, B.O.G.D, Projects ICT - R&D Funding

For the Controller

[name], [position]

Template only  
**STX-TUD**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

**Between:**

**STX FRANCE S.A. (STX)**, [please insert identification details] located at Avenue Antoine Bourdelle, CS 90180, 44613 Saint Nazaire Cedex, France, duly represented by [name of STX representative], acting as [position],

Hereinafter: the Controller,

**And:**

**TECHNISCHE UNIVERSITÄT DRESDEN (TUD)**, Helmholtzstrasse 10, Dresden, 01069, Germany represented by Sven Kreigenfeld, Head of Unit or his authorised representative

Acting Side: Faculty of Electrical and Computer Engineering, Institute of Principles of Electrical and Electronic Engineering; Chair of Circuit Design and Network Theory

Hereinafter: the Processor,

### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration on a ship owned and operated by STX on 17 March 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**STX FRANCE S.A.** is a Controller within the meaning of Article 3 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot

exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**TUD**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons from the Controller or from subjects working on behalf of the Controller and collect Personal Data on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in Article 2, alinéa 2, Article 3, I., Article 2, alinéa 3 and Article 35, alinéa 2 of Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of the operation of the chipless RFID system and providing the eVACUATE system with the number and type of persons who have crossed through a particular position that is used to maintain and keep up to date the Active Evacuation Route for a specific venue and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration on a ship owned and operated by STX on 17 March 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles,



duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants:
- that Personal Data will be processed in accordance with applicable data protection law and they are fit for their intended purpose herein;
  - that throughout the duration of the processing it will issue instructions to the Processor in accordance with the applicable laws;
  - to inform Processor without undue delay about relevant errors or irregularity.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.



- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.
- The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.
- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the Processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The parties shall be liable to each other for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

<p>6.1. The laws of the French Republic shall apply to this Agreement.</p> <p>6.2. In case of a dispute, parties will try to solve the issue in an amicable way.</p> <p>6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the applicable competent court plaintiff.</p> <p>Done in [location], on _____ (date), in two copies, each party having received one.</p> <p>For the Processor</p> <p>[name], [position]</p> <p>For the Controller</p> <p>[name], [position]</p>
--

## 7.4 Data processing agreements for Metro Bilbao (METB) validation demonstration

<div>Template only <b>METB-CDI</b></div> <p><b>[Proposal only – subject to internal legal review and approval by eVACUATE partners]</b></p> <p><b>Agreement</b></p> <p><b>Between:</b> <b>METRO BILBAO S.A. (METB)</b>, [please insert identification details] located at [address], Spain, duly represented by [name of METB representative], acting as [position],</p> <p>Hereinafter: the Controller,</p> <p><b>And:</b> <b>CROWN DYNAMICS INTERNATIONAL LIMITED (CDI)</b>, 21 Station Road West, Oxted Surrey, RH8 9EE, United Kingdom, duly represented by Paul Townsend, Associate Director,</p> <p>Hereinafter: the Processor,</p> <p><b>Whereas</b></p> <p>The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);</p> <p>The parties have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their</p>
--

companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act] implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**CDI**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of counting the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as

for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.
- The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.
- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Kingdom of Spain shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Paul Townsend, Associate Director

For the Controller

[name], [position]

Template only  
**METB-DIGINEXT**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement****Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [address], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

**And:**

**DIGINEXT**, 5 Rue Brindejone des Moulinais 31506 Toulouse Cedex 5 France, duly represented by Romain Charbit, Technical Project Leader (DXT),

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act] implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as to count the crowd flow over time exiting the stands in the live demonstration in order to validate crowd models and test time delays of visual sensor data through to display of crowd density on screen and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**DIGINEXT**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of integrating the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to integrate the video recordings directly into the common operation picture (COP) for situation awareness completeness, enabling the decision maker to see directly what is happening in a crisis environment and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation



of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.

- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any

advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.
- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Romain Charbit, Technical Project Leader

For the Controller

[name], [position]

Template only  
**METB-EXODUS**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

**Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [name of METB representative], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

**And:**

**EXODUS S.A.**, 73-75 Mesogeion Av & Estias Str 1, Postal Code 115 26, Athens, Greece, duly represented by Dimitris Skliros, CEO,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transforming and analysing of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act] implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration

and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**EXODUS**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of monitoring and control of the evacuation mode and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

**Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

**Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.

- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request

received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dimitris Skliros, CEO

For the Controller

[name], [position]

Template only  
**METB-ICCS**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

**Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [name of METB representative], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

**And:**

**INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (ICCS)**, Iroon Polytechniou, 9, 15773 Zografou, Attiki, Greece, duly represented by Konstantinos Karantzas,

Hereinafter: the Processor,

### **Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring as well as the acquisition of video data at certain spectral regions by means of thermal and hyperspectral sensors enabling the measurement of crowd density, velocity and direction estimation, as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act] implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**ICCS**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on



behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor. The Processor will also acquire and process thermal and hyperspectral data at a spatial resolution that does not allow the identification of natural persons.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purpose of measuring crowd density, velocity and direction estimation and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 – Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
  - to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
  - to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

- 4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.
- 4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

- 4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

- 4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.
- 4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.
- 4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.
- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain .

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor  
Konstantinos Karantzalos, ICCS

For the Controller  
[name], [position]

Template only  
**METB-INDRA**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

### **Agreement**

**Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [name of METB representative], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

**And:**

**INDRA**, 73-75 CTRA. DE LOECHES, 9, Edificio Principal, 28850 Torrejón de Ardoz, Madrid, duly represented by Pedro Garibi Pérez, Safety & Security Engineer,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act], implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**INDRA**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

#### **Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of studying crowd behaviour and training algorithms for crowd behaviour monitoring and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:

- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
- to prevent data processing systems from being used without authorization (access control),
- to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

- 4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.
- 4.10. The Processor commits not to enter into subcontracts.

**Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Pedro Garibi Pérez, Safety & Security Engineer

For the Controller

[name], [position]

Template only  
**METB-ITInnovation**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement**



**Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [name of METB representative], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

**And:**

**UNIVERSITY OF SOUTHAMPTON IT INNOVATION CENTRE (IT INNOVATION)**, Gamma House, Enterprise Road, Southampton SO16 7NS, UK, duly represented by Dr Zoheir Sabeur, Science Director,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act], implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**IT INNOVATION**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).

- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean recording, transforming, processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of performing crowd analysis and algorithm calibration and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring as well as for measuring crowd density, velocity and direction estimation and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read,

copied, altered or removed without authorization during processing, use and after recording (access control),

- to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

**Article 5 – Liability, Term and Termination**

- 5.1. The Agreement is concluded for the duration of the eVACUATE project.
- 5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.
- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

**Article 6 – Applicable law, Mediation and Jurisdiction**

- 6.1. The laws of the Kingdom of Spain shall apply to this Agreement.
- 6.2. In case of a dispute, parties will try to solve the issue in an amicable way.
- 6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Dr Zoheir Sabeur, Science Director

For the Controller

[name], [position]

Template only  
**METB-TIM**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

**Agreement****Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [name of METB representative], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

**And:**

**TELECOM ITALIA (TIM)**, Viale Parco de Medici, 61 – 00148 - Roma, duly represented by Marco Mancini, B.OG.D, Projects ICT - R&D Funding,

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act] implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**TIM**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws of the Controller and the Processor.

**Therefore, it has been agreed, as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provisions from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of studying crowd behaviour and training algorithms for crowd behaviour monitoring and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's company, and also to the European Commission for the purposes of demonstration and evaluation of the work.

- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.
- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants that throughout the duration of the processing it will issue instructions to the Processor in accordance with [insert provisions from the Spanish Data Protection Act] and any other applicable laws.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
  - to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),
  - to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
  - to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),



- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the Processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The Processor shall be liable to the Controller for the damages it causes by any breach of the Articles above. Liability as between the parties shall be limited to actual harm suffered. Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) shall be specifically excluded.

5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with



its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.

- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Kingdom of Spain shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute to the competent courts in the Kingdom of Spain.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

Marco Mancini, B.OG.D, Projects ICT - R&D Funding

For the Controller

[name], [position]

Template only  
**METB-TUD**

**[Proposal only – subject to internal legal review and approval by eVACUATE partners]**

#### **Agreement**

##### **Between:**

**METRO BILBAO S.A. (METB)**, [please insert identification details] located at [name of METB representative], Spain, duly represented by [name of METB representative], acting as [position],

Hereinafter: the Controller,

##### **And:**

**TECHNISCHE UNIVERSITÄT DRESDEN (TUD)**, Helmholtzstrasse 10, Dresden, 01069, Germany represented by Sven Kreigenfeld, Head of Unit or his authorised representative

