SYnergy of integrated Sensors and Technologies for urban sEcured environMent

D10.2

Baseline Knowledge report on the LESA frameworks

30 April 2020 **V3.0**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 787128

Project title	SYnergy of integrated Sensors and Technologies for urban sEcured environment
Project acronym	SYSTEM
Project number	787128
Start date of the project	1st September, 2018
Duration	42 months
Topic	SEC-10-FCT-2017. Integration of detection capabilities and data fusion with utility providers' network

Deliverable number	D10.2
Deliverable title	BASELINE REPORT ON THE LESA FRAMEWORK OF THE SYSTEM PROJECT
Leading partner	VUB
Partners contributing	//
WP of reference	WP10
Title of the WP of reference	LEGAL AND ETHICS MANAGEMENT
Task of reference	T10.2
Title of the task of reference	Participatory risk review and mitigation strategy
Deliverable type	Report
Dissemination level	PUBLIC
Due date	M20 – April 2020

Keywords	Ethics; Social Acceptance; Baseline; Regulatory; Privacy; Data Protection; Surveillance.
Abstract	This activity constitutes the second step of Impact Assessment outlined in work package 10. Specifically, the deliverable introduces the methodology, recalls the main legal and ethical considerations (developed in 10.1 and 10.8) to be taken into account, and provides a series of questions addressed to SYSTEM partners. Subsequently, as a third step in the Impact assessment, the answers to the questions will be analysed by the WP leader VUB and provide the basis for the WP10 risk reviews. In short, having outlined the relevant Legal Ethical and Social issues (LESA framework) in D10.1 and in D10.8, the present deliverable assesses the impacts of SYSTEM project activities on the LESA framework.
Editor	Sergi Vazquez Maymir, Eugenio Mantovani and Paul de Hert (VUB)

Contributors	//
Reviewers	Galya Toteva Terzieva (ISEMi), Simona Cavallini, Lorenzo Di Matteo (FORMIT)
Submission date of the draft to reviewers	20/03/2020
Submission date of the draft to the SAB (if required)	n.a.

Register of document versions

Partner acronym	Version number	Date	Suggested relevant changes	Notes
VUB	V1.0	20/12/2019	First Draft	Determined structure of the deliverable; Writing of the core text of the document
VUB	V.1.1	15/0/2020	Second Draft	Designed the structure questionnaire; Text editing.
VUB	V1.2	22/01/2020	Third Draft	Text editing; Refinement of LESA framework; Identification of target groups.
VUB	V1.3	10/02/2020	Fourth Draft	Text editing; Refinement of questions; Selection of questions per groups.
VUB	V1.4	20/02//2020	Fifth Draft	Text editing; Modified nomenclature of the Deliverable(s)); Format refinement; Refinement of questions formulation; Other.
VUB	V1.5	06/03/2020	Sixth Draft	Refinement of questions formulation; Format refinement; Checked spelling and grammar.
VUB	V1.6	19/03/2020	Seventh Draft	Revision of the text; Checked spelling and grammar; Instructions for partners introduced.
FORMIT	V2.0	24/03/2020		Request of minor adjustments/comments.
ISEMI	V2.1	24/03/2020		Request of minor adjustments/comments.
VUB	V2.2	04/05/2020		Integration of proposed adjustments (also addressing comments)
FORMIT	V2.2	21/04/2020	Quality check	Text editing

FORMIT	V3.0	30/04/2020	Final version	It was finalised during a period with a project amendment process open. Some minor changes (e.g. numbering of connected deliverables) will be required in case of approval of the amendment.
FORMIT	V3.0	28/08/2020	Final Version	Numbering of connected deliverables and other minor changes done according to the new version of the DoA (resulting from the amendment approved on 12/08/2020).

Every information is updated to the date of issue of this document

This document is composed by 44 pages

Table of Contents

List of Figures

List of Tables

List of acronyms and abbreviations

CA	Consortium Agreement
DoA	Description of Action
EB	Executive Board
EC	European Commission *or* Electrical Conductivity
ES	Exploitation Strategy
GA	Grant Agreement
LEA	Law Enforcing Agency
SME	Small and Medium Enterprise
LESA framework	Legal Ethical and Social issues and frameworks
ECtHR	European Court of Human Rights
DPLIAB	Data protection Laboratory on Impact assessment Brussels

EXECUTIVE SUMMARY

The present deliverable poses to SYSTEM project partner a series of questions designed to assess the impacts and risks of SYSTEM research activities and of the SYSTEM technology against the **Legal Ethical and Social issues and frameworks (LESA framework)** discussed and presented in D10.1 and D10.8.

The questionnaire is divided in the following six sections :

1) The area of technical description of SYSTEM.
2) The area of privacy.
3) The area of data protection.
4) The area of ethics and societal aspects
5) The area of LEAs' use of SYSTEM.
6) The area of collection and use of criminal evidence in the context of SYSTEM

For each area, a series of questions are formulated to the partners of the SYSTEM consortium. Given the role and expertise of each partners, the questions are addressed to specific groups of partners divided into four groups and listed in section 5 of this document "*Mobilising the LESA Framework via a Questionnaire: Instructions for partners*".

The nominated partners are requested to answer freely and in detail the questions and to report them to Sergi.vazquez.maymir@vub.be by the deadline of **15.04.2020**.

Subsequently, the answers will be analysed and systematised in a risk table.

The analysis of the risk table will result in a series of recommendation, in the generation of new questions and/or in the expansion of the LESA framework, should the answers highlight that new areas of legal ethical and social interest need to be taken into account.

1 MAIN ELEMENTS OF THIS DELIVERABLE

1.1. INPUT FROM OTHER WPS AND RELATION WITH OTHER SYSTEM DELIVERABLES

The present deliverable builds upon the findings outlined in the legal, ethical and societal frameworks introduced in deliverable *D10.1 Baseline Report on Legal aspects of SYSTEM* and *D10.8 Baseline Report on Ethical and Social* Acceptance aspects of SYSTEM. The answers to the questions contained in this deliverable will be analysed by the WP leader VUB and provide the basis for the regular WP10 legal, ethical and social acceptance risk reviews Reports (D10.3) and ultimately the Guidelines for deployment of SYSTEM (D10.7).

The deliverable is relevant for the organisation of tests and demonstrations in non-controlled environments under WP8.

1.2. REFERENCE DOCUMENTS

In order to set a framework in matter of a conflict between the Project Operational and Management Plan (D12.1) and other documents such as the Description of Actions (DoA) or the Grant Agreement, the following hierarchy will be applied:

1. Grant Agreement (GA);
2. Consortium Agreement (CA);
3. The Project Operational and Management Plan (D12.1).

The hierarchy related to the documents above implies that the latter document needs to be consistent with the former. In case of issues, this hierarchy of documents is mandatory.

1.3. PURPOSE OF THE DOCUMENT

This activity constitutes the second step of Impact Assessment outlined in work package 10. Specifically, the deliverable distils the main legal and ethical considerations (developed in 10.1 and 10.8) to be taken into account and provides a series of questions addressed to SYSTEM partners. The purpose is to draw out what measures the partners have taken or are taking to address the concerns or risks to the legal, ethical and social acceptance frameworks. Subsequently, the answers to the questions will be analysed by the WP leader VUB and included in WP10 legal, ethical and social acceptance risk review (D10.3).

1.4. STRUCTURE OF THE DOCUMENT

The document is structured in the following way:

1. **Introduction**
2. **Impact assessment methodology**: Description of the method followed in SYSTEM's impact assessment.
3. **Consolidated SYSTEM LESA Framework**: a schematic overview of the legal ethical and societal aspects that conform SYSTEM's LESA Framework.
4. **Mobilizing the LESA framework via the questionnaire:** instructions and guidance for the partners regarding the filling of the questionnaire.
5. **The Questionnaire**

2 INTRODUCTION

In general, impact assessment (IA) is an evaluation technique used to analyse the possible consequences of an initiative for a relevant societal concern(s), with a view to support an informed decision on whether to deploy the initiative and/or under what conditions.[1] As SYSTEM aims to take a significant step forward in deploying or carrying out research on urban integrated sensors and technologies, the mapping of their potential impacts is essential. Work package 10 of the SYSTEM project foresees the execution of an impact assessment of the risks the project poses in terms of Legal, in particular, Personal Data Protection, Privacy, Ethical and societal matters (LESA framework).

