EVACUATE

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:	D. 11.4
Delivery Date:	Mar 31, 2015
Classification:	Public
Editor(s):	Diana Dimitrova (ICRI/CIR, KUL)
Document version:	1.0 - 2015
Contract Start Date:	April 1st, 2013
Duration:	48 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
7th Framework Programme

SEVENTH FRAMEWORK PROGRAMME

Document Control Page

Title	**Ethical and legal evaluation report and recommendations**	
Editors	Diana Dimitrova	ICRI/CIR, KUL
Contributors	Name	Partner
	Nikolaos Papagiannopous	AIA
	Konstantinos Loupos	ICCS
Peer Reviewers	Hanneke Vreugdenhil	HKV
	Eduardo Martinez Gil	INDRA
Format	Text - Ms Word	
Language	en-UK	
Work-Package	WP 11	
Deliverable number	D.11.4	
Due Date of Delivery	31/03/2015	
Actual Date of Delivery	31/03/2015	
Dissemination Level	One of the following: Public Restricted to other programme participants (including the Commission Services) Restricted to a group specified by the consortium (including the Commission Services) Confidential, only for members of the consortium (including the Commission Services)	
Rights	eVACUATE Consortium	
Audience	☒ public ☐ restricted ☐ internal	
Date	31/03/2015	
Revision	HKV, INDRA	
Version	1.0	
Edited by	Diana Dimitrova (ICRI/CIR, KUL)	
Status	☐ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	01/03/2015	Initial draft	Diana Dimitrova (KUL)
0.2	10/03/2015	Comments by HKV and EXUS	Hanneke Vreugdenhil HKV) and Dimitris Petrantonakis (EXUS)
0.3	12/03/2015	Review of original text	Eduardo Martinez Gil (INDRA)
1.0	31/03/2015	Final version	Diana Dimitrova (KUL)

Table of Contents

Table of Figures

Executive Summary

The purpose of the present deliverable is to discuss in more depth the data protection requirements and principles that the project partners in eVACUATE have to follow in the course of their research activities when they work with personal data. The high-level requirements were provided in D11.1. However, with the advancement of the project, more clarifications and guidance in the application of the general principles have been needed in the past months. Therefore, this deliverable will report on the legal recommendations that have been provided to the partners and systematize the recommendations for the future activities of the partners when working with personal data. At the end, in Annex III, the partners can find a preliminary table (V1) which can help them assess their compliance with the data protection requirements.

D 11.4 is submitted together with D 11.2 on Ethical and Legal specifications, evaluation and recommendations. While D 11.2 focuses on the evaluation and recommendations with regards to the design of technologies developed in eVACUATE, this deliverable deals with the recommendations (and where applicable also evaluation of) on compliance with legal and ethical requirements during the research phase of the project. One of the tasks in WP11 concerns also ethical issues. Some of them have already been mentioned in D11.1 (e.g. aspects related to disabled people and children). Further ethical aspects, e.g. related to possible discrimination through (video) surveillance, are discussed in D11.2, which is submitted simultaneously with D11.4.

1. Introduction

Deliverable D11.1 already outlined the general data protection procedures that need to be followed in the research phase of the project. However, as their application to the research activities in eVACUATE has not always been straightforward to all partners in the project, this deliverable aims to assist the partners on how to implement the requirements in their work which involves personal data. Where relevant, practical examples will be provided. The application of the data protection requirements to research activities was explained in more detail already during the Plenary Meeting in Madrid (30 September – 2 October 2014):