Acting Side: Faculty of Electrical and Computer Engineering, Institute of Principles of Electrical and Electronic Engineering; Chair of Circuit Design and Network Theory

Hereinafter: the Processor,

**Whereas**

The parties are partners in the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161);

They have agreed to participate in a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, which forms part of the eVACUATE solution, during and after the demonstration at San Mames Metro Station in Bilbao, Spain, on 5<sup>th</sup> May 2017, and the compilation of subsequent reports and related research only in the framework of the research activities of the eVACUATE project;

**METRO BILBAO S.A.** is a Controller within the meaning of [insert provision from the Spanish Data Protection Act] implementing Directive 95/46/EC, for the personal data collected and processed in relation to the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and train algorithms for crowd behaviour monitoring, to monitor and control the evacuation mode as well as to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work, as explained above and used only for these research purposes within the eVACUATE project;

**TUD**, i.e. the Processor, agrees to process the still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons from the Controller or from subjects working on behalf of the Controller and collect Personal Data on behalf of the Controller. The Processor will perform technical processing and analysis of the still images (photographs) and moving images (video recordings) for the above research purposes in accordance with the instructions of the Controller and with the applicable data protection laws.

**Therefore, it has been agreed, as follows:**

**Article 1 – Definitions**

- 1.1. 'Personal Data', 'Controller', 'Processing' and 'Processor' shall have the same meaning as in [insert provision from the Spanish Data Protection Act], implementing Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Directive 95/46/EC).
- 1.2. 'Technical processing and analysis of the still images (photographs) and moving images (video recordings)' shall mean processing, analysis and understanding of the captured still images (photographs) and moving images (video recordings) for the purposes of the operation of the chipless RFID system and providing the eVACUATE system with the number and type of persons who have crossed through a particular position that is used to maintain and keep up to date the Active Evacuation Route for a specific venue and for dissemination and promotion of the project and the outcomes of the pilot exercises internally, within the Processor's organisation, and also to the European Commission for the purposes of demonstration and evaluation of the work.
- 1.3. 'Data Subjects' shall mean the volunteers who participate in the recording and processing activities, as described in item 1.2 above.

- 1.4. The categories of Personal Data collected and further processed in the framework of the aforementioned activity are still images (photographs) and moving images (video recordings) containing personal data, such as images of identifiable natural persons, captured during the demonstration at San Mames Metro Station in Bilbao, Spain on 5<sup>th</sup> May 2017.

#### **Article 2 - Subject**

- 2.1. The Agreement governs the processing of Personal Data undertaken by the parties thereto in the context of a research activity involving the making, transformation and analysis of still images (photographs) and moving images (video recordings) in order to study crowd behaviour and to train algorithms for crowd behaviour monitoring and to analyse the operation of the chipless RFID system providing the eVACUATE system with the number and type of persons who have crossed through a particular position and used to maintain and keep up to date the Active Evacuation Route for a specific venue and to disseminate and promote the project and the outcomes of the pilot exercises internally, within their companies and/or organisations, and also to the European Commission for the purposes of demonstration and evaluation of the work in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme (SEC – 2012.4.2-2, Grant Agreement Number 313161). It regulates the roles, duties, responsibilities and liabilities of the partners to this Agreement who are involved in the data processing activity.
- 2.2. The Processor shall only process the Personal Data collected by means of capturing the still images (photographs) and moving images (video recordings) on and in accordance with the instructions of the Controller.

#### **Article 3 – Warranties and obligations of the Controller**

- 3.1. The Controller agrees and warrants:
- that Personal Data will be processed in accordance with applicable data protection law and they are fit for their intended purpose herein;
  - that throughout the duration of the processing it will issue instructions to the Processor in accordance with the applicable laws;
  - to inform Processor without undue delay about relevant errors or irregularity.

#### **Article 4 – Warranties and obligations of the Processor**

- 4.1. The Processor agrees and warrants that he will only act on and in accordance with the instructions of the Controller and will process the Personal Data only on the Controller's behalf.
- 4.2. The Processor agrees and warrants:
- to prevent unauthorized persons from gaining access to data processing systems for processing or using personal data (access control),
  - to prevent data processing systems from being used without authorization (access control),
  - to ensure that persons authorized to use a data processing system have access only to those data they are authorized to access, and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording (access control),
  - to ensure that personal data cannot be read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media, and that it is possible to ascertain and check which bodies are to be transferred personal data using data transmission facilities (disclosure control),

- to ensure that it is possible after the fact to check and ascertain whether personal data have been entered into, altered or removed from data processing systems and if so, by whom (input control),
- to ensure that personal data processed on behalf of others are processed strictly in compliance with the controller's instructions (job control),
- to implement appropriate technical measures to ensure that personal data are protected against accidental destruction or loss (availability control),
- to ensure that data collected for different purposes can be processed separately.