Conducting an impact assessment requires cooperation between the parties to describe the activities, in particular the data processing operations, the types of processed data, the pursued legitimate interest and so on and so forth. For this reason, partners in projects are asked to explain in layman terms the details and functioning of the technology, including the processing operations, the data flows, and the reasoning behind the implementation of the technology. The layman description is important to enable legal experts to assess the relevant risks, impacts and propose appropriate mitigating measures. To guarantee the validity of the SYSTEM solutions, they should meet not only the technical requirements, but the legal and ethical standards (in particular those related to privacy, data protection, non-discrimination and criminal law) as well.

The concerns and risk areas raised by the SYSTEM project and technology were outlined in the legal, ethical and societal frameworks introduced in deliverable *D10.1 Baseline Report on Legal aspects of SYSTEM* and *D10.8 Baseline Report on Ethical and Social* Acceptance aspects of SYSTEM. With this deliverable, the task leader activates the principles enshrined in the LESA framework by means of questions, addressed to each of the partners and seeking to collect to assess how partners are coping with the areas of risks to the legal, ethical and social acceptance frameworks. The answers provided by the partners will be subsequently used to carry out Risk Review Reports (D10.3) and ultimately the Guidelines for deployment of SYSTEM (D10.7).

The questionnaire is divided into the following six areas:

1) The area of technical description of SYSTEM.
2) The area of privacy.
3) The area of data protection.
4) The area of ethics and societal aspects
5) The area of LEAs' use of SYSTEM.
6) The area of collection and use of criminal evidence in the context of SYSTEM.

For each area, a series of questions are formulated to the partners of the SYSTEM consortium. Given the role and expertise of each partners, the questions are addressed to specific groups of partners divided as follows:
GROUP 1: DATA FUSION AND ALGHORITHMIC DEVELOPMENT.
GROUP 2: SENSOR TECHNOLOGIES.
GROUP 3: LAW ENFORCEMENT AUTHORITIES.

[1] Policy brief #2 on methods for data protection impact assessment (2019);< https://lsts.research.vub.be/en/policy-brief-d.pia.lab >

GROUP 4: LOCAL PUBLIC INFRASTRUCTURE OPERATORS/ENTITIES.

The members of each group are listed in section 5 of this document *"Mobilising the LESA Framework via a Questionnaire: Instructions for partners"*.

3 IMPACT ASSESSMENT METHODOLOGY

Impact assessment is a risk mitigation process[2]. 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."*[3] The definition implies that risk, as a neutral term, is an essential element of human life,[4] and its management is part of the human existence.[5] The purpose of perceiving events as risks is to assess them in a homogeneous system as equal occurrences.[6] Everything is comprehensible as a risk, however inappropriate interpretation results different perceptions of the event: ideally the event will become a risk, otherwise it might result uncertain or ignorant perception.[7] The perception of risk is based on appropriate, comprehensive knowledge.

There is no one-size-fits all model for impact assessments. To work in practice, impact assessments must be scalable and flexible. In the case of SYSTEM, the assessment involves decision makers, municipalities, law enforcement authorities well as large and small private organisations. SYSTEM impact assessment is inspired by the method developed by VUB's Data protection impact assessment laboratory of Brussels (DPLIAB)[8] and consists of the following steps:

Phase I: Preparation of an impact assessment: Determining which activities require an impact assessment:		***Related Deliverable in SYSTEM***
1	*Screening:* initial description of the research activities carried by the project including a preliminary risk appraisal.	*SYSTEM's description of action.*
2	*Scooping:* definition of the principles, key criteria and framework setting the scope of the IA and identification of the societal concern, stakeholders affected.	D10.1 and D10.8 (The Baselines)
Phase II: Assessment		
3	Description: systematic description of the envisaged research activities, including: - Contextual description of the envisaged research activities, particularly: nature, scope, context, purposes, the legitimate interest of the stakeholders involved (data subjects, controllers, processors, third parties and public	*D10.2 Baseline Report on the LESA Framework*

[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

[3] 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]

[4] 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]

[5] Centre for Information Policy Leadership, 'The role of risk management in data protection' *op.cit.* 4

[6] Jack A. Jones, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (2005) 9 <http://www.slideshare.net/Kabogo/an-introductiontofactoranalysisofinformationriskfair680> [07/05/2016]

[7] Paul Slovic and Elke U. Weber, 'Perception of Risk Posed by Extreme Events' (2002) 16 <https://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf> [07/05/2016]

[8] Policy brief #2 on methods for data protection impact assessment (2019);< https://lsts.research.vub.be/en/policy-brief-d.pia.lab >

	authorities); - Technical description in particular of data flows (how algorithms work, where data is kept, transferred, etc); - Consultation with data subjects or the public with due respect for legitimate secrecy (i.e. the 'protection of commercial or public interests or the security of processing operations') (Article 35(9) of the GDPR). Appraisal of impact: identification of impacts. Assessment of the impacts of the activity.	
Phase III: Evaluation and treatment of the assessed impacts and decision-making based on the findings, general objectives		
6	*Recommendations:* the assessment process is concluded with a list of recommended measures. It is envisaged that these recommendations will: i. address the risks, 'including safeguards, security measures and mechanisms to ensure the protection of personal data', and ii. ensure compliance with the Regulation, 'taking into account the rights and legitimate interests of data subjects and other persons concerned' (Article 35(7)(d)).	*D10.3 Risk Reports* *D10.7: Guidelines for deployment of the SYSTEM technologies*
Phase IV: Ongoing steps Monitoring and review		
7	*Prior consultation with a supervisory authority*: if the assessment demonstrates a serious risk that would remain even after the data controller implemented the recommendations stemming from the assessment process, the data controller is obliged to refer to supervisory national authority for consultation, prior to the start of the personal data processing and in accordance with a prescribed procedure (Article 36 of the GDPR). Review: This review can therefore occur merely after a certain period of time for monitoring purposes, or when there is a change that renders the previous assessment obsolete (partially or totally).	*D10.3 Risk Reports*
Phase V: Revisiting		
9.	Revisiting: This step a decision is made as to whether to conduct the process again, entirely or in part. This step can occur every time the envisaged initiative is modified (before or after its deployment) or every time the context in which it is going to be deployed, or already has been deployed, changes. This step also ensures the continuity of the assessment process.	*D10.3 Risk Reports*

Table 1 - Data Protection Impact Assessment Phases

4 CONSOLIDATED SYSTEM'S LESA FRAMEWORK

As described in the previous section, the aim of the SYSTEM impact assessment is to identify, describe, and address impacts and risks of SYSTEM technological solutions to the legal, ethical and societal (LESA) framework, which we call LESA framework.

The LESA framework is the outcome of two deliverables: Deliverable 10.1 'Report on the Legal Framework of SYSTEM' and Deliverable 10.8 "Report on the Ethical and Societal aspects of SYSTEM".

This document distils the legal, ethical and societal frameworks that SYSTEM mobilises into "areas"; each area contains a series of conditions that SYSTEM project partners should take into consideration. If you are interested in the arguments that support the dentification of these areas, please refer to D.10.1 and D.10.8, just mentioned. They are available in the project repository.

