PUBLIC

D3.3 – Framework for Impact Assessment Against SoEL Requirements

Grant Agreement No.:740859
Project Acronym: ALADDIN
Project Title: Advanced hoListic Adverse Drone Detection, Identification Neutralisation
Date: 31h May 2018

Deliverable Identifier: D3.3 – Framework for Impact Assessment Against SoEL Requirements
Delivery Date: May 2018
Classification: PUBLIC
Editor(s): Deepan Sarma (VUB), Paul Quinn (VUB)
Document version: 1.0

Contract Start Date: 1st September 2017
Duration: 36 months
Project coordinator: Diginext (France)
Partners: CERTH (GRC), Fraunhofer IDMT (DEU), PIAP (POL), VUB (BEL), CS (FRA), IDS (ITA), SIRC (POL), MC2 (FRA), HGH (FRA), FADA (ESP), KEMEA (GRC), Acciona ACCI (ESP), MIF (FRA), Home Office CAST (GBR), PJ (PRT), MIPS (ITA), ADM (ESP).

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 740 859

Document Control

Title	3.1 – Data protection, Social, Ethical and Legal Frameworks	
Editors	Deepan Sarma	VUB
	Paul Quinn	VUB
Contributors		
Peer Reviewers	Luigia Nuzzo	IDS
	Manuel Garcia	FADA CATEC
Security Assessment	☒ passed ☐ rejected	
Format	Text - Ms Word	
Language	English-UK	
Work-Package	WP3	
Deliverable number	3.3	
Due Date of Delivery	31 May 2018	
Actual Date of Delivery	31 May 2018	
Dissemination Level	☒ Public ☐ Confidential (only Consortium members + EC) ☐ RESTREINT UE/EU RESTRICTED	
Rights	ALADDIN Consortium	
Date	31/05/2018	
Revision	None	
Version	1.0	
Edited by	Deepan Sarma (VUB)	
Status	☐ draft ☒ Consortium reviewed ☒ WP leader accepted ☒ Project coordinator accepted	

Revision History

Version	Date	Description and comments	Edited by
0.1	15/04/2018	Table of contents, framework of deliverable	Deepan (VUB)
0.2	11/05/2018	Initial draft	VUB
0.3	19/05/2018	Initial draft internally reviewed	VUB
0.4	25/05/2018	Revisions made based on internal review	VUB
0.5	28/05/2018	Revisions for project review (SAB, SELAB, reviewers)	DXT
0.6	30/05/2018	Revisions taking into account review	DXT
0.9	31/05/2018	Final version	VUB
1.0	31/05/2018	Version for submission	DXT

Executive summary

The project ALADDIN - Advanced hoListic Adverse Drone Detection, Identification and Neutralization is funded by the European Commission (EC) through the European H2020 research and innovation programme with Grant Agreement 740859.

This document, Deliverable 3.3 – Framework for Impact Assessment against SoEL Requirements, building on Deliverable 3.1, provides the ALADDIN impact assessment (IA) framework, against which project activities and outcomes will be evaluated. As the second deliverable of work package 3 (WP3), this document introduces the methodology to facilitate the observance of the SoEL (Social, Ethical, and Legal) principles throughout the course of the ALADDIN project, the heart of which is the impact assessment, tailored to the specificities of the project, which should be carried out for each element of the ALADDIN project.

The main elements of the methodology are the following: determination of activities which require an IA; parsing out the scope of the IA; assessment of impacts; evaluation and treatment of impacts; and monitoring and review. This deliverable represents the first part of the impact assessment. In order to ascertain whether the SoEL requirements identified in the deliverable (based upon the results of D3.1) will be met, a number of questions will be posed to each of the partners in the ALADDIN consortium in order to verify whether the measures taken within the design and implementation of the project will be sufficient to meet the requirements outlined. The application of the methodology this deliverable provides will be used to produce D3.4 and D3.5 – Impact Assessment Reports, in M18 and M36 respectively.

Contents

List of Tables

1. INTRODUCTION

1.1. Project Overview

The project ALADDIN - Advanced hoListic Adverse Drone Detection, Identification and Neutralization is funded by the European Commission (EC) through the European H2020 research and innovation programme with Grant Agreement 740859.

It spans 36 months and will follow an iterative and incremental development that implements a user-centred design process for the duration of the project. The project is split into two main iterations, each one being a complete development cycle composed of requirement collection, platform design, development, integration, and end-user testing and evaluation. The evaluative results of the first cycle will feed into the second, refining project aims and activities.

The main objective of the ALADDIN project is to study and develop a state-of-the-art, global, and extensible system to detect, localise, classify, and neutralise suspicious, and potentially multiple, light unmanned aerial vehicles (UAVs) over restricted areas. This system will be tailored to operational constraints (such as easiness of use and deployment, quality of detection, or safety) in order to deliver unprecedented tools for operational support, including investigations, and training.

ALADDIN will also assess relevant technologies, threat trends, regulations, and important issues such as the relevant societal, ethical, and legal (SoEL) frameworks. By doing so, it expects to develop new knowledge which will be made available to LEAs and infrastructure designers, constructors, and operators, through innovative curricula.

1.2. Purpose of Document

Work package 3 of the ALADDIN project foresees the execution of an impact assessment on the risks the project poses in terms of its data protection, social, ethical, and legal aspects. The key principles that must be met in each of these areas, were presented in deliverable D3.1. This ALADDIN impact assessment will occur in three phases: initial phase consisting in setting the framework (this deliverable), and then performing the impact assessment during each iteration of the

ALADDIN project: each one corresponding to Deliverable 3.4 and 3.5 respectively. This deliverable (D3.3) represents the first part of the impact assessment. In order to ascertain whether such requirements will be met, a number of questions will be posed to each of the partners in order to verify whether the measures taken within the design and implementation of the project will, given its particular context, be sufficient to meet the requirements outlined. The answers provided by the partners will be subsequently used in D3.4 and D3.5 to perform an analysis of whether the requirements have actually been met. Where necessary further steps will be suggested in order to ensure that any problems are addressed. Task 3.2 will accordingly involve intermittent reports at month 18 and 36 to ensure compliance.

1.3. Scope and Intended Audience

The intended audience of the document are the project stakeholders (European Commission DG HOME, ALADDIN Consortium executive members) and the project team (Consortium staff).

According to the preliminary security scrutiny in the DOA Part B (section 6.1), this deliverable is classified as PU = Public. The actual dissemination level has been confirmed as PU = Public by the Security Advisory Board (SAB) chaired by the Project Security Officer (PSO).

1.4. Structure of Document

This deliverable is divided into three parts. Section 1: Introduction, provides an overview of the ALADDIN project, and lays out the purpose of the document and its role as part of work package 3. Section 2: Methodology provides a detailed overview of the impact assessment process, including the motivation behind impact assessments, its methodology, and the role of this deliverable as part of the impact assessment process. Finally, section 3 provides a detailed look at the requirements determined in the previous deliverable (D3.1) concerning the three main categories of concern identified with a draft list of questions for each.