These measures shall ensure, having regard to the state of the art and the cost of their implementation, a level of security appropriate to the risks presented by the processing and the nature of the data to be protected.

The Processor also undertakes to take reasonable steps to ensure the reliability of any of his employees, who have access to the personal data.

4.3. The Processor further agrees that he shall not process the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties without prior authorisation by the Controller.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to the transformation of the video recordings and to abide by any advice and/or instructions issued by the competent national data protection authority with regard to the processing of these Personal Data.

The Processor shall also comply with the current and future applicable data protection legislation to the extent applicable to the Processor.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority, unless prohibited by law, (2) any accidental or unauthorised access, and (3) any request received from the data subjects with regard to the processing of these Personal Data pursuant to this Agreement.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorisation to do so from the Controller.

4.7. The Controller reserves the right to monitor the data processing activities and the Processor accepts their obligation to accept and cooperate.

4.8. The Processor shall rectify, erase and block the Personal Data when requested to do so by the Controller or by the data subject as well as after the processing has been carried out.

4.9. The Processor shall notify the controller the cases of violation by the Processor or its employees of provisions to protect personal data or of the terms specified by the controller.

4.10. The Processor commits not to enter into subcontracts.

#### **Article 5 – Liability, Term and Termination**

5.1. The Agreement is concluded for the duration of the eVACUATE project.

5.2. The parties shall be liable to each other for the damages it causes by any breach of the above Articles. Liability as between the parties shall be limited to actual harm suffered.

Punitive damages (i.e. damages intended to punish the Processor for its outrageous conduct) are specifically excluded.

- 5.3. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party does not comply with its obligations under this Agreement and has failed to remedy such default within fourteen (14) days after due notice.
- 5.4. Parties agree that upon termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In the latter case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

#### **Article 6 – Applicable law, Mediation and Jurisdiction**

6.1. The laws of the Kingdom of Spain shall apply to this Agreement.

6.2. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled amicably in due time, either party may bring the dispute before the applicable competent court plaintiff.

Done in [location], on \_\_\_\_\_ (date), in two copies, each party having received one.

For the Processor

[name], [position]

For the Controller

[name], [position]

## 8 Appendix III: Notifications to national data protection authorities

### 8.1 Notification submitted by Anoeta Stadium Real Sociedad (ASRS) to the Spanish Data Protection Authority

The controller has confirmed that necessary steps have been taken to consult the necessity of notifying the Spanish Data Protection Authority of the validation demonstrations.