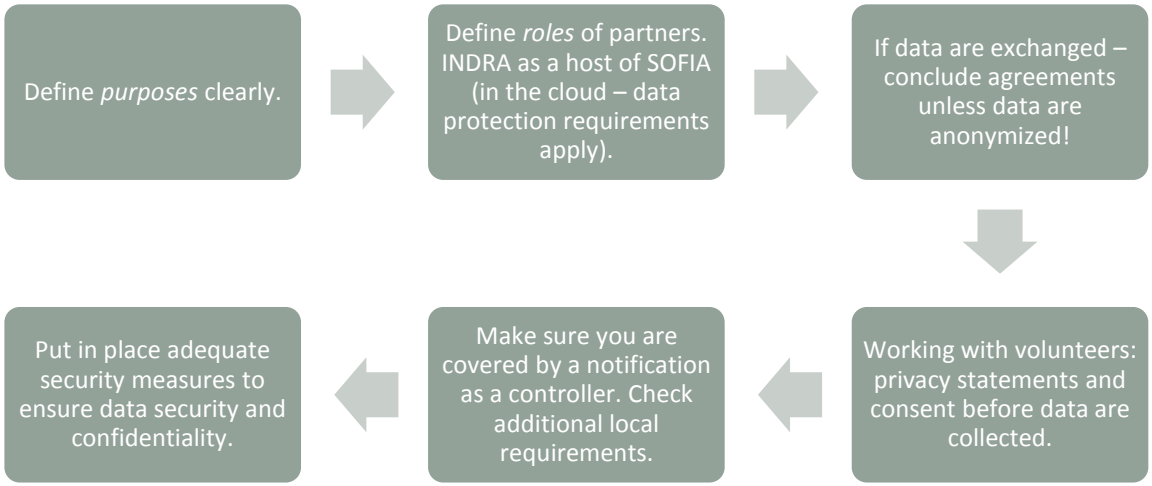

Figure 1: How to work with personal data in eVACUATE

In the following chapters these requirements will be elaborated on. With regards to the definition of personal data, the concept of what constitutes personal data was already discussed at length in D 11.1. As a recap, personal data means any information that may lead directly or indirectly to the identification of individuals, unless it is anonymized in such a way that there is no risk of identifiability. It is important for partners to bear in mind that compliance with the procedures elaborated below starts *in advance of* the actual research activity in which personal data will be processed. Therefore, partners are advised to start planning their activities several months *before each of* their personal data processing activities.

2. Data protection requirements when working with personal data

2.1. Purpose definition

Before personal data are processed (i.e. even *before the data are collected*), the partners should define the *purposes* for which they need to process the personal data. While it is evident most of the times that the data will be needed for research purposes, it is advisable to specify more narrowly these purposes. For example, when video recordings were made at Athens Airport (AIA) with actual passengers in April 2014, the reported purposes of these recordings were reported to study crowd dynamics and passenger flow, as well as collect data for algorithm training. Such narrower definition is recommendable for every separate research activity where personal data are processed. Defining the purpose is essential for determining what the boundaries of the legitimate use of the data are, which data and what storage period are relevant for that particular data processing.

2.2. Definition of the roles of the partners

As discussed in D11.1, *every separate* research activity needs to have a *controller*. This is the party that defines the means and purposes of the processing and takes responsibility for complying with the data protection requirements and procedures. Under the current data protection framework, the applicable law is the national law of the controller. Hence defining which partner will be the controller is essential, so that the further procedures according to the applicable national law are followed. For example, currently there is a requirement for submission of a notification to the national data protection authority of the controller and the exact proceedings are a matter of national law. When the Proposed General Data Protection Regulation enters into force, then it is expected that there will be only one applicable law for all EU Member States, namely the said Regulation. Still, certain local specifications could remain, e.g. in which cases a notification need to be submitted to the national DPA and what the exact content of the notification would be. Thus, the local specifications would still need to be observed.

In the above-mentioned example of AIA, the recordings were made at AIA. Some of the recordings were taken with equipment which belonged to ICCS, while others – with AIA equipment. Nevertheless, the images were immediately provided to AIA after the recordings and ICCS did not have access to them. Thus, from the very beginning the only partner having access to the images was AIA and their rules on further disclosure and usage of the data were followed, as defined by national law.

It is also possible that more than one partner is the controller for a particular activity. There are three possible constellations in such a case: (1) there are separate controllers, whereby the different controllers remain separated, take their decisions separately and each one is responsible separately although they work loosely together; (2) there are joint controllers, and each one will be responsible for a different subset of the data processing or (3) all the controllers will be responsible together for the entire operation. In (2) and (3) the controllers share the decision-making process.[1] In all cases each controller has to comply with his own obligations under his national law under the current framework. For this reason in practice it is considered easier when one party is the controller.