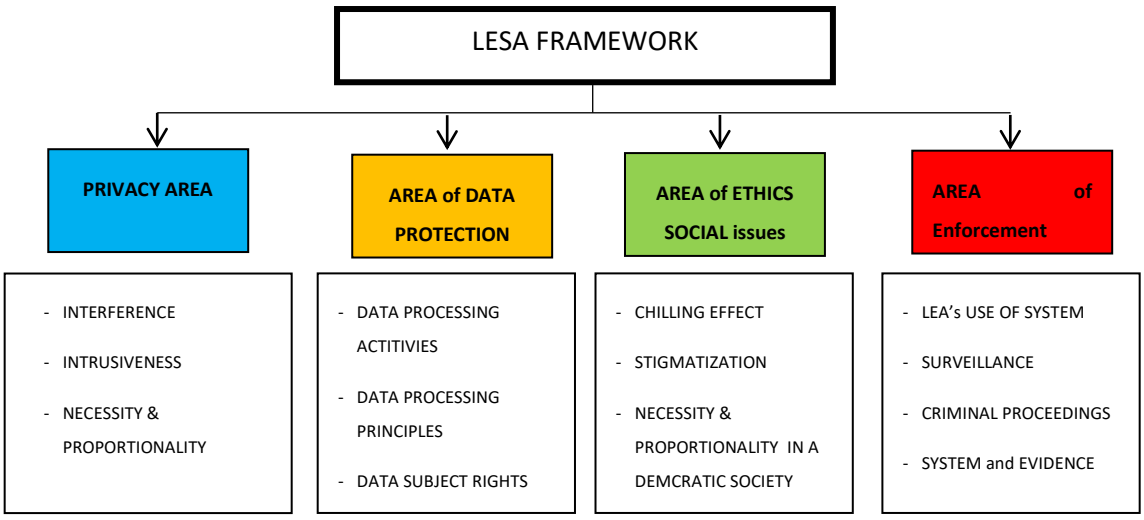

Figure 1 - LESA Framework Chart

The framework conditions summary:

CONDITIONS ON THE RIGHT TO PRIVACY	
Interference with privacy	The technologies within SYSTEM present different levels of interference with the right to privacy when dealt individually and as a unit. Thus they require both an individual and a joint assessment.
SYSTEM technological	**Sewage monitoring:** Sewage monitoring systems create interference with the right to privacy. Sewage monitoring becomes more intrusive as devices get nearer to residential buildings, for instance in city suburbs. The legitimacy of such interference will depend on a series of factors to be assessed on a case

solutions	by case basis (e.g. legal framework enabling from such interference to occur.)
	Drones: Drone surveillance is likely to be perceived as a highly intrusive method for collection of data. While drones are already used also by LEAs to identify illegal manufacturing of drugs and explosives, monitoring of individual dwellings is also technically possible; At the moment, this is possible only at close distance; However, it cannot be excluded that (more costly,) more refined "at a distance" cameras may be available in the near future.
	Thermal cameras: Drone-mounted thermal cameras may give the sense that one's home walls are not absolute barriers; the awareness that drones, particularly at close distance, can see through walls has a significant chilling effect (see below Ethics).
	Sensors: sewage, solid and air monitoring sensors can, to different degrees, constitute an interference with both the privacy sphere, in particular of the home.
	Data fusion: If combined with data from other sources and datasets, e.g, discrete sensors, analogic sensors, standard webpages, deep web, publicly accessible repositories (e.g. chambers of commerce or land registries) and mathematical models (e.g. a fluid-dynamic system model or the result of a spectroscopy), monitoring can reveal private information about the residents of a building.
Necessity	SYSTEM should be able to demonstrate that there is an objectively verifiable need to deploy a surveillance measure of its characteristics.
	SYSTEM should be used adequately by police according to the specific situations (where the use of surveillance systems could be considered necessary)
Proportionality	The deployment of the SYSTEM device should keep fair balance between private and public interests.
	SYSTEM should be as privacy friendly as possible. This means that, where possible, should be able to adjust its level of privacy protection depending upon the circumstances. Such 'adjustability' should take into account the sensor technologies used and the possibility that they may directly identify particular individuals (thermal cameras using infrared radiation may be able identify some features or characteristics of individuals).
	Police and other organizations should be able to set and programme a SYSTEM device relatively easily so as to ensure that its use would be proportional for the particularities of their respective cities.

CONDITIONS ON THE RIGHT TO PERSONAL DATA PROTECTION	
Nature of the data processing operations	The type of planned data processing activities~~,~~ regardless of whether they concern personal data, should be made explicit and documented.
Scope of the data processed	The Consortium must identify the full range of data that may be exploited in SYSTEM.
Compliance with data processing principles	The SYSTEM project should proactively demonstrate compliance with the rules of data protection law: 1) Lawfulness, fairness and transparency; 2) Purpose limitation; 3) Data minimisation; 4) Accuracy 5) Storage limitation; 6) Integrity and confidentiality.
Rights of citizens and data subjects	During research activities, SYSTEM partners should inform citizens about the main elements of tests, of the SYSTEM project and, in general, about the functioning (purpose, nature of monitoring, duration) of the technology implementation. The information of citizens should be carried with due respect to those aspects of SYSTEM that due to their nature must be kept confidential and therefore must not be disseminated.
	During the deployment, authorities operating SYSTEM should provide sufficient information to the public (e.g. by popular media or info campaign) and/or notify competent public authorities, such as public security bodies, about the deployment of the technology.
Data fusion: Algorithms and Automated decision making	Algorithms are necessarily selective in their design and are as subject to bias as the humans that programme them. It should be possible to explain how decisions based on automatic mechanisms (algorithmic logic) are taken, including consequences of such mechanisms for citizens.
CONDITIONS ON THE ETHICAL AND SOCIETAL ASPECTS	
SYSTEM at home	Surveillance systems like SYSTEM can contribute to erode the perception of privacy of homes because they introduce another surveillance device in societies that can already be described as a “surveillance societies.”
Autonomy, chilling effects and the surveillance society	SYSTEM surveillance can have a chilling effect as it reinforces the perception of being monitored. The autonomy of individuals living in communities who perceive they are under constant surveillance can be jeopardised.
Incidental Findings	In the context of research, an incidental finding policy must detail what happens in case, during research activities, information or facts that are criminally relevant arise.

Function Creep	Function creep occurs when a technology (or technique, programme, dataset, etc.) is used for a different purpose to the one for which it was originally designed.
The use of sensor technologies in solid waste	Garbage truck operators may see garbage trucks equipped with sensors as means to monitor their work activities and performances. Adequate safeguards should be taken to ensure that installing sensors on garbage trucks does not to monitoring of garbage truck workers.
Stigmatization of communities	While The deployment of SYSTEM technologies can lead to better protection of communities as producing illegal drugs and explosives endanger live, health and social life of persons who may witness criminal activities, the deployment of SYSTEM in certain areas, populated by ethnic minorities, could lead to the creation or reinforcement of stigma on certain communities.
Necessity and proportionality in a democratic society	It is important to be clear and transparent as to why a surveillance technology is deployed, especially if a single technology can be used for multiple categories of purposes (e.g. both law-enforcement and non-law-enforcement purposes).
CONDITIONS ON LEAs USE OF SYSTEM	
Legal basis	The use of surveillance practices must be based on legal grounds. The legal basis (such as regulation, power) allowing the deployment SYSTEM's method of surveillance should be identified before deployment.
Envisaged deployment	In case SYSTEM is used for monitoring of wide areas, clarification and justification of should be provided to the appropriate public authorities.
Evidence	In order to be effective, it is necessary to clarify the value of evidence emerging from SYSTEM monitoring in criminal proceedings. For instance to clarify if the information collected from SYSTEM is a first step for further collection and seizing of evidence.
Protocols of technologies deployment	Actions of LEAs follow protocols. LEAs' protocols concerning the use of SYSTEM must be identified.

Table 2 - Framework Conditions

5 MOBILISING THE LESA FRAMEWORK VIA A QUESTIONNAIRE: INSTRUCTIONS FOR PARTNERS

SYSTEM is a multidisciplinary project with different work streams, involving different forms of expertise. As mentioned in the Introduction, in order to assess the impacts of SYSTEM from a legal and ethical perspectives, it is necessary to establish a dialogue between technical partners specialised in processes of technological development and the legal and ethical partners.

In order to establish such a dialogue, a questionnaire has been prepared in **Annex 1**.

Project partners are asked to answer a series of questions that relate to the conditions elicited in the aforementioned LESA Framework.