### 8.2 Notification submitted by Athens International Airport (AIA) to the Hellenic Data Protection Authority

<b>Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα</b> Κηφισίας 1-3, Αμπελόκηποι, ΤΚ 115 23 Αθήνα Internet Site: <a href="http://www.dpa.gr">www.dpa.gr</a> Τηλ.: 210 6475601, Fax: 210 6475628		
<b>ΠΑΡΑΡΤΗΜΑ</b>		
Το παρόν έντυπο συνοδεύει το Έντυπο 2.0 της γνωστοποίησης (ένα για κάθε Έντυπο 2.0)		
<b>I. Πηγές και αποδέκτες</b>		
223. Συμπληρώστε με X τις πηγές και τους αποδέκτες των δεδομένων σας τον παρακάτω πίνακα:		
Π=Πηγές : Αυτοί από τους οποίους αντλείτε τις πληροφορίες    Α=Αποδέκτες : Αυτοί που λαμβάνουν πληροφορίες		
Κωδικός	Π	Α
Κωδικός Περιγραφή	Π	Α
P11 Τα ίδια τα υποκείμενα	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Φυσικά ή Νομικά Πρόσωπα που συνδέονται</b>		
P21 Οικογένεια / Συγγενείς	<input type="checkbox"/>	<input type="checkbox"/>
P22 Εντολοδόχοι	<input type="checkbox"/>	<input type="checkbox"/>
P23 Συνεργάτες	<input type="checkbox"/>	<input type="checkbox"/>
P24 Οικονομικοί αντιπρόσωποι	<input type="checkbox"/>	<input type="checkbox"/>
P25 Παρέχοντες Υπηρεσίες Υγείας	<input type="checkbox"/>	<input type="checkbox"/>
P26 Συμβολαιογράφοι	<input type="checkbox"/>	<input type="checkbox"/>
P27 Άλλοι	<input type="checkbox"/>	<input type="checkbox"/>
<b>Φυσικά ή Νομικά Πρόσωπα που συνδέονται</b>		
P31 Άλλα φυσικά πρόσωπα της ίδιας επιχείρησης	<input type="checkbox"/>	<input checked="" type="checkbox"/>
P32 Άλλα νομικά πρόσωπα του ίδιου ομίλου	<input type="checkbox"/>	<input type="checkbox"/>
P33 Άλλα τμήματα του ίδιου οργανισμού / επιχείρησης	<input type="checkbox"/>	<input type="checkbox"/>
P34 Πελάτες αγαθών / υπηρεσιών	<input type="checkbox"/>	<input type="checkbox"/>
P35 Άλλοι	<input type="checkbox"/>	<input checked="" type="checkbox"/>
P44 Υπουργεία	<input type="checkbox"/>	<input type="checkbox"/>
P45 Δικαστήρια	<input type="checkbox"/>	<input type="checkbox"/>
P46 Δημόσιες Αρχές	<input type="checkbox"/>	<input type="checkbox"/>
P47 Υποθηκοφυλακεία	<input type="checkbox"/>	<input type="checkbox"/>
P48 Οργανισμοί Τοπικής Αυτοδιοίκησης	<input type="checkbox"/>	<input type="checkbox"/>
P49 Εθνικό Τυπογραφείο (ΦΕΚ)	<input type="checkbox"/>	<input type="checkbox"/>
P50 Άλλοι	<input type="checkbox"/>	<input type="checkbox"/>
<b>Νομικά Πρόσωπα Ιδιωτικού Δικαίου</b>		
P61 Χρηματοπιστωτικοί φορείς	<input type="checkbox"/>	<input type="checkbox"/>
P62 Ασφαλιστικοί φορείς	<input type="checkbox"/>	<input type="checkbox"/>
P63 Ενώσεις προσώπων (Σωματεία)	<input type="checkbox"/>	<input type="checkbox"/>
P64 Άλλοι	<input type="checkbox"/>	<input type="checkbox"/>
P71 Τύπος	<input type="checkbox"/>	<input type="checkbox"/>
P72 Δημόσια προσιτοί κατάλογοι (Επικοινωνία)	<input type="checkbox"/>	<input type="checkbox"/>

Νομικά Πρόσωπα Δημοσίου Δικαίου	
P41 Λοιπές Δημόσιες Υπηρεσίες	<input type="checkbox"/> <input type="checkbox"/>
P42 Ασφαλιστικά Ταμεία (ΙΚΑ, ΤΕΒΕ κλπ)	<input type="checkbox"/> <input type="checkbox"/>
P43 Φορείς Κοινή Ωφέλειας (ΟΤΕ, ΔΕΗ,	<input type="checkbox"/> <input type="checkbox"/>

P73 Οδηγοί / κατάλογοι εκθέσεων, επαγγελμαμάτων, εταιρειών, διαφημιστικά φυλλάδια κλπ  
P74 Άλλοι

**224. Άλλες πηγές, αναφέρατε:**

---



---



---

**225. Άλλοι αποδέκτες, αναφέρατε:**

**Ερευνητικοί Φορείς, Πανεπιστήμια, Εταιρίες**

---



---



---

**II. Κατηγορίες Προσωπικών Δεδομένων**

**226. Σημειώστε με Χ τα προσωπικά δεδομένα (ευαίσθητα και μη) που υφίστανται επεξεργασία / περιέχονται στο αρχείο σας:**