2. METHODOLOGY

2.1. Motivation for impact assessments

Impact assessments (IAs) are carried out to assess the consequences of activities. IAs help to identify different impacts of the activity. The subject of the impact depends on the type of the IA, e.g. environmental, social, economic, privacy, data protection, technology, etc. Impact assessments are carried out prior to the start of the activity (ideally at an early stage of the planning or designing); therefore it is appropriate to predict the potential benefits and adverse impacts. IAs help decision-makers find the best and most beneficial solutions.[1] As ALADDIN is an ambitious research and innovation project aiming to tackle organized criminal groups and terrorism using UAVs, the mapping of the potential impacts of the system is essential. To guarantee the legitimacy of the ALADDIN system, it should meet not only the technical requirements, but the legal and ethical standards (in particular those related to privacy, data protection and criminal law) as well. An impact assessment of ALADDIN on such values and requirements – described in Deliverable 3.1 – will identify the steps which should be taken in order to guarantee that the ALADDIN system is legally and ethically acceptable.

The elements of an impact assessment may vary, depending on the specific area in which it is conducted. However in most cases the steps of these impact assessments are similar:

- *Determining which activities require an impact assessment*
- *Defining the principles, key criteria and framework which will set the scope of the IA (this occurred in ALADDIN Deliverable D3.1)*

[1] E.g. environmental impact assessments originated from green movements in the 1960s (read more at: International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice <https://www.eianz.org/document/item/2744> [07/05/2016]) and social impact assessments (SIA) were developed in the 1980s. SIAs aim at ensuring that developments or planned interventions maximise the benefits and minimise the costs of those developments, including, especially, costs borne by the community (for more information read: The Interorganizational Committee on Guidelines and Principles for Social Impact Assessment: Guidelines and Principles for Social Impact Assessment <http://www.nmfs.noaa.gov/sfa/social_impact_guide.htm> [07/05/2016])

- *Assessment of the impacts of the activity (this deliverable will focus on the method of this assessment)*
- *Evaluation and treatment of the assessed impacts and decision-making based on the findings, general objectives (this will occur in ALADDIN Deliverables D3.4 & D3.5)*
- *Monitoring and review (this will occur in ALADDIN Deliverable D3.6 and D3.7)*

There is no one-size-fits all model for impact assessments. To work in practice, impact assessments must be scalable, flexible and applicable both for large organisations and for small SMEs.[2] The tools and methodologies can be tailored based on the scope of application. To remain effective, the model of impact assessments must be based on clear goals and principles. A prominent principle of IAs is proactivity: in order to be effective the impact assessment should be carried out prior to the start of the activity, at an early stage, while the most efficient moment to carry out an impact assessment is the final phase of the development.[3]

Treating and managing the elements of the ALADDIN project as risks is advantageous, as it facilitates the assessment and treatment of the different aspects of life in a homogeneous system. Risk management can be considered as a "systematic process of identifying and assessing risks, avoiding or mitigating them where possible, and then accepting and managing the remaining risks".[4] The advantage of the process is the establishment and application of a framework which lets risk-takers handle risks.[5] Risk assessment can be separated into three integral parts and one subsequent reactive part: identification, analysis, evaluation and treatment of risk.[6] With an assessment the decision-makers of ALADDIN will be able

[2] Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson and Orla Lynskey, 'Risk management in data protection' in 5 International Data Privacy Law 95,98 <http://idpl.oxfordjournals.org/content/5/2/95.full.pdf+html> [07/05/2016]
[3] Drawn from Paul Quinn et al, FORENSOR D2.2.
[4] Centre for Information Policy Leadership, 'The role of risk management in data protection – Paper 2 of the Project on Privacy Risk Framework and Risk-based Approach to Privacy' 2014, 5 <https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF> [07/05/2016]
[5] Dionne *op.cit.* 8
[6] ISO 31000:2009 2.18

to identify the future event, along with its possibility of occurrence, its impacts and handle them afterwards.[7]

In the context of Work Package 3 (SoEL aspects), those risks are related to the need to meet the legal and ethical requirements outlined in D3.1. The management of risks at the project level is described in D1.5 – Risk Management Plan V1 - and reported in the serial deliverables D1.6 to D1.10 (every 6 months) respectively. In the remainder of the document, the risks that are mentionned are related to SoEL aspects.

2.2. Impact Assessment Methodology

The primary aim of the ALADDIN impact assessment will be to assess potential impacts of the application of the ALADDIN project in terms of adherence to the legal and ethical principles outlined in Deliverable 3.1 – 'Data Protection, Social, Ethical and Legal Frameworks'. As described in Deliverable 3.1, the ALADDIN project may result in a risk to privacy, to the right to the protection of personal data, as well as pose challenges to the existing regime of telecommunication, aviation, and criminal law. Therefore, this deliverable will focus on the methodology of the assessment of these risks with special attention on their impacts.

The general steps of an Impact Assessment are described below together with how such a methodology will be used within work package 3 of the ALADDIN project.

ALADDIN Work package 3 implements each of the main elements of IAs. The overall design of the Impact Assessment is reflected in the work package structure itself. The scope and criteria are identified in Deliverable 3.1. Deliverables 3.3, 3.4 and 3.5 represent the actual processes of SoEL risk assessment (i.e. identification, analysis, evaluation and treatment). The 'treatment' of risk will occur as a response to the Impact Assessment reports and the periodic evaluations of the implementation of the impact assessment report (D3.6 and D3.7). The framework of SoEL risk management is a continuous cycle of operations which keep the risk assessment process appropriate and up-to-date. This process requires interaction with all the partners of the ALADDIN consortium. The three processes of identification, analysis

[7] Read more at: IEC 31010:2009 Risk management — Risk assessment techniques <https://www.iso.org/obp/ui/#iso:std:iec:31010:ed-1:v1:en> [07/05/2016]

and evaluation (extended with treatment), in the context of the ALADDIN project (WP3) are described below.

This document (D3.3) represents the first step in terms of an assessment of whether the *principles, key criteria and frameworks* described within D3.1 will be adhered to by the ALADDIN project. In order to do this, it will employ a questionnaire format whereby questions are addressed to each partner in terms of the efforts they have made or will make within the ALADDIN project to ensure that the principles etc. described in D3.1 will be adhered to. These questions will be based on a series of requirements that have been identified as a result of the research that was carried out in D3.1 (described below). Partners of the ALADDIN consortium should, to the best of their ability, answer the questions that have been addressed to them, indicating what action they have taken, and where such action has not been taken – to explain why not. The information will be collated and used to make an evaluation report in D3.4 and in D3.5. This report will highlight the efforts that have been made in meeting the criteria in question and where insufficient efforts have been made will call for further efforts (in consultation with the partners concerned).