A data processing activity can also have one or more *processors*. These are normally the partners that processes personal data on behalf of the controller for the same purpose as the controller and only under his/her instructions. This could be the case, for example, when during the validation demonstrations one partner, e.g. the end-user, is designated as the controller and the other partners who process personal data (e.g. for analytical and evaluation purposes) during the demonstration and after it are the processors.

Special attention needs to be paid to the role that *INDRA* plays as the host of SOFIA. SOFIA is the backbone of eVACUATE, i.e. the platform through which all the data will be processed. This means that technically INDRA can obtain access to the data processed through SOFIA, thus in essence they would be involved in the processing of personal data. Therefore, their specific role in each data processing activity needs to be *defined in advance* so that its responsibilities are clarified and if necessary, agreements with the (other) controllers are signed. No matter whether INDRA as the host of SOFIA will be involved as a controller or processor for the separate data processing activities, the organization still has responsibilities in terms of the security of (personal) data that will be processed via SOFIA.

2.3. Collection of data from volunteers

When project partners collect data directly from volunteers, they must provide the volunteers *at least* with the following information: the identity and contact of the controller; the purposes of the processing and how the individuals can exercise their rights - to access, rectify, block or erase their personal data, withdraw consent, object to the processing. It is recommendable also to mention how the data will be processed, whether the data will be stored and for how long, whether it will be shared with other partners in addition to the controller.

[1] Olsen, T. and Mahler, T. "Identity management and data protection law: Risks, responsibility and compliance in 'Circles of Trust' – Part II," Elsevier, Computer Law and Security Report 23 (2007), p.419.

This information is needed so that the volunteers can make an informed decision whether to disclose their personal data or not and how to exercise their rights once they give their consent for the data processing. After the information has been provided, the controller should ask for their consent.
A template of a privacy statement/consent form can be found in Annex I. It is a generic template which needs to be tailored to each specific data processing activity. The reason is that the different data processing activities could have different purposes, different controllers, collect different categories of data, etc. Since such information is the core of every privacy statement, it should be adapted to the individual activity at hand. The information should be communicated in an understandable way to the volunteers. This means that if necessary, the privacy statement should be translated into different languages.

2.4. Usage of data not directly collected by the project partners or collected by them but for other purposes

There could be cases where the partners do not collect data directly from volunteers but wish to (1) re-use the data collected by them for other purposes or (2) re-use data provided by parties not member of the consortium, which has not been collected for research purposes in eVACUATE.
Both instances refer to the re-use of data collected for a different purpose. In general, in these cases the data subjects still need to be informed about the data processing. However, if the provision of such information would involve a disproportionate effort or would be impossible, especially where the data are re-used for historical or scientific research, such as in eVACUATE, then this provision could be derogated from. However, appropriate safeguards still need to be taken to prevent misuse or abuse of data.[2]

Case (1) could arise, for example, when one of the end-users in eVACUATE decides to re-use the recordings lawfully collected by them and stored in the course of the daily CCTV surveillance on their premises and to allow the other partners to use these recordings for research purposes in eVACUATE. One option is for the controller to anonymize the images permanently and irreversibly in such a way that they do not constitute personal data any longer and cannot be reversed, in which case the data protection framework would not apply if there is no risk of identifiability of the individuals recorded. However, if the data are not anonymized before the disclosure, then a new legal basis for the processing needs to be established as there would be a change of the original purpose of processing and disclosure to further parties. It is also advisable to notify the data protection authority of the intended change of purpose and disclosure of data to the project

[2] Article 11 (2) Directive 95/46/EC

partners. If the disclose would be allowed, both parties should sign the relevant agreement, delimiting the further usage of data and defining their responsibilities (see section 2.5 below).

Case (2) could arise if the partners wish to use pre-collected data by entities not part of the consortium and who collected the data for other purposes, e.g. law-enforcement authorities. The above legal discussion of case (1) applies to case (2) as well. The difference with case (1) is that the controller of the data, i.e. the one who owns the data, does not belong to the consortium. If he wishes to disclose unanonymized data to one or more partners of the consortium, first of all a legal basis for the disclosure and subsequent re-use of the data should be established. That is quite challenging as it would be difficult to motivate how the disclosure of personal data to a research project in which the controller does not participate would benefit the controller, e.g. be necessary for the fulfillment of his duties or be necessary for the purposes of the legitimate interests by the controller. In addition, the controller should again notify the relevant data protection authority of the change of purpose of the processing of the data.
If a legal basis is found and the data protection authority is notified and does not prohibit the processing, then again an agreement needs to be concluded with the parties receiving the data (see section 2.5 below). It should be very clear whether the partners of the consortium when receiving the data agree to become controllers, and thus amongst others have to notify their respective data protection commissions, or they receive the data as processors and process the data on behalf of the controller only.