Specifically, the questions presented in the questionnaire are divided into six **areas**:

1) The area of technical description of SYSTEM.
2) The area of privacy.
3) The area of data protection.
4) The area of ethics and societal aspects.
5) The area of LEAs' use of SYSTEM.
6) The area of collection and use of criminal evidence in the context of SYSTEM

The questions presented in the questionnaire are addressed to **four group of partners**. It is therefore important that each partner identifies to which group his or her institution of affiliation belongs.

Where no specific group is indicated then ALL PARTNERS are requested to provide answers to each question. Nevertheless, if you believe that your contribution to an answer could be valuable, do feel free and encouraged to answer, even if you do not belong to the group indicated.

The only exception is the coordinator, FORMIT. Given its role, the coordinator is expected to provide an answer to all questions.

At the beginning of each section, we have inserted a brief introduction.

Following each question, a brief explanation is provided to explain the rationale behind the question and assist the relevant partners in answering. In the event you still have doubts how to answer, please do not hesitate to contact:

Sergi Vazquez Maymir (sergi.vazquez.maymir@vub.be)

And

Eugenio Mantovani (Eugenio.Mantovani@vub.be)

If you think that you are unable to provide an answer, please state so, and provide a brief explanation.

The groups of partners are:

GROUP 1: DATA FUSION AND ALGHORITHMIC DEVELOPMENT	**GROUP 2:** SENSOR TECHNOLOGIES	**GROUP 3:** LAW ENFORCEMENT AUTHORITIES	**GROUP 4:** LOCAL ENTITIES
1. POLITECHNIKA WARSZAWSKA 2. RESI INFORMATICA SPA 3. UNIVERSITAET DER BUNDESWEHR MUENCHEN) 4. ISEM-INSTITUT PRE MEDZINARODNU BEZPECNOST A KRIZOVE RIADENIE 5. USTAV HYDROLOGIE SLOVENSKEJ AKADEMIE VIED	6. FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. 7. SENSICHIPS Srl 8. T4I ENGINEERING SMPC 9. BLUE TECHNOLOGIES SP ZOO 10. HOCHSCHULE FRESENIUS GEMEINNUETZIGE GMBH	11. OSSERVATORIO SULLA SICUREZZA E DIFESA CBRNE 12. MINISTERIO DELLA DIFESA 13. BUNDES KRIMINALAMT 14. CENTRALNE LABORATORIUM KRYMINALISTYCZNE POLICJI 15. PREZIDIUM POLICAJNEHO ZBORU SR	16. ACQUALATINA SPA 17. ROMA CAPITALE 18. ACEA ATO2 SPA 19. AMA 20. PREZIDIUM POLICAJNEHO ZBORU SR 21. AKADEMIE VIED 22. BRATISLAVSKA VODARENSKASPOLOCNO STA.S

Table 3 Groups of project partners

Finally, what will happen after you have provided answers?

The information will be used to draft the Risk Review reports, foreseen under T10.3. These reports highlight the impacts, risks and the measures adopted to mitigate the said impacts or risks to the LESA framework. Specifically, the evaluation and treatment of your answers will help the legal and ethical partner VUB to document the mitigating measures implemented or that will be implemented and to outline any residual risks. Following the first evaluation report, three periodic risk reports will be produced at months M22, M26 and M30 (Deliverable 10.3 Risk review reports)[9].

[9] M22 = June 2020; M26 = October 2020; M30 = February 2021.

ANNEX 1: THE QUESTIONNAIRE

Following the instructions provided in section 5 of this deliverable, partners should, to the best of their ability, answer the following questions.

Please try to make an effort and write more than a few words, explaining your own views, what actions have been taken or should be taken; if, in your view, no action is required because there is no problem or concern to tackle, please state so and explain why not.

Please return the questionnaire to:

Sergi Vazquez Maymir (sergi.vazquez.maymir@vub.be)

Deadline: 15 April 2020

SECTION 1: TECHNICAL DESCRIPTION OF SYSTEM IN GENERAL AND DATA FUSION AND ALGORITHMIC DEVELOPMENTS IN PARTICULAR

In general, SYSTEM aims at producing a tailored network of sensing devices, which will be integrated through a data fusion monitoring centre. SYSTEM components will support the detection of home-made explosives (HME) and synthetic drugs manufacturing by detecting intermediates and impurities of the production process and precursors used for their synthesis. SYSTEM will acquire and process data from the sewage wastewater and solid waste networks as well as air emissions from target areas in real-time. These utility networks will be monitored continuously to detect and relate the occurrence of *abnormal use of chemicals* transported/provided within the whole area covered by SYSTEM. In this regard, networks of sensing devices – working in different and complementary utilities and environments – will be integrated into SYSTEM to be deployed across different urban areas in six cities, and their data will be fused into an improved data-based decision support system (SYSTEM DoA Annex 1, Part B, p. 9).

Specifically, with respect to the **data fusion and algorithmic development in SYSTEM,** the project DoA states, "the Monitoring Centre enables the following data management functions: collection, verification, storage, visualization, search, correlation, and elaboration. The system embeds a data fusion engine that can be configured to address a large variety of situations requiring intensive data processing. It can aggregate data from a variety of sources and formats, including discrete sensors, analogic sensors, standard webpages, deep web, publicly accessible repositories (e.g. chambers of commerce or land registries) and mathematical models (e.g. a fluid-dynamic system model or the result of a spectroscopy). Data is processed with **proprietary data fusion algorithms** allowing different types of analysis, including statistical techniques (e.g. multivariate analysis, statistical inference), machine learning (e.g. tree kernels, pattern recognition), and mathematical analysis (e.g. sparse matrix computation heuristics, topological analysis)." (SYSTEM DoA Annex 1, Part B, p. 30). It is intended that new algorithms be considered to handle additional sources of data such as geographic and topological data, physical models, structured and unstructured data collected from the web, and other sensors not necessarily part of SYSTEM.

With the following questions, we wish to clarify some technical aspects of SYSTEM.

While some of these questions relate to technical deliverables of the project, we ask partners to describe the **technical elements** in layman terms.

This is important, in general, to avoid the risk that research and innovation projects are obscure to nonspecialized audiences. In particular, activities such "aggregation of data from a variety of sources, can have relevant public, legal and ethical, implications that need to be made explicit.

Technical description of SYSTEM as a whole	
Relevant to	***Required Input***
Group 1, Group 2	1. **Provide a brief overview of the element of SYSTEM you are developing.**
	Reason*: Provide a brief description for non-specialists helps to understand the system in its entirety. This is important both for assessment purposes as well as for compliance with transparency principles.*
	Answer:
Group 1, Group 2	2. **What are the main functionalities of this element and its role in SYSTEM as a whole?**
	Reason*: The description of the functionality of an element contributes to the understanding of the dependencies and relationships between different parts of SYSTEM.*
	Answer:
Group 1, Group 2	3. **Have you tested the accuracy and reliability of your element? What is the level of technological readiness attained now (March 2020) and what is the aim for the real case demonstration (M20)?**
	Reason: *Real case scenario testing requires a high technological readiness level (TLR).*
	Answer:
Group 1, Group 2	4. **Based on your expertise, would it be possible to attain the same purpose of the technology you are developing using other techniques or methods, including traditional, non-technological, techniques and methods?**
	Reason: *The necessity of an element can be gauged against the possibility or the impossibility of using alternative methods.*
	Answer:
Group 1, Group 2	5. **What are the costs of production of your element? Are there any alternative, cheaper solutions, with same effectiveness**?