The requirements upon which the questionnaires are based are described below. For the sake of clarity they have been split into three different sections. These relate to the main areas that were discussed in D3.1. They are:

1. *Requirements related to data protection*
2. *Requirements related to privacy in the broader sense*
3. *Requirements related to neutralization technologies*

This deliverable contains an indicative list of questions tailored to be answered when an element of the ALADDIN project is developed. This means any partner, who develops an element of ALADDIN, should carry out an IA by providing answers to the questionnaire and applying recommendations found as an outcome thereof, before the element (or the whole ALADDIN system) is deployed. The same activity should be carried out when the specific element changes in a way that such a change can have an impact on the data protection, social, ethical, and legal requirements. Please note that the questions listed in each section are for

informative purposes and subject to modification prior to being provided to the respective partner.

2.2.1. Identification

The term 'risk' is usually used in the context of an adverse consequence of an event; however it is not necessarily a negative term: *"risk is the probability of an event multiplied by some measure of its consequence."*[8] The definition implies that risk, as a neutral term, is a necessary aspect of life[9], its management a part of everyday life, an element of human life.[10] The purpose of perceiving events as risks is to assess them in a homogeneous system as equal occurrences.[11] The perception of risk is based on appropriate, comprehensive knowledge.

An important part of risk assessment is the articulation of a clear and consistent risk statement. The statement is an expression of a relationship between a real, existing event or fact and a potential, unrealised second event or fact.[12] Clear statements help in the identification of possible adverse effects. To help the identification, the assessor should consider the originating source of the risk as it can certify the validity of the risk statement, and it may be helpful in identifying additional risks as well. The last aspect of the process is the identification of the possible outcome and the nature of impact in order to describe the possible consequences.[13] The impact assessment contained in this report is split into three areas, correlating to risks in terms of privacy (in a broad sense), risks relating to data protection and risks relating the use of neutralization technologies. In each of these sections the main risks that

[8] Gary Yohe and Robin Leichenko, 'Chapter 2: Adopting a risk-based approach' (2010) New York City Panel on Climate Change 2010 Report, Annals of the New York Academy of Sciences 29,31 <http://onlinelibrary.wiley.com/doi/10.1111/j.1749-6632.2009.05310.x/epdf> [07/05/2016]
[9] Peter L. Bernstein, *Against the Gods: The Remarkable Story of Risk* (New York, John Wiley & Sons Inc 1998) referred by Jonathan B. Wiener, 'Precaution in a Multirisk World', in Dennis J. Paustenbach (ed.), *Human and Ecological Risk Assessment: Theory and Practice* (New York, John Wiley & Sons Inc, 2002), 1511 <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1923&context=faculty_scholarship> [07/05/2016]
[10] Centre for Information Policy Leadership, 'The role of risk management in data protection' *op.cit.* 4
[11] Jack A. Jones, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (2005) 9 <http://www.slideshare.net/Kabogo/an-introductiontofactoranalysisofinformationriskfair680> [07/05/2016]
[12] Microsoft Operations Framework (MOF) Risk Management Discipline, 'Identifying Risks in Operations' <https://technet.microsoft.com/en-us/library/cc535338.aspx> [07/05/2016]
[13] *Ibid.*

will need to be addressed within the context of SoEL aspects of the ALADDIN project will be tackled in terms of requirements vis-a-vis deliverable D3.1. Each of these requirements will represent an obstacle that the ALADDIN project will have to overcome or ensure that the benchmark requirements outlined in D3.1 are met within the context of ALADDIN as a project, and also by the deployment of any element created within that project.

To help the identification of risk the following type of questions will be posed and requested to be answered in D3.4 and in D3.5:

- What are the functionalities and the need for those functionalities as an element of the ALADDIN system?
- How does the functionalities of the ALADDIN system impact the principles of data protection?
- How does the functionalities of the ALADDIN system impact the principles of privacy?
- How does the functionalities of the ALADDIN system impact the principles of ethics?
- How does the functionalities of the ALADDIN system impact the principles of criminal law?

2.2.2. Analysis

ALADDIN is a multidisciplinary project with different work streams, operating within different specialisms and different forms of expertise. Consequently, it is not always possible that all partners that are involved in such projects understand the difference between abstract principles and requirements and the practical steps needed to secure them. Technical partners that are specialised in processes of technological development may not have a good understanding of legal principles and likewise, legal or ethical partners may not in realty have the ability to grasp by themselves what is needed in terms of practical and technical steps to actualize those principles. In order to address this issue this impact assessment uses a questionnaire-based approach whereby a series of questions relating to a particular requirement is given to each partner. In doing so the respective partner is able to describe what exactly has been or will be done to meet a particular requirement as it relates to them. It is only with such specialised feedback from each partner that one can accurately

assess whether the requirements that have been posed have been met. It must be noted that the set of posed requirements, as a benchmark, in itself will not guarantee the sufficient outcomes of the assessment.

During the analysis of the identified risks the following type of questions will be posed and requested to be answered in D3.4 regarding each risk:

- What is the likelihood of occurrence of this risk?
- What is the magnitude of the impact should this risk occur?

2.2.3. Evaluation and treatment

The answers provided by each partner, with their expertise in their specific context within the ALADDIN project, will allow an accurate evaluation of whether adequate steps have been taken in terms of meeting the requirements that relate to the risks identified in Deliverable 3.1. Such answers will be used to create an evaluation report (Deliverable 3.4) that will outline what steps have been taken and whether these are sufficient in order to meet the requirements that were outlined in Deliverable 3.1. Where the steps taken have not been sufficient the evaluation report will, through consultation with the relevant partners, outline what further steps may be necessary to ensure that the requirements that are identified are met. Subsequent to the first evaluation report, two periodic reports will be produced at months 18 and 36 (D3.4 and D3.5). These reports will follow the progress made by each partner and affirm that the efforts outlined in the responses to the questionnaire posed in the present deliverable and / or the suggested amendments in the evaluation report of Deliverable 3.1 have been / are being implemented. The following type of questions will help to carry out the review of the progress:

- What mitigating measures have been already implemented or will be implemented to minimise or avoid risks?
- Are there any residual risks left? If yes, are they justified?

3. REQUIREMENTS

3.1. Technical description of ALADDIN

Conducting an impact assessment requires strong cooperation between the parties, especially since high-end technology is applied (e.g. the ALADDIN system). To successfully describe the processing operations, the involvement of every party and their active participation is indispensable. The involved parties need to comprehend the main characteristics of the processing operations, the types of processed data, the expected outcomes and, in certain cases, the pursued legitimate interest.

The exchange of information between the parties can raise issues if the communication between the parties is not effective or frequent. The assessment can be conducted successfully only if every element of the envisaged processing operation and the procedure of the assessment is clear for the parties. To achieve this on the one hand the parties shall describe extensively the details and functioning of the processing operations, the elements which are connected to personal information in every possible way, and the reasoning behind the application of the respective element. On the other hand the legal expert of the ALADDIN project shall describe the reasoning behind the whole assessment, including its goals, length, parts, intermediate and final results, liabilities and possible consequences. Issues might also arise from the different goals and professional language the parties use. The parties need patience, openness and the intention to understand the point of view of the other party. The information-sharing, as the first part of the impact assessment of ALADDIN, will rely on an extensive questionnaire found in this deliverable and starts with a request of a technical description because of the aforementioned reasons.