2.5. Exchange of personal data between the eVACUATE partners

In principle, if one partner collects or obtains in another way personal data for research purposes in eVACUATE and wishes to share the data for research purposes with other partners in eVACUATE, an agreement needs to be concluded between them.

This would not be obligatory in the case where the data that is exchanged has been anonymized in such a way that there is no risk that real persons can be (re-)identified through this data and the anonymization is irreversible and permanent.
The case of AIA is a good example of anonymization. When ICCS handed over the original recordings to AIA, ICCS provided AIA with software which blurs the images of the individuals. According to the information provided by ICCS and AIA, this anonymization is permanent and irreversible. It is in principle up to the controller to decide whether the anonymization eliminates all risks of identifiability and therefore the data is to be treated as non-personal data. Such practices are welcome in eVACUATE as during the research phase it is not always necessary to work with personally identifiable information, unless

there is justification to the contrary. Thus, when for the purposes of research keeping the personal data in an identifiable form is not necessary, it is recommended to anonymize it. In addition, permanent blurring of images is an implementation of Privacy by Design.

In case the data are treated as personal data, then the controller should conclude an agreement with the partner receiving the data. The purpose of this agreement is to regulate the roles of each party (i.e. whether the receiving party will receive the data as a controller or processor) and the respective responsibilities of each party regarding data protection, including data security, and to delimit the usage of the data. A template was distributed to the partners in September 2014, see Annex II. The template, like the template for the privacy statement, needs to be adapted for each individual personal data exchange as the participating partners could be different; their relationship could be different, e.g. controller-to-controller or controller-processor; and the nature of personal data and object of exchange could differ. Once the agreement is adapted and properly filled out, it needs to be reviewed by the legal departments of the partners to check whether it is compliant with their national laws.

2.6. Data minimization

One of the principles of data protection is data minimization, which means collecting and further processing only the personal data which are necessary for the research purposes of eVACUATE. In practice, this means that when carrying out the demonstrations and tests, the partners should restrict the collection of data to what is necessary for their research. It is highly recommendable to anonymize the data, unless it is justified why personally identifiable information would be needed for the purposes of research. This is especially valid in the case of video footage, which contains images of individuals. As eVACUATE does not aim to develop technology for facial recognition, etc, it would seem disproportionate to store the footage without properly blurring the images. Therefore, anonymization is recommended.

2.7. Data storage and purpose limitation

The partners are reminded that they are supposed to delete the (personal) data as soon as it is not necessary any more for the purposes of research in eVACUATE. Thus, a reasonable storage time would be until the end of the project, unless the partners motivate why the data should be stored longer and the data subjects are informed of this when they provide their consent.

In addition, the partners have to ensure that the data they possess are not re-used for other purposes, e.g. disclosed to parties outside the project. Thus, they may use the data only for research purposes and as explained by them in the privacy information notice.

2.8. Rights of data subjects

When partners process personal data, they need to fully respect the rights of the data subjects, inform the data subjects of their rights and allow them to exercise these rights. These are (1) the right of information, e.g. whether data are being processed, by whom, for what purposes, etc, (2) the right of access to their data, e.g. provide copies of the data processed on the particular data subject, (3) right to rectification of the said data, (4) the right to objection, erasure and blocking. If the data subject wishes to withdraw his consent from the data processing, there should be mechanisms to do so. If someone requests the deletion of their data, the data should be deleted.