	Reason: *In order to increase the affordability of the whole SYSTEM device, cost effectiveness should be taken into consideration, bearing in mind that LEAs of different countries have different spending capacities.*
	Answer:
Group 1, Group 2, Group 3	6. **From a technical point of view, do you think that SYSTEM technology can be repurposed to monitor activities other than explosive manufacturing and drug production?**
	Reason: *it is sensible to understand how easily SYSTEM can be repurposed to monitor activities that did not fall within the purview of activities for which the technology is developed.*
	Answer:
Group 1, Group 2	7. ***Is there anything else you would like to emphasize regarding the technological solution you are developing?***
	Reason: *Any additional input from you can be useful to minimise unforeseen risks.*
	Answer:
Group 1, Group 2	8. **Please estimate a range of false positives for each type of monitoring foreseen in SYSTEM**
	Reason: *An assessment of false positive rates is required for all sewage monitoring technologies, but especially for those that can be relatively closer to a target building (such MilliMole and MicroMole), as the consequences of these relatively more intrusive technologies are more serious.*
	Answer:

Table 4 Technical description of SYSTEM as a whole

Data fusion and algorithmic development	
Group 1	1. **In layman terms, what is the logic behind the algorithm that you are developing? In particular, how does your solution enable the triggering of an alert?**
	Reason: *in order to assess the technology, the logic and rationale behind automated decision making must be clear. Specifically, we must clarify what automated decisions are taken in SYSTEM so, e.g, pinpointing where an alert occurs, delimiting an area of interest, or displaying information clearly, etc..*
	Answer:
Group 1	2. **Can human intervention oversee the process of algorithmic decision, how?**
	Reason*: In case of mistakes or errors or malfunctioning, users must be able to intervene.*
	Answer:
Group 1	3. **Can the algorithms triggering an alert be edited/modified easily (i.e. by a (corrupt) police officer using the device)? If not, who has the ability to alter the logic behind algorithms?**
	Reason: *it is important to assess whether it is possible to bend the algorithms to jeopardise or to steer maliciously criminal investigations.*
	Answer:
Group 1	4. **Is the data collected stored in a secure way and safe from unintentional/malevolent access? Pleased describe briefly the security measures.**
	Reason: *if data is stolen or modified the robustness of SYSTEM is compromised.*
	Answer:
Group 1	5. **Can false positives arise? For instance, is it possible that the data collected are not accurate because, e.g, the presence of a nearby factory alter the sewage stream? As result the data fusion centre might be processing tampered data.**
	Reason**:** *The accuracy and reliability of all SYSTEM component technologies depend on the rate of false positives.*

	Answer:
Group 1	6. **Can an investigative judge or magistrate, who may be in charge of approving warrants for the use of surveillance devices by the police, have access to the rationale behind the detection algorithms? Can they ask to modify the detection algorithms?**
	Reason: *Judges in different jurisdictions may need or require adapting the way SYSTEM monitors an area to the different necessities or requirements of national law or powers.*
	Answer:
Group 1	7. **Are the detection algorithms used likely to be comprehensible to law enforcement authorities (e.g police, investigating judges and magistrates)? It is training required or advised or foreseen?**
	Reason: *Those in charge of approving the use of surveillance devices/ approving warrants in criminal investigations may want to know how, when and what SYSTEM will record before using it.*
	Answer:
Group 1	8. **Will the alerts triggered be stamped so that it will be possible to track when an alert was triggered exactly? Can such time stamps be altered?**
	Reason: *The decision-making process in SYSTEM must be verifiable. The inclusion of a time stamp may be important for instance to justify the adoption of other measures, e.g. using drones. This is also important to justify investigating decisions in court, should an allegation of arbitrariness be raised by a defendant in court.*
	Answer:
Group 1	9. **Is there a chain of custody stamp in the metadata. If not what other methods will be used to demonstrate a valid chain of custody to track the origin of the alerts**?
	Reason: *A chain of custody stamp can be important in demonstrating that evidence was not tampered with.*
	Answer:

Group 1	10. **Is it possible to alter the map of criminal activities provided by the collected data?**
	Reason: *It is important to ensure that the map derived from SYSTEM data is secured and cannot be modified.*
	Answer:
Group 1	11. **Does SYSTEM keep a record of data processing activities? How are the records maintained? What are the rules of access to this documentation?**
	Reason: *The maintenance of the record of the activities is required by law (art. 30 GDPR) and could be advantageous in multiple cases.*
	Answer:
Group 1	12. **Please explain how the communication channels within the Genesi Monitoring Centre are are kept secured from any external interferences.**
	Reason: *Adequate technical organisational measures should be adopted to ensure that data processing operations are safe.*
	Answer:

Table 5 - Data fusion and algorithmic development

SECTION 2: AREA OF PRIVACY

In this section we address the impacts in terms of privacy in a wider sense, meaning outside the concept of data protection.[10] Privacy is understood as an opacity tool against interference upon individuals' private sphere; as such it embodies normative choices about the limits of governmental and private actors on citizens.[11] SYSTEM, by its very nature, interfere with the privacy of individuals. Of course, this does not mean that SYSTEM interference on privacy are illegal; whether infringements to right to privacy of individuals are acceptable will depend on whether SYSTEM surveillance is considered necessary and proportional. These requirements have been elicited by the ECtHR in a number of cases, many of which were discussed in Deliverable 10.1 and 10.8.[12]

As for necessity, in the words of the European Data Protection Supervisor "*necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal*".[13] As such, necessity is not something the SYSTEM project will be able to influence directly; that is to the particular public authorities and law enforcement agency 'on the ground' to decide , taking into account the particular local conditions. The questions presented below relate to possible ways in which SYSTEM as a project could demonstrate the necessity (and proportionality) of its development and deployment.

Necessity aims to answer a series of ***why*** questions, such as

1) Why do we need certain processing of data?
2) Why alternatives less intrusive are insufficient to address the problem?
3) Why the proposed processing can handle/target the problem more effectively than others?

The assessment of proportionality follows the assessment of necessity. The assessment of **proportionality** involves examining whether the (necessary, above) interference with the right to privacy and with fundamental rights and freedoms is proportionate. Assessing proportionality must also consider **the effectiveness of the solution proposed.**[14]

An example of proportionality is, for instance, the possibility of limiting the range of the monitoring in a way so that it only covers certain times or to restrict it to areas where there is "reasonable suspicion" or highly likeliness of criminal activities being perpetrated. Another example would be the possibility of operating sensors and data processing on a case by case basis, such as to limit the use

[10] For a discussion on privacy in a broad sense (i.e. beyond its mere relevance to the control of personal data see: D. Solove, *Understanding Privacy*. (Cambridge: 2008).

[11] De Hert P, Gutwirth S. Privacy, Data Protection and Law Enforcement, Opacity of the Individual and Transparency of the power

[12] 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

[13] EDPS, "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 11 April 2017, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

[14] EDPS EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data

of detection algorithms depending on the particular case or the use of sensor to specific areas.

In short, whilst the assessment on necessity aimed to answer "why" (a determinate activity had to be carried out), the proportionality test asks how or how much:

- How much does the surveillance interfere with fundamental rights (intensity)?
- How much relevant is the objective the processing aims to tackle?
- How much efficient is the envisaged solution in fulfilling its objective?

Accordingly, the questions posed below are related to aspects that have been identified as possibly contributing towards the development and deployment of SYSTEM in terms of making its use more likely to be proportional.

CONDITIONS ON NECESSITY	
Relevant to	**Required Input**
Group 3, FORMIT.	1. **Referring statistics or other knowledge, please demonstrate the genuine problems you are trying to address using SYSTEM?**
	Reason: *Reason: Surveillance activities must undergo an empirical assessment of the problem motivating such interference based on enough verifiable evidence.*[15]
	Answer:
Group 3, FORMIT	2. **Please state which illegal activities (drug and explosive manufacturing) are within the scope and which are outside (e.g., drug consumption).**
	Reason*: The scope of any surveillance activity must be clearly delimited and described.*
	Answer:
Group 3, FORMIT.	3. **Are you aware of other alternatives that could potentially help addressing the problems mentioned in the previous point? Are you aware of a similar surveillance measures being developed or already been deployed?**
	Reason: *The necessity assessment of SYSTEM must consider any possible alternative. In the event existing measures are deemed insufficient or inadequate, please motivate your answer.*

[15] Citing a report on drug "problems" without linking the statistics to the type of drug trafficking concerned by the proposed directive did not constitute, in the view of the EDPS, a valid reference (paragraph 11). See Guidelines on assessing necessity of measures that limit the fundamental rights to privacy and to the protection of personal data.