The questions posed below are related to the technical aspects of the ALADDIN project. Partners should provide answers indicating where efforts have been made in the areas identified. Where this is not the case partners will be asked to provide advice based on their experience on what could be done within the context of the ALADDIN project to make this more likely.

Table 3.1 Questionnaire for technical description of ALADDIN components

Relevant to Partner(s)	*Required Input*
ALL PARTNERS	1. Provide a brief overview of the element of the ALADDIN device you are developing.
	Reason: A brief description for non-specialists helps to understand the system in its entirety and compare it with e.g. the SoEL requirements.
	Answer:
ALL PARTNERS	2. What are the functionalities of this element?
	Reason: The description of the functionality of an element would contribute to the understanding of its relevance.
	Answer:
ALL PARTNERS	3. What is the need for this element? Would it be possible to substitute it with a different element?
	Reason: The necessity of the element relating to other functionalities or system requirements clarifies its application.
	Answer:
ALL PARTNERS	4. What outcome (form of contribution to the whole system) is expected from the element?
	Reason: As part of the technical description the element should be positioned in the whole system in order to see its connection with other elements.
	Answer:
ALL PARTNERS	5. What are the costs of the deployment of the element? Is there an option for cheaper solution with same effectiveness?
	Reason: In order to increase the accessibility of the ALADDIN system, cost

	effectiveness should be taken into consideration.
	Answer:
ALL PARTNERS	6. Is there anything else that you would like to emphasize regarding the element?
	Reason: An additional question relating to the relevance of the element would minimize the chance of accidental ignorance.
	Answer:

3.2. Requirements Related to Data Protection

The General Data Protection Regulation (GDPR)[14] replaces the previous regime of European data protection law embodied in Directive 95/46/EC. As a Regulation rather than a Directive, it takes force in member states without being transposed into member state law, and takes effect as of May 25, 2018. The new data protection (DP) regime imposes stricter obligations on data controllers in order to increase the level of compliance with provisions of the GDPR, and does so through the levying of significant fines on those data controllers who do not demonstrate compliance. Its purpose is to *"protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"*[15]. One of the novelties will be the application of the risk-based approach in European data protection law on a larger scale. Reasons behind this innovative step are the pace of technological changes, the increasing number and size of data processing operations of public authorities and market actors or the natural development of different management techniques.[16] A calibrated risk-based approach is advantageous when handling large volume of processed personal data or in reducing the amount of privacy-invasive

[14] Regulation (EU) 2016/679, 27 April 2016
[15] Art. 1 (2) GDPR
[16] Roger Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer, Law and Security Review 123 <http://www.rogerclarke.com/DV/PIAHist-08.html> [07/05/2016]

tools.[17] The Article 29 Data Protection Working Party of the European Commission describes the risk-based approach as a bouquet of *"strengthened obligations result from processing which is considered as a risk for the persons concerned"*[18]. Although it is not an entirely new concept, as it is apparent in the Directive as well,[19] it has gained significantly more attention in the recent years,[20] during the development of several principles[21] in the GDPR.

In addition, Directive (EU) 2016/680, the Police and Criminal Justice Data Protection Directive (Criminal Directive), regulates data processing activities related to law enforcement, and is similar in substance to the GDPR, though as a Directive, rather than a Regulation, its applicability depends on the extent to which it is implemented into national law. As stated in D3.1, its scope is limited 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".[22]

As the group of end users of the ALADDIN system is likely to be comprised of actors whose activities may fall under either the Criminal Directive or the GDPR, it is important to take into consideration both data protection frameworks.

It is not clear the extent to which the ALADDIN project will process data that constitutes "personal data" according to its definition under the GDPR or the Criminal Directive. One of the motivations behind the impact assessment process is to determine if, and the extent to which, the ALADDIN project processes personal data.

---

[17] Centre for Information Policy Leadership, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' 2014 <https://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf> [07/05/2016]

[18] Article 29 Data Protection Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP218) 30 May 2014, 2 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> [07/05/2016]

[19] For example art. 8, 17 and 20 DPD

[20] For example: White paper of the World Economic Forum, 'Rethinking Personal Data: A New Lens for Strengthening Trust' May 2014, 17 <http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf> [07/05/2016]

[21] As the Working Party described in its statement on the role of a risk-based approach: art. 24 – Responsibility of the controller; art. 25 – Data protection by design and by default; art. 30 – Records of processing activities; art. 32 – Security of processing; art. 35 – Data Protection Impact Assessment; art. 40 – Codes of conduct; art. 42 – Certification.

[22] D3.1, "Data protection, Social, Ethical and Legal Frameworks", pg. 67.

As such, the European data protection framework should be taken into consideration at this stage. As per article 35, the GDPR requires data controller to conduct an assessment of the impact of the envisaged processing operations on the protection of personal data, when a type of processing is likely to result in a high risk for the rights and freedoms of the individual.[23] Article 27 of the Criminal Directive mandates the same.[24] The goal of the impact assessment is not only to foster compliance but also to identify and resolve potential adverse impacts.[25]

In the section below the requirements for the ALADDIN project (as derived from the analysis performed in Deliverable 3.1) are listed. These are the data protection requirements that ALADDIN must, as a project, meet. The questionnaire outlined below has been designed so as to discern whether adequate efforts have been made in meeting these requirements.

Requirements Related to Data Protection for the ALADDIN project

1. ***Data Processing of the ALADDIN project must have a legal basis***
2. ***ALADDIN project must ensure that the processing of personal data adheres to certain processing principles:***
    a. ***Processing must be fair, lawful, and transparent***
    b. ***The processing should have a specific, legitimate, and explicitly defined purpose. Furthermore, it should not be further processed in a way incompatible with those purposes.***
    c. ***The project should ensure that the processed personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed***

[23] Art. 35 (1) GDPR
[24] Art. 27 of the Criminal Directive.
[25] Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1 – Revision of existing PIAs (2011) 189 <http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf> [07/05/2016]

d. ***Measures must be taken to ensure that personal data is of satisfactory quality***

3. ***The ALADDIN project shall designate a (single) controller (or declare joint controllership), who has responsibility and control over the data processing operations.***
4. ***The ALADDIN project should proactively demonstrate compliance with the rules of data protection law.***
5. ***If there are determined to be data subjects, ALADDIN should inform data subjects about the main elements of ALADDIN project and the functioning of the device.***
6. ***The processing of personal data in ALADDIN should be transparent and foster trustworthiness.***
7. ***The ALADDIN project should ensure the security of data processing. Appropriate technical and organizational measures should be taken so as to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.***
8. ***The ALADDIN project shall maintain a detailed documentation regarding the processing activities.***
9. ***If there are determined to be data subjects, The ALADDIN project should respect and ensure the rights of the data subjects, provide sufficient information regarding the processing of any personal data by the ALADDIN system and notify data subjects about the deployment of the system.***
10. ***The ALADDIN project should meet additional legal requirements if the processed personal data will be used in cross-border cooperation of police or judicial authorities.***
11. ***Adequate protection must be provided when personal data, stored by ALADDIN, is processed in third countries.***