2.9. Data security and confidentiality

The current data protection legal framework, i.e. Article 17 of Directive 95/46/EC requires that the security of processing is guaranteed. Pursuant to that provision, the controller should ensure a level of security, which is commensurate with the risks represented by the processing and the nature of the data to be protected. It requires the controller to take the necessary organizational and technical measures to protect data, *amongst others*, from unlawful processing, accidental loss, destruction, etc. When the data are processed on behalf of the controller by a processor, the latter also has to implement such security measures. Normally, the obligations of the processor are regulated in the controller-processor agreement. Pursuant to Article 17 (3), the laws of the country in which the processor is established are also incumbent upon him. Thus, the data should be kept secure and confidential at all times.
In Article 30 of the General Data Protection Regulation, the requirement of security would apply also to processors, independent from the controller-processor agreement.

2.10. Notification to the Data Protection Authority

As a general rule, the controller should submit a notification to his national data protection authority (Article 18 (1) Directive 95/46/EC). Sometimes there are exemptions to this general rule, e.g. where the controller has appointed a data protection officer, who is responsible for the data processing (Article 18 (2) Directive 95/46/EC).[3] Depending on the

[3] This refers to a data protection officer appointed by or working for the controller of a certain data processing activity. For example, if one of the eVACUATE end-users becomes a controller for one of the validation demonstrations and this end-user has a data protection officer, then this data protection officer

type of processing and the established procedures by national data protection authority of the controller, sometimes the data processing activity is subject to prior authorization by the authority, while in other cases only a notification suffices. Thus, the controller is advised to check in his national law whether he is subject to the notification obligation and submit a notification, unless he is already covered by an existing one.

The General Data Protection Regulation proposes a modification of the current framework, expected to be adopted and enter into force end of 2015 or in 2016. However, these dates are speculative. If these proposed rules enter into force, then both controllers and processors would be obliged to keep proper documentation of the data processing operations under their responsibility. The documentation should contain similar information to the information provided by the controller to the data protection authorities when submitting a notification, e.g. name and contact details of the controller, the purposes of processing, the personal data to be processed and the affected individuals, etc (Article 28 Proposal for GDPR). They should be ready to present this documentation to the supervisory authority when requested to do so (Article 29 Proposal for GDPR). For certain data processing operations that present a higher risk (if indicated so by the results of the privacy impact assessment or if the activity falls within the scope of operations that need prior authorization as established by the relevant data protection authority), the prior checking and authorization of the national authority would be required (Article 34 Proposal for GDPR).

2.11. Local Specifications

The partners are reminded that the requirements discussed above derive from the EU level legal framework. Additional specifications and/or recommendations might apply as a matter of national legislation and/or guidelines from local data protection authorities, national court judgments, etc. Therefore, the legal departments of the partners who process personal data need to be involved in order to make sure all local requirements are satisfied. In which cases a partner is subject to the notification requirement is also to be checked by the respective partners.

Last but not least, there can be other requirements that do not stem from the personal data protection framework. For example, in the case of AIA, the partners who requested access to the recordings were invited to sign a separate Non-Disclosure Agreement (NDA) with AIA to commit the receiving partners not to further distribute the anonymized images as they are the property of AIA.

should be notified. Currently, this practice is not widely spread. However, when the proposed GDPR enters into force (in 2015 or 2016), more entities might be obliged to appoint data protection officers. In this case, the obligation to notify the DPA might not apply in all cases.

3. Cloud storage

In eVACUATE the (personal) data are processed through the SOFIA platform and this platform is stored in a Microsoft Azure cloud. This has been the case for the testing sessions in February/March 2015, where at the time of the writing of the deliverable it is planned not to process personal data. Later, for the final validation demonstrations, which are planned to take place on the end-user premises and during which personal data is highly likely to be processed, the data *will not be processed in the cloud and it will not leave the end-user premises*,as agreed within the consortium..