	Answer:
Group 3, FORMIT.	4. **In your opinion, is the ***wide monitoring*** of entire cities the most suitable approach to fight explosive manufacturing and drug production?**
	Reason: *The necessity of SYSTEM to monitor city wide areas must be justified.*
	Answer:
Group 3, FORMIT	5. **In a real case scenario would all the sensors developed in SYSTEM always be used (e.g. waste truck monitoring, sewage sensor, air sniffing sensors, drones)? Please explain the value of monitoring all types of waste, namely: a) sewage b) solid and c) air monitoring. Explain what type of insights each might provide to the investigation of the serious crime targeted in SYSTEM**
	Reason: *the necessity of waste monitoring must be assessed both individually and based on enough and reasoned grounds in each scenario. While solid waste monitoring might be relevant in one city it might not be the case for another.*
	Answer:
Group 3, FORMIT	6. **In your opinion, for how long should SYSTEM monitoring system be in place? Why?**
	Reason*: The duration of the surveillance must be duly justified.*
	Answer:
Group 3, FORMIT	7. **Based on your expertise please describe a scenario where the deployment of a thermal camera would be necessary.**
	Reason: *Interventions involving use of the thermal camera should be exceptional and conducted only based on confidence that innocent parties will not be unnecessarily captured in images.*
	Answer:

Table 6 - Conditions on Necessity

CONDITIONS ON PROPORTIONALITY	
Relevant to	**Required Input**
Group 3	**In your view does SYSTEM need to be deployed in as many and as large as possible areas in order to be effective?, or, Do you think that SYSTEM can attain this same purpose by being deployed in restricted areas, tailored to specific "intelligence-gathering" purposes.** - **In you think that the first case is true, please explain the reasons why targeted surveillance cannot achieve the same result as wide surveillance.** - **In case you think that the first case is true, please explain what arguments militate against deploying SYSTEM in wide areas.**
	Reason: *surveillance technologies collecting information tend to expand themselves into large systems, with an increased risk of control over individuals. This expansion of technology is justified arguing that the more information a technology gathers, the more refined will be the surveillance. This argument collides with the assessment of adequacy and jeopardize the proportionality requirement.*
	Answer:
Group 4	2. **Do you think that SYSTEM could be deployed in <u>any</u> city? Do all its components work equally regardless of where they are being deployed?**
	Reason: *The suitability of SYSTEM to achieve its goals must be assessed against the criteria that make a city (town, etc.) a 'good fit' for SYSTEM technologies (e.g. 'Your town would benefit from SYSTEM if it meets these criteria…').*
	Answer:
T4i **Group 3**	3. **How far away from the targeted building can a drone operate while still providing accurate data that could qualify as evidence? What is the scale of accuracy in thermal imaging?**
	Reason: *This aspect is relevant to assess the acceptable level of intrusiveness of thermal imaging via drones.*
	Answer:
Group 3	4. **Based on your experience, for how long is it genuinely necessary to have information available for offline analysis, in order to achieve the goals, set by SYSTEM?**
	Reason: *The assessment of proportionality must consider the relationship between the data which must be retained and the threat to public security for which data is retained.*

	Answer:
FORMIT, Group 1 Group2 and Group 3	5. **Once fully operational, what are the financial costs of the whole SYSTEM: including staff training, operation and maintenance of sensors, data processing activities (e.g. storage, security)? If possible, please provide an estimate.**
	Reason: *The cost of deployment represents an element in assessing the appropriateness of a measure when compared to possible alternatives.*
	Answer:

Table 7 - Conditions on Proportionality

SECTION 3: AREA OF DATA PROTECTION

Whilst privacy is an instrument protecting the opacity of the individual, the right to personal data protection refers to a set of instruments designed to ensure the transparency of processing. Whilst, strictly speaking, SYSTEM technology is not targeting data relating to an identified or identifiable individual, SYSTEM does entail a systematic monitoring of public domain areas. Accordingly, the General Data Protection Regulation (GDPR, or the Regulation) requires a Data protection Impact Assessment (DPIA). This assessment is aimed at operations which involve:

i. 'systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person';

ii. processing, on a large scale, of special categories of data or of personal data relating to criminal convictions and offences; and

iii. 'systematic monitoring of a publicly accessible area on a large scale' (Article 35(3) of the GDPR).

In these cases, the Regulation requires a "systematic description of the envisaged processing operations" (Article 35(7)(a)), in particular a **contextual description** of the envisaged data processing operations, particularly their nature, scope, context and purposes, the legitimate interest of the controller (if applicable) and the stakeholders involved (data subjects, controllers, processors, third parties and public authorities), and a **technical description** containing personal data flows and – possibly – a visualisation thereof.

Accordingly, the questions below seek to scope out these requirements with regards to both SYSTEM as a research project and as a systematic and extensive surveillance tool. The questions are divided into general questions relating to data processing, transparency, and security of data processing.

CONDITIONS ON THE RIGHT TO DATA PROTECTION	
Relevant to	**Required Input**
Group 1, Group 3, Group 4	1. **According to your own area of expertise please list and briefly describe the data sets processed by SYSTEM.**
	Reason: *As required by the GDPR, an account of what data is collected of each SYSTEM technology should be prepared.*
	Answer:
Group 1, Group 3,	2. **Please think and write what kinds of additional information could potentially be captured either, 1) intentionally; 2) unintentionally or 3) as a by-product of collecting the target data or information. Please identify and briefly describe each**

Group 4	**data set**
	Reason: *For instance, sewage monitoring could provide information about cleaning or bathing habits. Whilst this data set is "innocent", that is, procure no harm to rights and freedoms, it must nonetheless be taken into account.*
	Answer:
Group 1	3. **Who is responsible for the control of the collected data and decides how the data will be used?**
	Reason: *As required by the GDPR, it is important to establish who has control of the purpose and the means of the data processing activities. .*
	Answer:
Group 1	4. **Do you think that, based on the data collected by SYSTEM, LEAs will be able to single out an individual person(s) or a few persons involved in the targeted illicit activities? If your answer is yes or, please provide an explanation.**
	Reason*: The GDPR requires asking whether the data recorded by the SYSTEM device can be related to an identified or identifiable natural person.*
	Answer:
Group 1	5. **For how long will the data gathered be retained? What will happen with the data collected during the project after the project has come to an end? Please provide answer from the perspective of the research being conducted during the SYSTEM project**
	Reason*: Based on the principle of storage limitation (Article 5 (e) of the GDPR) the processing of data should be kept for no longer than is necessary for the purposes which the data is processed for.*
	Answer:
Group 1	6. **Who will have access to the data processed in SYSTEM during the research activities? What are the rules of access (with special attention to its conditions, mode, and limits)?**

	Reason: *The more people likely to have access, the higher the risk that the data can be misused. It should be possible to log and demonstrate any processes that have been applied to the data processed in SYSTEM.*[16]
	Answer:
ALL PARTNERS	7. **Please indicate if your Organization has any internal policy or protocol on data protection law.**
	Reason: *the GDPR requires the controllers or processors to proactively demonstrate compliance with data protection law. This requirement can be satisfied if the controllers or processors abide by an internal data privacy protocol or code. (this requirement is in addition to the requirement of having a Data Protection Office, already verified)*
	Answer:
Transparency	
FORMIT	8. **Do you plan to inform "the public" about the monitoring activities planned in the SYSTEM project tests and demonstrations? If no, please explain why.**
	Reason: *The GDPR principle of accountability entails that processing activities are conducted under the responsibility of a verifiable person or authority. Given the scope and nature of SYSTEM activity, "the public" can means citizens in general, elected representatives, town halls executives, assemblies of stakeholders, e.g., in water management systems, or in solid waste management companies, etc. Any organism which provides a link with the public.*
	Answer:
	9. **If not, please indicate which piece of national legislation allow SYSTEM test to be run in your cities without informing the public. Please indicate 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.*
	Answer:
FORMIT	10. **If yes, please identify the authorities and describe the channels or and forms that you intend to use, such as press releases to local newspapers, ad hoc meetings**