12. ***The deployment of the ALADDIN system should keep fair balance between private and public interests.***

13. ***In case the system is able to connect to databases of personal data (i.e. a UAV owner registry) the project must ensure that that such access is in accordance with all European data protection law.***

The questions posed below are related to aspects that have been identified as possibly contributing towards a potential ALADDIN being compliant with DP provisions in a number of situations. Partners should provide answers indicating where efforts have been made in the areas identified. Where this is not the case, partners will be asked to provide advice based on their experience on what could be done within the context of the ALADDIN project to make this more likely.

Table 3.2 Questionnaire on Data Protection for the ALADDIN project

Relevant to Partner(s)	***Required Input***
	Questions relating to the processed data
ALL PARTNERS	1. What types of data will be collected? Are the participants able to identify a natural person with the collected data (in itself or combined with other data, such as records from public databases)?
	Reason: If the data, recorded by the ALADDIN system, relates to an identified or identifiable natural person it becomes personal data, thus data protection law becomes applicable.
	Answer:
ALL PARTNERS INVOLVED IN THE USE CASE SCENARIOS	2. Will any personal data be collected during the use cases? If so, please describe.
	Answer:

ALL TECHNICAL PARTNERS	3. If processing personal data, do you process special categories of personal data (such as data concerning health)?
	Reason: specific types of data fall under the scope of stricter rules as their processing results in a higher risk to the rights and freedoms of the data subjects.
	Answer:
ALL TECHNICAL PARTNERS	4. If processing personal data, does the collected data meet the requirements of relevancy and accuracy? How do you ensure that data will remain accurate when disclosing it to third parties?
	Reason: the processed data should be relevant and accurate. The ALADDIN device should record only those types of personal data which are necessary to reach the goal of the processing, furthermore the processed data must be accurate and kept up to date.
	Answer:
ALL TECHNICAL PARTNERS	5. If processing personal data, would you be able to estimate the amount of processed data and the number of data subjects?
	Reason: larger number of processed personal data and data subjects would mean higher severity of impact in case of an unauthorized breach. Frequent recording would also affect the lifetime of the device.
	Answer:
	Questions relating to the data controller
ALL TECHNICAL PARTNERS AND DXT (COORDINATOR)	6. Who has responsibility for control of the processed personal data and who decides how can it be used? Who determines the means and details of the processing operations?
	Reason: The controller shall be held liable for the processing operation. In ALADDIN there are multiple parties with different expertise. The roles and responsibilities of controller and processor should be clarified, or joint controllership should be declared.

	Answer:
DXT (Coordinator)	7. If processing personal data, will a data processor be used? If yes please explain who and why – with special attention to the contact person, address, applied technology, and also attach existing contract.
	Reason: This question closely relates to the previous one. If some parties will act as processor, their roles should be described in terms of a contract. The data processing contract would ensure that data is processed only in accordance with the instructions of the controller.
	Answer:
DXT (Coordinator)	8. Would an organizational change (either in consortium or in single organisation) affect the processing of personal data in any sort of way?
	Reason – The personal data of the data subjects should be protected in the same way, regardless of the change of the participants in the project.
	Answer:
LEAs and End Users	9. Will any personal data be transferred to third countries? If yes, does the third country provide adequate protection? What is the legal ground of the transfer?
	Reason: the ALADDIN device might record data which will be necessary in any form of international cooperation (either police, aviation-related, or other forms).
	Answer:
ALL PARTNERS	10. How do you demonstrate compliance with data protection law?
	Reason: the GDPR requires the processor to proactively demonstrate compliance with data protection law.
	Answer:

	Questions relating to the data processing
TECHNICAL AND LEAs	11. Please introduce the functioning of the element of the ALADDIN system concerning data processing (for non-specialists, with special attention to the method of data processing and the tools to be used)!
	Reason: the systematic description of the envisaged data processing operation is an indispensable element of the impact assessment.
	Answer:
ALL PARTNERS	12. If processing personal data, how do you inform the data subjects about the intended data processing operation (what is the content and the used platform)? Please describe methods to be used to provide information to the data subjects.
	Reason: when personal data will be processed, the data subjects shall be notified prior to the processing. This means when individuals will stand or walk in front of the device, they must know that they might be recorded. The rights of the data subjects shall be guaranteed.
	Answer:
VUB, LEAs	13. If processing personal data, what is the legal ground and the purpose of the data processing? What are the expected benefits of the processing?
	Reason: the processing of personal data shall be based on a legitimate legal ground and shall have specified purposes.
	Answer:
ALL PARTNERS INVOLVED IN THE USE CASE SCENARIOS	14. If processing personal data, is the end date of the processing set (how long is the personal data retained)? What will happen with the personal data afterwards? Please answer from the perspective of research conducted during the ALADDIN project (use cases).
	Reason: the processing of personal shall have an end date. The rules of data minimization shall be taken into consideration.

	Answer:
Technical Partners	15. What Privacy Enhancing Technologies (PETs) are used?
	Reason: PET is a system of ICT measures protecting informational privacy by eliminating or minimising personal data, thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system. These include, inter alia, encryption or access controls.
	Answer:
TECHNICAL PARTNERS	16. How do you ensure the security of data? Please explain.
	Reason: appropriate technical and organisational measures should be applied to ensure the level of security, which is appropriate to the potential risk, such as: safeguards against interception of wireless transmission; secured control rooms and rooms where information is stored; trained staff; etc.
	Answer:
TECHNICAL AND LEA PARTNERS	17. If processing personal data, is the access to the personal data restricted? What are the rules of access (with special attention to its conditions, mode, and limits)?
	Reason: Relating to questions 5, 6 and 15 the details of processing operations should be clarified and documented (via e.g. logs, permissions).
	Answer:
TECHNICAL AND LEA PARTNERS	18. Are the processing operations documented? How are the records maintained? What are the rules of access to this documentation?
	Reason: The documentation will help in the identification of risks both for the controller and for the supervisory authority. Furthermore, the maintenance of the record of the activities could be advantageous in multiple cases.