**Ομάδα Α: ΔΕΔΟΜΕΝΑ ΜΗ ΕΥΑΙΣΘΗΤΑ**

<p><b>A1. Στοιχεία Αναγνώρισης</b></p> <p><input type="checkbox"/> A1.0 Προσωπικά στοιχεία</p> <p><input type="checkbox"/> A1.1 Επίσημα στοιχεία Ληξιαρχείου</p> <p><input type="checkbox"/> A1.3 Καταγωγή</p> <p><input type="checkbox"/> A1.4 Στοιχεία Ταυτότητας (πχ Υπηκοότητα)</p> <p><input type="checkbox"/> A1.5 Λοιπά στοιχεία αναγνώρισης</p> <p><b>A2. Προσωπικά χαρακτηριστικά</b></p> <p><input checked="" type="checkbox"/> A2.0 Φυσικά χαρακτηριστικά</p> <p><input type="checkbox"/> A2.1 Ενδιαφέροντα, συνήθειες</p> <p><input type="checkbox"/> A2.2 Μετακινήσεις – ταξίδια</p> <p><input type="checkbox"/> A2.3 Στοιχεία προσωπικότητας</p> <p><input type="checkbox"/> A2.4 Λοιπά στοιχεία προσωπικών</p> <p><b>A3. Οικογενειακές συνθήκες</b></p> <p><input type="checkbox"/> A3.0 Έγγαμος βίος</p> <p><input type="checkbox"/> A3.1 Οικογενειακή κατάσταση</p> <p><input type="checkbox"/> A3.2 Κοινωνικές επαφές</p> <p><input type="checkbox"/> A3.3 Λοιπά στοιχεία οικογενειακών συνθηκών</p> <p><b>A4. Εκπαίδευση</b></p> <p><input type="checkbox"/> A4.0 Δεδομένα ακαδημαϊκής δραστηριότητας</p> <p><input type="checkbox"/> A4.1 Τομείς ειδίκευσης και πιστοποιητικά</p> <p><input type="checkbox"/> A4.2 Σπουδαστικό / Μαθητικό Αρχείο</p> <p><input type="checkbox"/> A4.3 Εγγραφή σε επιτροπές</p> <p><input type="checkbox"/> A4.4 Επαγγελματική ειδίκευση</p>	<p><b>A5. Οικονομική κατάσταση</b></p> <p><input type="checkbox"/> A5.0 Έσοδα, περιουσιακά στοιχεία,</p> <p><input type="checkbox"/> A5.1 Απολογισμός εξόδων</p> <p><input type="checkbox"/> A5.2 Δάνεια, υποθήκες, πιστώσεις</p> <p><input type="checkbox"/> A5.3 Επιδόματα, εργασιακά προνόμια,</p> <p><input type="checkbox"/> A5.4 Δεδομένα ασφάλισης, σύνταξης</p> <p><input type="checkbox"/> A5.5 Αγαθά και υπηρεσίες που</p> <p><input type="checkbox"/> A5.6 Αγαθά και υπηρεσίες που προσφέρει</p> <p><input type="checkbox"/> A5.7 Τραπεζικοί λογαριασμοί, πιστωτικές</p> <p><input type="checkbox"/> A5.8 Κληρονομιά</p> <p><input type="checkbox"/> A5.9 Αποζημίωση</p> <p><input type="checkbox"/> A5.10 Λοιπά στοιχεία οικονομικής</p> <p><b>6. Εργασία</b></p> <p><input type="checkbox"/> A6.0 Παρούσα εργασία</p> <p><input type="checkbox"/> A6.1 Δεδομένα Πρόσληψης</p> <p><input type="checkbox"/> A6.2 Ιστορικό εργασίας</p> <p><input type="checkbox"/> A6.3 Εργασιακή συμπεριφορά</p> <p><input type="checkbox"/> A6.4 Περιγραφή εργασίας</p> <p><input type="checkbox"/> A6.5 Αξιολόγηση εργασίας</p> <p><input type="checkbox"/> A6.6 Εκπαιδευτικό αρχείο</p> <p><input type="checkbox"/> A6.7 Δεδομένα ασφάλειας</p> <p><input type="checkbox"/> A6.8 Αμοιβές και κρατήσεις</p> <p><input type="checkbox"/> A6.9 Εργασιακές παροχές</p>
---	---