[16] This is a requirement for example of the Association of Chief Police Offices (ACPO) of England, Wales and Northern Ireland. See: http://www.bcs.org/content/ConWebDoc/7372

	with stakeholders, presentation at competent political committee, etc.
	Reason: *The requirement of accountability and transparency must consider the different scope and nature of activities undertaken. "The public" means citizens, elected representatives, town halls, assemblies of stakeholders in water management systems, or in solid waste management companies, etc. Any organism related to the public sphere.*
	Answer:
Group 1, Group 3 , FORMIT	11. **Is it possible for the public to ask questions about SYSTEM research activities? What concrete *opportunities does the public (as defined above, citizens, elected representatives, town halls, assemblies of stakeholders etc) to ask questions about the project's research activities?***
	Reason*: the accountability and transparency are meaningless if there is no way ask information about who is accountable for the purpose, means and duration of SYSTEM activities.*
	Answer:
Security	
Group 1	12. **Please identify where the data is stored during the research activities carried in SYSTEM. If applicable please identify the service provider.**
	Reason: *If data is stored outside the EU the application of different legal framework should be identified.*
	Answer:
Group 1	13. **How do you ensure the security of data of the data processing activities during the research?**
	Reason: *appropriate technical measures should be applied to ensure the level of security, such as: safeguards against interception of wireless transmission; secured control rooms and rooms where information is stored.*
	Answer:

Table 8 - Conditions on The Right To Data Protection

SECTION 4: AREA OF ETHICS AND SOCIETAL ACCEPTANCE

As outlined in the Baseline report on Ethical and Societal aspects of system, new security procedures and measures can be met with resistance, nourishing or societal tensions or distrust arises. That is why new solutions must be effective and flexible to deal with criminal activities, but also ensure its societal acceptance.

Furthermore, ethical compliance represents a fundamental aspect in research projects funded by the European Union. In SYSTEM special attention must be put on the potential impacts that the research might have on those individuals directly or indirectly engaged: workers of water management companies, of sewage companies, as well as workers in solid waste management factories.

CONDITIONS ON THE ETHICAL AND SOCIETAL ASPECTS	
Relevant to	**Required Input**
Group 3	1. **In your view how could SYSTEM surveillance affect citizens' trust in law enforcement?**
	Reason: *citizens may come under the impression that the police knows everything about them, this might put the police and public authorities under a negative light.*
	Answer:
Group 3, Group 4	2. **Do you think that by testing or deploying SYSTEM in certain areas of cities specific ethnic or social groups may feel targeted or stigmatized?**
	Reason: *The discriminatory concerns on disadvantaged neighborhoods attached to the use of modern surveillance technologies has been observed with the deployment and operation of CCTV systems stigmatization and discrimination.*
	Answer:
Group 3, Group 4	3. **If you have answered positively to the previous question, how do you plan to minimize the risk of stigmatization against specific groups?**
	Reason: *specific groups might feel increasingly targeted, if the decision to test or deploy SYSTEM is not justified.*
	Answer:
Group 4	4. **How do you plan to inform solid waste truck operators? Are you going to inform trade unions?**

	Reason: *Participation of workers should be based on consent.*
	Answer:
Group 4	5. **How do you ensure that operators of waste trucks are not monitored by either employers or the police?**
	Reason: *On account of the principle of data minimization in article 5 (c) of the GDPR, data processing in SYSTEM cannot be used to monitor employees taking part if the research activities.*
	Answer:
ALL PARTNERS	6. **How do you plan to ensure the safety of workers involved in testing and demonstrations? Do the insurance cover accidents that may arise in connection to project activities?**
	Reason: *Appropriate safety measures must be taken in order to ensure the safety of workers, such as personnel of sewage waste companies installing the sensors*
	Answer:
ALL PARTNERS	7. **Beyond the one provided by the consortium, does your organization have an incidental findings policy for research activities such as the one posed by SYSTEM**
	Reason: *Incidental findings are defined as results that arise from a research activity, but which are outside of the original purpose for which the test or procedure was conducted.*
	Answer

Table 9 - Conditions On The Ethical And Societal Aspects

SECTION 5: KEY GENERAL PRINCIPLES RELATED TO THE DEPLOYMENT OF SYSTEM BY LEAS

As provided in SYSTEM's DoA, the technologies in SYSTEM are developed to ideally meet the requirements of any Law enforcement authority in the EU. Ultimately the full exploitation of SYSTEM will take advantage of "data fusion capabilities, integrating information provided by several components of the network itself in a synergic way". A typical application would include the distribution of several devices of SYSTEM to monitor simultaneously different locations and/or utility networks of a city with the aim at reducing the area of interest, thanks to an integrated and improved understanding of the substances detected and the possible place where those come from (SYSTEM DoA Annex 1, Part B, p.33). In view of the utilization of SYSTEM by law enforcement and public authorities it is sensible to assess some aspects related to the use of SYSTEM surveillance in concrete settings.

THE DEPLOYMENT OF SYSTEM BY LEAS	
Relevant to	**Required Input**
Group 3	1. **In the event SYSTEM is acquired LEA's in your Country, which authority would be in charge of approving its deployment ? i.e. which organisation(s) and, perhaps, units (e.g. drug unit, counterterrorism) , which individuals (or individuals, e.g. *officers of a certain rank)***
	Reason: *The use of surveillance technologies must be authorised by legitimate authorities acting with power vested in them by law.*
	Answer:
Group 3	2. **Has your institution/organization appointed a Data Protection Officer? If yes, please provide his or her contact details.**
	Reason: *Directive 2016/680 makes mandatory for Member States to designate a data protection officer (Article 32). Directives are subject to the legislative implementation by Member States.* *This question does not refer to the data protection that has been appointed in the context of SYSTEM research activities. If the two persons coincide, pls indicate the DPO, nonetheless.*
	Answer:
Group 3	3. **In the event SYSTEM would be operational and ready to be deployed in your jurisdiction, would your DPO be obliged by the laws and regulations of your country, to perform and Impact assessment?**

	Reason: *Any organisation (LEA or otherwise) adopting SYSTEM or SYSTEM component technologies should assess the impact on their stakeholders (including, notably, their employees).*
	Answer:
Group 3	4. **Based on your national legislation please provide the legal provision or regulation that would allow for the monitoring and analytical activities foreseen in SYSTEM. If such surveillance is not currently provided by law, just state so.**
	Reason: *SYSTEM should only be used where deployment has been approved correctly as prescribed by the law. The processing of personal data shall be based on a legitimate legal ground shall have specified purpose.*
	Answer:
Group 3	5. **If you were unable to answer to the previous question, please indicate what laws, power or procedures at in place in your jurisdiction for approving the use of covert (e.g. wiretapping) and regular (e.g. CCTV) surveillance measures?**
	Reason: *The use of surveillance practices must be based on legal grounds. The legal basis allowing the deployment SYSTEM's method of surveillance should be identified.*
	Answer:
Group 3	6. **In your opinion, how would a SYSTEM alert would be qualified: information, intelligence or evidence? For instance, how would you qualify an output from SYSTEM Data Fusion suggesting the location of a clandestine laboratory qualify as: information, intelligence or evidence?**
	Reason: *it is important to understand how knowledge would collect from SYSTEM be qualified in criminal proceedings in order to assess its impact on individual procedural rights (e.g. fair trial).*
	Answer:
Group 3	7. **Imagine that SYSTEM sends an alert. Please describe what follows next, such as an operational protocol.**
	Reason: *Any alarm based on automatic processing that could trigger events of serious consequence for any person should be reviewed by a qualified individual before the consequences are set in motion.*
	Answer:

Group 3	8. **Imagine that unauthorised actors gained access to SYSTEM. Or that someone locate the sensors. What possible risks to you envisage?**
	Reason: *It is sensible to anticipate all possible risks related to the deployment of surveillance activities, starting from the risk that the technology is appropriated by criminals*.
	Answer:

Table 10 - The Deployment of SYSTEM by LEAs

SECTION 6: THE AREA OF COLLECTION AND USE OF CRIMINAL EVIDENCE IN THE CONTEXT OF SYSTEM

SYSTEM could also provide material used as evidence in criminal proceedings. In order to be able to make use of such a manner the data will have to have been collected, stored, and handled in a manner that is compatible with rules concerning the gathering and use of evidence in criminal proceedings and fair trial. [17]

Rules concerning the admissibility of evidence are primarily a matter for national legal systems. It is not possible therefore to present a single legal approach for the SYSTEM project that would be acceptable in all jurisdictions. Some key general elements can however be gathered from European Sources, such as the ECtHR's interpretation of Article 6 ECHR on such issues.[18] These include:

- *Evidence must be collected fairly;*
- *Evidence must be of a sufficient quality;*[19]
- *Evidence should not be gathered through entrapment; and*
- *The gathering of evidence should be subject to appropriate use and oversight.*[20]

It is necessary for those involved in the design of a SYSTEM to be aware of these principles. As with other sections as series of questions is in order to assess the impacts on those principles.