	Answer:
	Questions relating to the data subjects
ALL PARTNERS INVOLVED IN USE CASE SCENARIOS	19. If processing personal data, how do you ensure that data subjects can exercise their rights? Please answer from the perspective of both research conducted during the ALADDIN project (i.e. use cases) and the use of the ALADDIN system in normal operating circumstances.
	Reason: a platform should be established where data subjects can practice their rights. Proper documentation should make it possible to find the information the data subject seeks.
	Answer:
ALL PARTNERS INVOLVED IN USE CASE SCENARIOS	20. How do you provide information to the data subject about the processing operation of ALADDIN? What is the content of the notice? Please answer from the perspective of both research conducted during the ALADDIN project and the use of the ALADDIN system in an ordinary operating circumstances.
	Reason: To guarantee fair processing, the provided information must be given in advance, in an understandable language.
	Answer:
ALL PARTNERS INVOLVED IN USE CASE SCENARIOS	21. If processing personal data, would the use of a layered notification system help the individuals to gain more information and understand the necessity of the ALADDIN system?
	Reason: For practical reasons short notices (with the possibility to access condensed and full notices as well) are considerable options in case of ALADDIN.
	Answer:
ALL PARTNERS	22. If processing personal data, are data subjects involved to the development phase? If yes, on what extent?

	Reason: The engagement of data subjects to the development phase could provide additional information regarding potential risks; furthermore, it could provide assurance of the outcome of the risk management and increase of the mutual understanding among data subjects and the ALADDIN project.
	Answer:
ALL PARTNERS	23. How do you plan to collect the views and feedbacks of stakeholders?
	Reason: There are multiple ways to collect feedback, e.g. online platform, questionnaires, meetings with representatives, etc.
	Answer:
	The role of personal data with respect to criminal law
LEAs and End Users	24. If processing personal data, does the party in question constitute: i. a public authority competent for 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, or **ii.** any other body or entity entrusted by Member State law to exercise public authority and public powers?
	Reason: Personal data processed by an actor falling into one of the above categories for specific purposes (stated below) is subject to the Criminal Directive rather than the GDPR.
	Answer:
LEAs and End Users	25. If processing personal data, is the purpose of the processing the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties?
	Reason: If the processing of personal data is for these purposes, and the processes is undertaken by the relevant party (see #25), then the processing is subject to the Criminal Regulation.

LEAs and End Users	26. If processing personal data, will the personal data processed by ALADDIN be used in cross-border cooperation by law enforcement authorities?
	Reason: Where personal data move across borders it may put at increased risk the ability of natural persons to exercise data protection rights to protect themselves from the unlawful use or disclosure of those data. There may be additional legal requirements that need to be met by the controller, as per the Criminal Directive and Chapter 6 of the Council Decision 2008/615/JHA.[26]
	Answer:
Technical Partners, LEAs and End Users	27. If processing personal data, how do you plan to differentiate between personal data of different categories of data subjects?
	Reason: The Criminal Directive posits that, where possible, distinctions should be made between different categories of data subjects such as, suspects; persons convicted of a criminal offence; victims; and data subjects who do not fall under any of these categories.[27]
	Answer:
LEAs and End Users	28. How do you make distinction between personal data based on their accuracy and reliability?
	Reason: Personal data should be distinguished in accordance with their degree of accuracy and reliability.
	Answer:
LEAs	29. How do you plan to keep fair balance between the competing private and public interests (e.g. public safety and right to access to personal data which is used as an evidence)?
	Reason: As the processing of personal data by police or national security authorities constitutes an interference with fundamental rights, its proportionality and necessity should be taken into consideration on a wide

[26] Directive (EU) 2016/680, Recital 94.
[27] Ibid., Recital 31.

	scale.
	Answer:
LEAs	30. Is it possible that, if it is absolutely necessary, the ALADDIN system will be used to process personal data without informing the data subjects? If yes, what safeguards or security measures would be applied?
	Reason: Covert surveillance interferes with the right to private life of the individual, however if adequate safeguards are applied it might be considered proportionate. It must be noted that if personal data will be processed by the controller without informing the data subject, he or she must be informed as soon as possible without inhibiting law enforcement activity.
	Answer:

3.3. Requirements Related to Privacy in the Broader Sense

In thinking of impacts in terms of privacy in a wider sense (i.e. outside the concept of data protection), it is necessary to look at the potential use for which the ALADDIN system may be employed. This is because the ALADDIN project is attempted to develop a sort of surveillance technology that, while not directed at individuals, may inadvertently pose a possible threat to the privacy of individuals. Even though the ALADDIN system is intended to address a threat to privacy and security (in the form of UAVs), through its monitoring and classification capabilities, it may pose a threat to privacy. Even in the context where such surveillance activities do not collect personally identifying information (the domain of data protection law), such activities may still exert psychological pressure upon individuals that may be capable of altering their behaviour.[28] This can be the case whether the monitoring and classification takes place in the context of public events, in urban environments, or in rural environments. However, such potential infringements on personal privacy are not always unacceptable. This includes potential uses in incidents relating to security

[28] See D3.1, "Data protection, Social, Ethical and Legal Frameworks", pg. 23.

for which ALADDIN is intended. Depending on the level of infringement of privacy that occurs and the intended use, the deployment of the ALADDIN system may be acceptable in most contexts.[29] The dual concepts of *proportionality* and *necessity* provides a useful way of judging when such infringements may be acceptable.

Article 8 of the European Convention of Human Rights (ECHR) recognizes this by offering a qualification to its general protection *inter alia* for measures that are intended to prevent crime.[30] This does not mean that the mere fact that where an 'ALADDIN like' device is used in order to detect or prevent crime, it will automatically be legal. This is because the use of such a device in a particular context would have to meet the conditions of being both described in law and being *necessary* and *proportional*. [31] These requirements have been elicited by the European Court of Human Rights in a number of cases.[32]

Necessity refers to the notion under most legal frameworks (in addition to the case law described by the European Court of Human Rights under article 8) that intrusions into individual privacy (including in public spaces) only occur when necessary and as described in law. However, the necessity of a particular context is not something the ALADDIN project will be able to influence directly – that is to the particular authority (airport authority, law enforcement authority) that decides to utilize the system (i.e. on the particular local conditions that may require the deployment of the system). As such, this concept is less relevant for the purpose of the impact assessment.

Proportionality refers to several inter-related concepts, but chief among these is the notion of balancing – that the rights of somebody may be infringed if the benefit sought by the act of infringement outweighs the harm caused by the infringement

[29] This is further discussed in D3.1, "Data protection, Social, Ethical and Legal Frameworks", pg. 23.
[30] For more on Article 8 ECHR see Ibid., pgs. 29-34.