☐ A4.5 Λοιπά στοιχεία

☐ A6.10 Λοιπά στοιχεία εργασίας

**A7. Δεδομένα ηλεκτρονικών επικοινωνιών**
☐ A.7.0 Δεδομένα θέσης

☐ A.7.1 Δεδομένα κίνησης

☐ A.7.2. Άλλο

**Ομάδα Β: ΕΥΑΙΣΘΗΤΑ ΔΕΔΟΜΕΝΑ**
**B1. Φυλετική ή Εθνική προέλευση**
☐ B1.0 Εθνική Καταγωγή

☐ B1.1 Μειονότητες

☐ B1.2 Φυλετική προέλευση

**B2. Πολιτικά Φρονήματα**
☐ B2.0 Δεδομένα πολιτικών πεποιθήσεων

**B3. Θρησκευτικές Πεποιθήσεις**
☐ B3.0 Δεδομένα θρησκευτικής πίστης

**B4. Φιλοσοφικές Πεποιθήσεις**
☐ B4.0 Δεδομένα φιλοσοφικών πεποιθήσεων

**B5. Συνδικαλιστική δράση**
☐ B5.0 Συνδικαλιστική δραστηριότητα

**B6. Υγεία**
☐ B6.0 Φυσική κατάσταση

☐ B6.1 Πνευματική κατάσταση

☐ B6.2 Ανικανότητες και αναπηρίες

☐ B6.3 Διαιτητικές ή άλλες σχετικές ανάγκες

☐ B6.4 Ιατρικό ιστορικό ασθενούς

☐ B6.5 Χορήγηση φαρμάκων

☐ B6.6 Λοιπά στοιχεία υγείας

**B7. Κοινωνική πρόνοια (για φορείς με συναφή**
☐ B7.0 Ασφάλιση

☐ B7.1 Σύμβαση

**B8. Ερωτική ζωή**
☐ B8.0 Σεξουαλική ζωή

**B9. Ποινικές διώξεις**
☐ B9.0 Καταγγελίες

☐ B9.1 Διώξεις

☐ B9.2 Διοικητικά μέτρα

☐ B9.3 Διοικητικές ποινές

**B10. Καταδίκες**
☐ B10.1 Αποφάσεις δικαστηρίων

☐ B10.2 Ποινικό Μητρώο

**III. Τόποι επεξεργασίας**

227. Συμπληρώστε τους τόπους επεξεργασίας των δεδομένων σας (αν είναι περισσότεροι του ενός):

**Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:**

228. Οδός: **Κτήριο Διοίκησης (17)**

229.Αριθμός:

230.

Ταχ.Κώδικας:

**19019**

231. Πόλη :

**ΣΠΑΤΑ**
**Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:**

228. Οδός: **Ηρώων Πολυτεχνείου**

229.Αριθμός:

**9**

230.

Ταχ.Κώδικας:

**15773**

231. Πόλη :

**Αθήνα- Ζωγράφου**
**Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:**

228. Οδός: **CTRA. DE LOECHES , Edificio Principal, Torrejón de Ardoz,**

229.Αριθμός:

**9**

230.

Ταχ.Κώδικας:

**28850**

231. Πόλη :

**Madrid**
**Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:**

228. Οδός:	Station Road West, Oxted	229.Αριθμός:	21
230. Ταχ.Κώδικας:	RH8 9EE	231. Πόλη :	Surrey
<b><u>Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:</u></b>			
228. Οδός:	Rue BrindeJonc des Moulinais	229.Αριθμός:	5
230. Ταχ.Κώδικας:	31506	231. Πόλη :	Toulouse
<b><u>Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:</u></b>			
228. Οδός:		229.Αριθμός:	
230. Ταχ.Κώδικας:		231. Πόλη :	
<b><u>Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:</u></b>			
228. Οδός:		229.Αριθμός:	
230. Ταχ.Κώδικας:		231. Πόλη :	
<b><u>Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:</u></b>			
228. Οδός:		229.Αριθμός:	
230. Ταχ.Κώδικας:		231. Πόλη :	
<b><u>Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:</u></b>			
228. Οδός:		229.Αριθμός:	
230. Ταχ.Κώδικας:		231. Πόλη :	
<b><u>Τόπος διεξαγωγής επεξεργασίας / εγκατάστασης αρχείου:</u></b>			
<b>IV. Εκτελούντες την επεξεργασία</b>			
<b>232. Συμπληρώστε τους εκτελούντες την επεξεργασία των δεδομένων σας (αν είναι περισσότεροι του ενός):</b>			
233. Επωνυμία /			
Ονοματεπώνυμο:	Διεθνής Αερολιμένας Αθηνών/Νικόλαος Παπαγιαννόπουλος		
234. Κύρια δραστηριότητα /			
Επάγγελμα:	Αρχιτέκτονας Βάσεων Δεδομένων (IT&T)		
Κτήριο		236.	
235. Οδός:	Διοίκησης (17)	Αριθμός :	237. Ταχ.Κώδικας: 19019
239.		240.	
Σπάτ	Χώρ	Ελλάς	Ηλεκτρονική
238. Πόλη :	α	α	ΠαπαγιαννοπουλοςN@aia.gr
		διεύθυνση:	