SYSTEM AND CRIMINAL EVIDENCE	
Relevant to	**Required Input**
Group 3	1. **Based on your expertise, could the information provided by SYSTEM be used at Court as evidence either of a suspect's guilt or of LEAs justification for triggering a criminal investigation?**
	Reason: *the prerogative of the suspects and his/her fair trial rights might differ based on how the data is interpreted.*

[17] For a good analysis see "RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW" Council of Europe/European Court of Human Rights, 2014 http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf See also: J. Ingle, Overview: Criminal Law, Evidence and Procedure', *Cambridge Journal of International and Comparative Law*, 3,((2014) 265-268

[18] For a good overview of general principles pertaining to criminal evidence see: ibid.,

[19] CASE OF BYKOV v. RUSSIA (Application no. 4378/02), CASE OF JALLOH v. GERMANY (Application no.5481/00)

[20] Whilst the ECtHR has accepted the possibility of covert surveillance activities, it has stated that given there is a potential to infringe upon individual rights. In order to reduce this risk, such activities should be supervised by suitable individuals or organisations. This may include investigatory judges or in appropriate circumstances prosecutors. See for example: CASE OF BANNIKOVA v. RUSSIA (Application no.18757/06)

	Answer
Group 1, Group 3	2. **Is there a threshold (in terms of quality) for the use of images or videos in court or can courts use their discretion?**
	Reason: *SYSTEM image quality from thermal cameras will be lower than many conventional CCTV images. It is necessary to know whether this will be a problem in terms of evidence in criminal proceedings.*
	Answer:
Group 1, Group 3	3. **Will it be possible to present defendants with copies of the data or videos that may be used against them in legal proceedings?**
	Reason: *All evidence and processes applied thereto should be capable of transparent disclosure to both defendants and the court. A defendant may wish to access evidence against him, both before and during court proceedings in order to prepare his or her defence.*
	Answer:
Group 1, Group 3	4. **Will it be possible to explain and demonstrate any processes that have been applied to defendants and their legal counsel?**
	Reason: *Any processes applied to the evidence should be repeatable and be capable of explanation. A defendant may wish to access evidence against him, both before and during court proceedings in order to prepare his or her defence.*
	Answer:

Table 11 - SYSTEM and Criminal Evidence

BIBLIOGRAPHY

The Admissibility of Electronic Evidence in Court: Fighting Against High Tech Crime, created within the context of the CYBEX initiative concerned with the Admissibility of Electronic Evidence in Court https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf [21/05/2016]

Article 29 Data Protection Working Party, 'Statement on the role of a risk-based approach in data protection legal frameworks' (WP218) 30 May 2014, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf> [21/05/2016]

Association of Chief Police Offices (ACPO) of England, Wales and Northern Ireland, 'Presenting digital evidence to court' http://www.bcs.org/content/ConWebDoc/7372

Case - MALONE v. THE UNITED KINGDOM. (Application no. 8691/79)

Case - Peck v the United Kingdom (Application no. 44857/98)

Case - PJ & H v United Kingdom (Application no. 0004478/98 2001)

Case - Rotaru v. Romania [GC] (Application no. 28341/95, ECHR 2000-V)

Case - S. and Marper v United Kingdom (Application nos. 30562/04 and 30566/04)

Case - BYKOV v. RUSSIA (Application no. 4378/02)

Case - JALLOH v. GERMANY (Application no.5481/00)

Case - BANNIKOVA v. RUSSIA (Application no.18757/06)

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> [21/05/2016]

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]

C. Kuner, F. H. Cate, C. Millard, D. Jerker B. Svantesson and O. Lynskey, 'Risk management in data protection' in 5 International Data Privacy Law 95 <http://idpl.oxfordjournals.org/content/5/2/95.full.pdf+html> [21/05/2016]

D. Klitou, '*Privacy Invading Technologies and Privacy by Design*' 2014

D. Solove, *Understanding Privacy.* (Cambridge: 2008)

D. Wright and P. De Hert (eds.), *Privacy Impact Assessment* (Springer, Dordrecht 2012)

Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

G. Yohe and R. 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 <http://onlinelibrary.wiley.com/doi/10.1111/j.1749-6632.2009.05310.x/epdf> [21/05/2016]

G. Dionne, 'Risk Management: History, Definition and Critique' (2013) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2231635> [21/05/2016]

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]

International Association for Impact Assessment: Principles of Environmental Impact Assessment Best Practice <https://www.eianz.org/document/item/2744> [21/05/2016]

ISO 31000:2009 Risk management – Principles and guidelines (2009)

J. Ingle, Overview: Criminal Law, Evidence and Proceedure', *Cambridge Journal of International and Comparative Law*, 3,(2014) 265-268

J. A. Jones, 'An Introduction to Factor Analysis of Information Risk (FAIR)' (2005) <http://www.slideshare.net/Kabogo/an-introductiontofactoranalysisofinformationriskfair680> [21/05/2016]

J. F. Short Jr, 'The Social Fabric of Risk: Towards the Social Transformation of Risk Analysis' (1984) 49 American Sociological Review 711 <https://oied.ncsu.edu/selc/wp-content/uploads/2013/03/The-Social-Fabric-at-Risk-Toward-the-Social-Transformation-of-Risk-Analysis.pdf> [21/05/2016]

Microsoft Operations Framework (MOF) Risk Management Discipline, 'Identifying Risks in Operations' <https://technet.microsoft.com/en-us/library/cc535338.aspx> [07/05/2016]

P. Schaar, 'Privacy by Design, *Identity in the Information Society*' 3,(2) (2010)

P. Slovic and E. U. Weber, 'Perception of Risk Posed by Extreme Events' (2002) <https://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/slovic_wp.pdf> [21/05/2016]

P. 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) <http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1923&context=faculty_scholarship> [07/05/2016]

Privacy Impact Assessment Framework for data protection and privacy rights: Deliverable D1 – Revision of existing PIAs (2011) <http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf> [07/05/2016]

R. Macroy, Regulation, Enforcement and Governance in Environmental Law 2014

Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L119/1 [2016]

RIGHT TO A FAIR TRIAL - ARTICLE 6 OF THE CONVENTION – CRIMINAL LAW" Council of Europe/European Court of Human Rights, 2014 http://www.echr.coe.int/Documents/Guide_Art_6_criminal_ENG.pdf

R. Clarke, 'Approaches to Impact Assessment' Brussels, 22 January 2014 <http://www.rogerclarke.com/SOS/IA-1401.html#RA> [21/05/2016]

R. Clarke, 'Privacy Impact Assessment: Its Origins and Development' (2009) 25 Computer, Law and Security Review 123 <http://www.rogerclarke.com/DV/PIAHist-08.html> [21/05/2016]

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> [21/05/2016]

V. Kosta, *Fundamental Rights in EU Internal Market Legislation* (Hart Publishing, 2015)

White paper of the World Economic Forum, 'Rethinking Personal Data: A New Lens for Strengthening Trust' May 2014 <http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf> [21/05/2016]