[31] Case of PJ & H v United Kingdom (Application Number 0004478/98 2001) For more discussion of this case in the context of surveillance matters overall see: R. Macroy, Regulation, Enforcement and Governance in Environmental Law 2014). p297

[32] See for example: *Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V).17,* Case of S. and Marper v the United Kingdom (Applications nos. 30562/04 and 30566/04), Case of MALONE v. THE UNITED KINGDOM. (Application no. 8691/79), Case of Peck v the United Kingdom (Application No. 44857/98) For more discussion on the rulings of the ECtHR in the context of surveillance issues V. Kosta, *Fundamental Rights in EU Internal Market Legislation* 2015). P92

itself, in light of the importance of the competing values in question.[33] Such an idea is useful insofar as it allows one to assess whether certain actions can be justified or not.[34]

In the remainder of this section this requirement will be discussed, with the aim of identifying what exactly such requirements mean in concrete terms in the context of the ALADDIN project. In this first part of the ALADDIN impact assessment, it is necessary to gather information from other partners in order to assess how exactly the requirements identified are, and can be, realised through the work the ALADDIN project is undertaking.[35] With this requirement, the authors have accordingly attached a series of questions (see below) that will assist in the second part of the impact assessment (i.e. Deliverable 3.4). With each of these questions, reasoning will be provided in order to assist the relevant partners in answering the questions that have been directed to them.

Proportionality

Where ALADDIN as a research project is able to make a realistic difference to this question of proportionality, and therefore by extension legality, is by making the design of the device in question as 'privacy friendly' as possible. This need presents both an opportunity and an imperative to incorporate Privacy by Design (PbD) in the design and development of the ALADDIN prototype. This may be accomplished by designing the device in a way that it only audio-visually records activity after the detection of drones. Through doing so, the chances are higher that the use of the device in a particular circumstance will be deemed as being 'proportional'. A failure to do so would run the risk that the use of the ALADDIN system could be circumscribed to only the most particular of contexts (i.e., aerodrome surveillance, but not the monitoring of public events) and would reduce both its appeal and potential uptake.

In order to boost the potential proportionality of the ALADDIN system it should also be possible for the operating criteria of the system to be altered on a case by case

[33] Ibid.
[34] See D3.1, "Data protection, Social, Ethical and Legal Frameworks", pg 21§2.1.7.
[35] For more discussion of the method used in this impact assessment and the overall approach of Work package 3 please see the introductory section of this document.

basis. For example, if the 'classification' component draws upon databases (whether exclusive to law enforcement authorities or otherwise) to identify the owner of the UAV, it could involve the ability to customize which databases are drawn upon, or exclude the accessing of 3rd party databases altogether. The points below relate to these aspects and represent properties that, where possible, should be built into a potential ALADDIN device.

3.4. Requirements related to proportionality

1. ***The ALADDIN system should be as privacy friendly as possible.***
2. ***The ALADDIN system, where possible, should be able to adjust its level of privacy protection depending upon the circumstances in which it is to be deployed.***
3. ***Such 'adjustability' should take into account the potential quality of the data that may be captured through the sensors deployed and inter alia the possibility that they may directly identify particular individuals, including through the accessing of public or private databases.***
4. ***Any incidental capturing of data that might constitute personal data, if not related to the purpose of the system (i.e. UAV detection/neutralization), should be deleted as soon as possible.***
5. ***Captured data should be securely stored.***[36]
6. ***Data captured by sensors should only be accessible by authorized personnel.***
7. ***The ALADDIN system should be capable of being programmed to capture images, sound, and data connected to UAVs only.*** [37]
8. ***Users should be able to programme the ALADDIN system relatively easily so as to ensure that its use would be proportional for a particular situation.***
9. ***In the case the system is able to connect to databases of personal data (i.e. a UAV owner registry or criminal database), this feature must be customizable to***

[36] There is also overlap here with the requirements outlined concerning data protection, in particular concerning the principle that data be stored in a secure manner.
[37] There is also overlap here with the requirements outlined concerning data protection, in particular concerning the principle of data minimization.

fit the particular context in which the system is deployed.

The questions posed below are related to aspects that have been identified as possibly contributing towards the potential ALADDIN system in terms of making its use more likely to be 'proportional' in a number of situations. Partners should provide answers indicating where efforts have been made in the areas identified. Where this is not the case, partners will be asked to provide advice based on their experience on what could be done within the context of the ALADDIN project to make this more likely.

Table 3.3 Questionnaire on Privacy for the ALADDIN project

Relevant to Partners	Required Input
TECHNICAL PARTNERS	1. Will the sensors allow for personal data about individuals (faces, voices) to be captured? If so under what conditions?
	Reason: If sensors only process data related to UAVs or at least are precluded from processing data about individuals the use of the system will likely be deemed more proportional.
	Answer:
TECHNICAL PARTNERS	2. Can car number plates be identified? Can UAV number plates be detected?
	Reason: If car number plates are not visible the use of the device will likely be deemed more proportional.
	Answer:
TECHNICAL PARTNERS	3. If so under what conditions?
	Reason: If faces and vehicle (non-UAV) number plates can only be read under perfect or optimal conditions 'proportionality' in any given scenario will

	be more likely.
	Answer:
TECHNICAL PARTNERS	4. Is there a possibility to exclude the detection of individuals so that only UAVs are detected by the sensor algorithms?
	Reason: If only UAVs are detected, proportionality in a particular instance will be much more likely.
	Answer:
TECHNICAL PARTNERS	5. Do the sensors or the system continually record data or do they only record when a UAV is detected?
	Reason: If the data is regularly deleted, it reduces the chance of privacy risks as a result of malevolent action of others (i.e. that someone would be able to access and steal the data from the system in question).
	Answer:
TECHNICAL PARTNERS	6. If data about non-UAV information (car license plates, individuals, etc.) is logged, is such unused data deleted automatically?
	Reason: If the data is regularly deleted, it reduces the chance of privacy risks as a result of malevolent action of others (i.e. that someone would be able to access and steal the data from the system in question).
	Answer:
TEHCNICAL AND LEA PARTNERS	7. Who will have access to the data in question?
	Reason: The more people are likely to have access, the less likely that the use of the surveillance device will be 'proportional' in a particular instance, if personal data is recorded.
	Answer:
TCHNICAL PARTNERS	8. Can the features described in questions 1-7 be customizable on a case by case basis?
	Reason: Where such features can be programmed on a circumstantial basis to fit the particular circumstance in question (i.e. large public event vs. airport

	perimeter), proportionality, in a particular instance will be more likely.
	Answer:
TECHNICAL AND LEA PARTNERS	9. Can the algorithms for activation of UAV detection be altered simply (i.e. by the law enforcement authorities using the system)?
	Reason: The ease with which such adjustments can be made will be important in allowing the relevant authorities to adjust the system to make it more 'proportional' in a given circumstance (i.e. large public events vs. airport perimeter)
	Answer:
TECHNICAL AND LEA PARTNERS	10. If not, who has the ability to alter the algorithms for detection and activation?
	Reason: The ease with which such adjustments can be made will be important in allowing the relevant authorities or experts to adjust the device to make it more 'proportional' in a given circumstance.
	Answer:
TECHNICAL PARTNERS	11. Is the stored data secure from unintentional/malevolent access?
	Reason. An increased likelihood of theft of data will make the use of the device in question less proportional.
	Answer:
TECHNICAL PARTNERS	12. Will it be a simple matter to adapt the detection, localization, and classification algorithms of the ALADDIN system to specific circumstances or a difficult and time consuming task?
	Reason: The easier it is to adapt and modify detection, localization, and classification algorithms, the more likely that the ALADDIN system can be adapted so as to be appropriate for a particular circumstance and thus be 'proportional', in the case it logs personal data.
	Answer:
TECHNICAL PARTNERS	13. Will the alteration of the detection, localization, and classification algorithms require prolonged contact between the relevant end users