233. Επωνυμία /	<b>Institute of Communication and Computer Systems (ICCS),</b>			
Ονοματεπώνυμο:	<b>Ζαχαρίας Κανδυλάκης,</b>			
234. Κύρια δραστηριότητα /				
Επάγγελμα:	<b>Ερευνητικό Κέντρο/ Βοηθός Ερευνητής</b>			
	<b>Ηρώων</b>	236.		
235. Οδός:	<b>Πολυτεχνείου</b>	Αριθμός :	<b>9</b>	237. Ταχ.Κώδικας: <b>15773</b>
		240.		
	239.	Ηλεκτρονική		
238. Πόλη :	<b>Αθήνα</b>	Χώρα	<b>Ελλάς</b>	διεύθυνση: <b>zach.kandylakis@gmail.com</b>
233. Επωνυμία /	<b>INDRA/ Pedro Garibi Pérez</b>			
Ονοματεπώνυμο:				
234. Κύρια δραστηριότητα /				
Επάγγελμα:	<b>Safety &amp; Security Engineer</b>			
	<b>CTRA. DE LOECHES,</b>	236.	237.	
235. Οδός:	<b>Edificio Principal,</b>	Αριθμός :	<b>9</b>	Ταχ.Κώδικας: <b>28850</b>
	<b>Torrejón de</b>	239.	240. Ηλεκτρονική	
238. Πόλη :	<b>Ardoz,</b>	Χώρα	<b>Madrid</b>	διεύθυνση: <b>pgaribi@indra.es</b>
233. Επωνυμία /	<b>University of Southampton IT Innovation Centre</b>			
Ονοματεπώνυμο:	<b>(ITInnovation)/Dr Zoheir A. Sabeur,</b>			
234. Κύρια δραστηριότητα /				
Επάγγελμα:	<b>Science Director</b>			
		236.	237.	
235. Οδός:	<b>Gamma House,</b>	Αριθμός :	Ταχ.Κώδικας: <b>SO167NS,</b>	
	<b>Enterprise Road,</b>	239.	240. Ηλεκτρονική <b>zas@it-</b>	
238. Πόλη :	<b>Southampton</b>	Χώρα	<b>UK</b>	διεύθυνση: <b>innovation.soton.ac.uk</b>
233. Επωνυμία /	<b>Crowd Dynamics International Limited (CDI) / Paul Townsend,</b>			
Ονοματεπώνυμο:				
234. Κύρια δραστηριότητα /				
Επάγγελμα:	<b>Associate Director</b>			
	<b>Station Road</b>	236.		
235. Οδός:	<b>West</b>	Αριθμός :	<b>21</b>	237. Ταχ.Κώδικας: <b>RH8 9EE</b>
		240.		
	239.	Ηλεκτρονική		
238. Πόλη :	<b>Surrey</b>	Χώρα	<b>UK</b>	διεύθυνση: <b>paul.townsend@crowddynamics.com</b>
233. Επωνυμία /	<b>DIGINEXT / Romain Charbit</b>			
Ονοματεπώνυμο:				
234. Κύρια δραστηριότητα /				
Επάγγελμα:	<b>Technical Project Leader</b>			

235. Οδός:	<b>Rue BrindeJonc des Moulinais</b>	236. Αριθμός :	<b>5</b>	237. Ταχ.Κώδικας:	<b>31506</b>
			240.		
238. Πόλη :	<b>Toulouse</b>	239. Χώρα	<b>France</b>	240. Ηλεκτρονική διεύθυνση:	<b>romain.charbit@diginext.fr</b>
233. Επωνυμία / Ονοματεπώνυμο:					
234. Κύρια δραστηριότητα / Επάγγελμα:					
235. Οδός:		236. Αριθμός :		237. Ταχ.Κώδικας:	
			240. Ηλεκτρονική διεύθυνση:		
238. Πόλη :		239. Χώρα			

### 8.3 Notification submitted by STX France (STX) to the French Data Protection Authority

The controller has advised that notification to the French Data Protection Authority (CNIL) is not necessary in the case of validation demonstrations.

### 8.4 Notification submitted by Metro Bilbao (METB) to the Spanish Data Protection Authority

The controller has confirmed that the internal legal department has been consulted on this matter and appropriate steps have been taken, if and as necessary. Guidance has been provided on the required steps that have to be taken at national level and assistance with the consent form and the data processing agreements has been provided when requested.