In case any personal data are processed in the Microsoft Azure cloud during eVACUATE, the partners should be aware that when they process personal data in the cloud, their obligations with regards to personal data remain. Cloud computing in itself poses additional data protection risks that should be paid careful attention to. These risks stem primarily from the fact that when personal data are stored in the cloud, their location is not permanent and it is not known how the data are moving across borders. This could be especially problematic when the data moves to countries outside the European Union, where personal data does not enjoy a high level of protection. There is a risk that the data might be accessed by unauthorized individuals or authorities (e.g. law enforcement authorities in third countries) and used for other purposes than the originally pre-defined ones, such as law-enforcement.[4]

If eVACUATE partners actually process personal data through the cloud, and if they commission the processing of data to the cloud provider, who will process the data as instructed by the respective partners, it is assumed that the eVACUATE partner(s) would be the controller(s) and the cloud provider – the processor. However, depending on the specific role of the cloud provider, the latter might be also a controller and thus have additional data protection responsibilities on its own. The applicable national law would be the one of the controller(s). Thus, the following recommendations should be taken into account by partners who intend to process personal data in the cloud so that they are compliant with the EU data protection framework:

- Transparency towards individuals whose data would be processed in the cloud and transparency of the cloud provider towards the cloud client;
- Purpose limitation of the data processing;
- Erasure of data as soon as they are not necessary any longer from different servers at different locations; storage media should be destroyed, demagnetised or otherwise erased, e.g. through overwriting;
- Contract on data security would need to be concluded, which would regulate the scope and duration of the service. It also needs to define where the data are

[4] Article 29 Working Party, "Opinion 05/2012 on Cloud Computing," Adopted on 1st July 2012.

located, how request for disclosure by any authorities should be handled; how the operations on personal data will be logged and audited, and how the partners in the cloud service will inform of changes to the services, data breach notification, security and confidentiality measures;

- Rights of data subjects should be guaranteed and the data subjects should have the opportunity to exercise all their rights under the EU Data Protection Framework;
- The cloud provider should grant portability of the personal data they process;
- Accountability of the service provider to the controller and of the controller to the respective data protection authorities and the data subjects should be given;
- When transfers to third countries are undertaken, the Article 29 Working Party has recommended the usage of standard contractual clauses – "Standard Contractual Clauses 2010/87/EU" as approved by Article 29 Working Party. Such clauses would also need to be concluded between the cloud provider and subcontractors of the cloud provider.[5]

4. Conclusion

The present deliverable sought to provide a step-by-step analysis of the procedures that the eVACUATE partners need to observe when working with personal data in the research phase of the project. These steps need to be considered for every individual processing of personal data. As the deliverable demonstrates, the procedures could take a certain time. Therefore, it is recommended that activities which involve personal data processing are planned well in advance in order to determine the responsibilities of the partners and the steps which each of them needs to take in order to comply with the applicable data protection framework.

[5] *Ibid*

Annex I
Privacy Statement/Consent Form

TITLE OF RESEARCH ACTIVITY

(Part of eVACUATE: "A holistic, scenario-independent, situation-awareness and guidance system for sustaining the Active Evacuation Route for large crowds," FP7-SEC-2012.4.2 -2, Grant Agreement 313161)

Please read and confirm your consent to participate in this interview by signing and dating this form.

1. I confirm that the purpose of **[the research activity]** and the collection of my personal data, including **[description of data to be collected]** has been explained to me and that I have had the opportunity to ask questions about the research and have had these answered satisfactorily.

2. I understand that my participation is voluntary, and that I am free to withdraw from **[research activity]** at any time without giving any reason and without any implications for my legal rights.

3. I allow the researcher to **[describe what the activity is, e.g. to record me, to use my mobile phone data, etc]**. I understand and agree that anonymized data may be used in presentations and publications, posters, brochures and internet material distributed to the public, stemming from the research but not in any way that might allow for identification of individual participants.

4. I understand that data will be kept secure and confidential at all times.

5. I have been informed of and I agree with the following:
   - The controller of the processing of my personal data is **[insert name of controller, their address and contact details].**
   - The personal data collected and processed, either by the controller **[or its processors – if applicable],** include **[categories of data]**.
   - The purpose of the collection of my personal data is **[describe purpose, in the framework of the eVACUATE project, insert link to website]**. My personal data will only be processed, used and be made available for research purposes **[e.g. on evacuation]** and related topics by the eVACUATE project partners.
   - I have the right to access the information collected and stored about me, as well as the right to have rectified the data which concerns me as long as such data are not anonymised. This right can be exercised by contacting **[insert name of controller and contact details]**.

- My personal data will be retained for maximum **[insert storage period]** and will only be used for research purposes. I understand and agree that my data may be used however anonymously during and after this term.

6. I agree to take part in **[insert research activity]** and with the information and processing of my personal data as explained above.

Name of respondent	Date	Signature
Name of project participant (if necessary	Date	Signature

Annex II

Controller – Processor Agreement

Template only

Name of controller – Name of processor/or other controller

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

Agreement

Between:

Name and address of controller, duly represented by _____ (name and function) and _____(name and function),

Hereinafter: the Controller,

And:

_____ (name and address of company), duly represented by _____(name and function) and _____(name and function),

Hereinafter: the Processor [or again controller],

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). They have agreed to participate in [research activity for which data processing is necessary] and the compilation of subsequent reports and related research in the framework of the research activities of the eVACUATE project;

[Name of institution] is a controller within the meaning of [Article in national law of the controller], implementing Directive 95/46/EC, for the personal data collected and processed in relation to [research activity] and used for research purposes;

The Processor agrees to collect, to process and/or to receive personal data on behalf of the controller for the above research purposes in accordance with the instructions of the controller and with the applicable data protection laws; [if it is a controller – processor relationship].

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 in the data protection law of the controller], 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 date (hereinafter Directive 95/46/EC).

["Name of research activity"] shall mean [description].

"Data Subjects" mean the volunteers who participate in [the activity in 1.2] or if not voluntary – describe who the Data Subject is.

The categories of personal data collected in the framework of the aforementioned activity are [list them].

Article 2 - Subject

The Agreement governs the processing of personal data undertaken by the project partners in the context of [research activity] in the framework of the eVACUATE project, a project funded by the European Commission under the FP 7 programme

(SEC – 2012.4.2-2). It regulates the roles, duties and responsibilities of the partners to this Agreement and involved in the data processing activity.

The Controller shall provide to the Processor the specifications and the instructions, by agreed forms, email and otherwise, for the processing of the Personal Data collected [describe how they are collected]. [if it is a controller – processor agreement].

Article 3 – Warranties and obligations of the Controller

The Controller agrees and warrants that throughout the duration of the Processing it will issue instructions to the Processor in accordance with the [data protection law to which they are subject], and any other applicable laws.

Article 4 – Warranties and obligations of the Processor [when it is a controller-processor agreement only].

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 [add/delete points according to national law of the controller]:

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 his processing of the Personal Data for the [research activity in eVACUATE] 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 will 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 of the stakeholders when requested to do so by the controller or by the data subject as well as after the work 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 issue subcontracts.

Article 5 – Term and Termination

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

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.

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. [if a controller-processor agreement].

Article 6 – Applicable law, Mediation and Jurisdiction

6.1. The laws of [choose applicable law, advisable law of controller] shall apply to this Agreement.

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 [country of Article 6.1.].

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

The Processor

_____ (name and function)

_____ (name and function)

The Controller

_____ (name and function)

_____ (name and function)

Annex III

Tentative data protection compliance template (V1) during trials and in real-life situations (As inspired by the ADDPRIV Project)[6]

Data protection requirement	Trial (AIA, STX, ASRS, METB)	Compliance level (Full, Partial, None)	Comment
Is the *purpose* of the processing specified?			Is the purpose clearly articulated and restricted?
Is the *controller* defined? Are there *processors* as well?			
Is there a *legal basis* for the processing?			Which legal basis was relied on?
If the legal basis is *consent*, have the data subjects been properly *informed*?			In an understandable language?
If the legal basis is *consent*, did the data subjects provide their *explicit and voluntary consent*?			
Has only the *minimum personal data* necessary been collected?			And the rest been deleted or anonymized.
Is the data processed only for the *specified purpose*?			Data not processed for incompatible purposes.
Is the data *deleted or completely anonymized* at the end of the project/trial?			
Is the data processed *accurate*?			Data from different sensors, e.g. RFID, EVAMAPP.
Is the *security* of data ensured?			
Is *access* to data properly controlled?			
If data are *exchanged* between partners, have relevant data exchange agreement been signed?			
Has the controller sent a *notification* to his DPA *where necessary*?			
Are the data subjects' rights respected?			Right to information, access to personal data, data rectification, blocking or erasure; object to processing, withdraw consent.
Have other (local) requirements been complied with?			E.g. additional NDA agreements?

[6] www.addpriv.eu