	and technical staff?
	Reason: the more difficult the alteration of algorithms are, the less likely that a surveillance device will be able to be altered to be 'proportional' for a particular circumstance and thus be 'proportional', in the case it logs personal data.
	Answer:
TECHNICAL PARTNERS	14. Will the alteration of detection, localization, and classification algorithms be expensive (in terms of monetary value)?
	Reason: the more difficult the alteration of detection algorithms are, the less likely that a surveillance device will be able to be altered to be 'proportional' for a particular circumstance and thus be 'proportional', assuming the system stores personal data.
	Answer:
TECHNICAL PARTNERS	15. Will those performing alteration of the technical algorithm (whether detection, localization, or classification) have to be familiar with the deployment site in question?
	Reason: the more difficult the alteration of algorithms are, the less likely that a surveillance device will be able to be altered to be 'proportional' for a particular circumstance and thus be 'proportional'.
	Answer:

3.5. Requirements related to neutralization technology

The aim of the ALADDIN project is to develop a system that will be capable of detecting, localizing, classifying, and neutralizing suspicious UAVs over restricted areas. In order to be able to deploy the system in the contexts for which it was designed, it will make use of various technologies to deliver its functionalities. While the classification and detection technologies will need to pay particular attention to privacy and data protection law, requirements linked to this area (neutralisation) will be particularly important for the functionalities of the system related to the

neutralization of UAVS, regardless of the ultimate means by which this is achieved. This is because any attempt to neutralize target UAVs will necessarily interfere with the functionalities of movable private property -- an electronic device that is regulated by a host of regulations, including domestic aviation and telecommunication law. As such, such requirements may relate to the means of neutralization in several ways, including:

1. The authorization of the means of neutralization in question.
2. The laws to which the particular means of neutralization is subject.
3. The context in which the particular means of neutralization takes place.
4. The use of force in a particular means of neutralization.

Deliverable 3.1 discussed examples of a number of rules and principles that apply to the interference with the functionalities of an aerial vehicle constituting private property not only in the context of criminal law, but also aviation and telecommunications law in particular. It will be necessary for those involved in the design of the ALADDIN system to be aware of these principles in order to, to as great an extent as possible, ensure that all the functionalities of the anti-UAV system will be capable of being deployed to as wide a user base as possible in its target markets.

The role of the ALADDIN impact assessment is to take such general principles of criminal, aviation, and telecommunications law that apply more specifically to the ALADDIN context. As with other sections of this impact assessment, the requirements in question will be confirmed and verified by posing questions to each partner concerning issues that are relevant to them.

Requirements related to the use of neutralization technologies

1. ***If the neutralization means used by ALADDIN constitutes a use of force, it should only be used where deployment has been approved correctly as prescribed by the law.***

2. ***If use of force is employed, it must be reasonable and proportionate (the degree of force used must be the minimum required in the circumstances to achieve the lawful objective)***
3. ***Any neutralization means that interferes with telecommunications signals should only be used where deployment have been approved correctly as prescribed by law.***

The questions posed below are related to the requirements identified above. They represent areas where clarification may be needed in order to ascertain whether these requirements have been met. Each partner should fill in the questions that are relevant to them. The information will be used in the second part of this impact assessment to ascertain where the requirements stated above have been met and, where this is not the case, where further action may be necessary.

Table 3.4 Questionnaire on Neutralization technologies for the ALADDIN project

Relevant to Partner	Required Input
Technical Partners, LEAs and End Users	1. How are UAVs classified? Are they classified based on whether the UAV is being used in the commission of a crime?
	Reason: Whether the targeted UAV is being used in the commission of a crime or not may have ramifications in terms of the recourse that may be available. For instance, the legality of the use of force that can be employed when the UAV is being used in the commission of a crime may differ from when it is not, or when it is being used in the commission of a civil wrong, depending on the jurisdiction.
	Answer:

Technical Partners	2. What are the means of neutralization that your element of the ALADDIN system concerns?
	Reason: The legality of the means of neutralization may be highly dependent on the technology chosen.
	Answer:
Technical Partners, LEAs and End Users, VUB	3. Does your element make use of means to neutralize UAVs that could be considered a use of force?
	Reason: Employment of the use of force against targeted UAVs may trigger additional legal requirements that are highly contextual and may be jurisdiction-dependent.
	Answer:
Technical Partners, LEAs and End Users	4. Under what circumstances are the means to neutralize UAVs authorized? Does it require the consent of a third-party?
	Reason: Jurisdictions may require state authorities to be explicitly authorized by law in order to employ neutralization measures against UAVs. Knowing the existence of such requirements is crucial in determining the viability of this component of the system.
	Answer:
TECHNICAL PARTNERS	5. Does the ALADDIN system offer a choice of means by which the targeted UAV can be neutralized? Does the ultimate decision to choose a particular neutralization method lie with the user?
	Reason: Allowing a choice of means to be used would allow end users to tailor the use of the system to the particular circumstances, which is crucial if the means of neutralization is considered a use of force.
	Answer:
Technical Partners	6. Relating to the previous question, are there algorithms that determine what means of neutralization to employ?

	Reason: Whether the determination over what kind of neutralization means to be employed is made by end users or determined through algorithms may have significance with respect to the legality of the component.
	Answer:
TECHNICAL PARTNERS	7. Can the neutralization component of the ALADDIN system be customizable on a case-by-case basis?
	Reason: Where such features can be programmed on a contextual basis to fit the particular circumstance in question, the proportionality of its use in a particular instance may be more likely.
	Answer:
TECHNICAL PARTNERS	8. Can the means for the activation of the neutralization component be altered simply?
	Reason: The ease with which such adjustments can be made will be important in allowing LEAs to adjust the device to make it more 'proportional' in a given circumstance.
	Answer:
LEAs and End Users and VUB	9. Are there laws authorizing the use of neutralization measures against UAVs in your jurisdiction? Are they based upon the UAV being connected to the commission of a crime, or could it include civil wrongs? (i.e. trespassing in certain jurisdictions)
	Reason: The use of neutralization measures against targeted UAVs may require statutory authorization, particularly when employed by state authorities. Whether a statutory framework exists is crucial in determining the legality of the use of neutralization measures.
	Answer:
LEAs and End Users and VUB	10. What are the procedures in your jurisdiction for approving the use of neutralization measures?
	Reason: Many jurisdictions may require neutralization measures to be

	approved by a respective authority in order to be employed. The existence, or lack thereof, of an approval mechanism may be crucial in determining the viability of its use, particularly by LEAs.
	Answer: