SYnergy of integrated Sensors and Technologies for urban sEcured environMent

D10.4
LEGAL AND ETHICS SUPPORT PACKAGE

31 March 2021 **V4.0**

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	36 months
Topic	SEC-10-FCT-2017. Integration of detection capabilities and data fusion with utility providers' network

Deliverable number	D10.4
Deliverable title	LEGAL AND ETHICS SUPPORT PACKAGE
Leading partner	VRIJE UNIVERSITEIT BRUSSELS (VUB)
Partners contributing	n.a.
WP of reference	WP10
Title of the WP of reference	LEGAL AND ETHICS MANAGEMENT
Task of reference	T10.3
Title of the task of reference	LEGAL AND ETHICS MANAGEMENT
Deliverable type	REPORT
Dissemination level	PUBLIC (with the request to maintain it temporarly CONFIDENTIAL only for members of the Consortium (including the Commission Services)
Due date	M5 – January 2019. Foreseen in the DoA at M3 – November 2018. Extended by Mr. De Candido (DG HOME) with the email sent to Ms. Cavallini (FORMIT) on 10 December 2018.

Keywords	**Forms, templates, incidental findings policy, participants consent, non-disclosure agreement.**
Abstract	**This deliverable composes the Legal and Ethics support of the SYSTEM project. This file comprises documents that are or might be relevant to the SYSTEM project in order address the legal and ethical questions resulting from the project research activities. Therefore, the document represents a compendium of forms, and a living document that will be updated during the project life cycle.**

Editor	Sergi Vasquez Maymir (VUB), Eugenio Mantovani (VUB),
Contributors	n.a.
Reviewers	Steffen Krause (UNIBWM), Lorenzo Di Matteo (FORMIT)
Submission date of the draft to reviewers	23 January 2019

Submission date of the draft to the SAB (if required)	Not required

Register of document versions

Partner acronym	Version number	Date	Suggested relevant changes	Notes
VUB	V1.0	23/01/2019	First draft (all.)	//
UNIBWM	V2.0	29/01/2019	//	//
FORMIT	V2.1	29/01/2019	Executive Summary; Table of Contents; 1.2; 1.6; 8.	//
FORMIT	V3.0	01/02/2019	None	//
VUB	V4.0	31/03/2021	New version of the incidental finding policy and deatuls about the approval from the Security Advisory Board (Chapter 7)	//

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

This document is composed by 34 pages

Table of Contents

List of figures

List of tables

List of acronyms and abbreviations

DPO	Data Protection Officer
EB	Executive Board
EC	European Commission *or* Electrical Conductivity
ES	Exploitation Strategy
IPR	Intellectual Property Rights
LEA	Law Enforcing Agency
LESA	Legal Ethical and Social Acceptance
LEM	Legal and Ethical Manager
NSA	National Security Authority
PMB	Project Management Board
QA	Quality Assurance
SAB	Security Advisory Board
SME	Small and Medium Enterprise
SB	Stakeholders Board

EXECUTIVE SUMMARY

This deliverable comprises the Legal and Ethics support package (D10.4) of the SYSTEM project. It contains a number of templates and forms to be used by partners of SYSTEM to address the legal and ethical issues raised or emerging during the project research activities: information sheet, consent form, communication forms, Non-disclosure agreement, incidental finding policy, etc.

The supportive documentation included in this deliverable is part of SYSTEM's ethics management strategy, described in WP10 and in Section 5.1, Proposal 787128 - SYSTEM - Part B Annex 1. The supportive documentation included in D10.4 will be referred to and mobilised by D10.1 (Report on legal and ethical compliance of SYSTEM research activities) and D10.3 (Risk review reports).

This deliverable must be considered as a "living document"; the templates and forms included in this version reflect the state of the art of the project (currently M1 since the signature of the GA). As the project unfolds, this deliverable will be updated: object of these updates will be either the existing forms and documents, which will be filled in with details that are at the moment missing, or with new supportive documents that may become necessary, such as import/export protocols.
Accordingly, this deliverable will be regularly updated.

This deliverable contains a number of templates and forms to be used by partners of SYSTEM to address the legal and ethical issues raised or emerging during the project. As such, this deliverable must be considered as a "living document", which is accessible to all partners of SYSTEM. As the project unfolds, new documents concerning the management of the ethical and legal aspects of the project activities, will be included in this deliverable. Project partners are invited to consult this document as they look for templates, relevant authorites, or forms.

1. MAIN ELEMENTS OF THIS DELIVERABLE

1.1. INPUT FROM OTHER PROJECTS

Legal and ethics support package (D10.4) receives no particular inputs from other projects.

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

The present deliverable provides a common basis of communication mechanisms and documentation for all partners to communicate either internally, e.g., to the leader of WP10 and the legal and ethical manager (LEM), or externally, e.g., with research participants or with national authorities, stakeholders, etc.
The forms and templates contained in this document will need to be adapted to the activities carried out by the consortium, which involve the participation of human beings and /or the processing of personal data. Therefore, the elicitation of concrete details about tests or demonstrations is key to adapt or specify the content of the templates and forms contained in this deliverable.
Accordingly, the content of the legal and ethical support package will need to be tailored to the description and definition of the scenarios in WP1 “Scenario definition, users and system requirements”. Particularly Requirements scenario definition and system concept (D.1.1) and Data retrieval definition (D1.2). For similar reasons, Deployment plan (D8.1) from WP8 (“Demonstration execution and evaluation of SYSTEM”) will also be of importance.
Other expected forms of collaborations include the translation of some pieces of information into the national language of the country where tests are to be carried out. In general, all WPs are expected to cooperate in the development of the necessary forms and templates that might be necessary for the national framework concerned, for instance with regard to the drafting of communications addressed to their relevant national authorities. Considering this, the present WP might potentially require input from all WPs of SYSTEM.
The supportive documentation included in this deliverable is part of SYSTEM’s ethics management strategy, described in WP10 and in Section 5.1. The supportive documentation included in 10.4 will be referred to and mobilised by D10.1 (Report on legal and ethical compliance of SYSTEM research activities) and D10.3 (Risk review reports). These deliverables will describe, respectively, the applicable legal frameworks and identify the ethical, privacy, data protection, as well as societal issues that might arise from the research activities or from the implementation of SYSTEM technology in society.

1.3. APPLICABILITY

This deliverable contains a number of templates and forms to be used by partners of SYSTEM to address the legal and ethical issues raised or emerging during the project. As such, this deliverable must be considered as a “living document”, which is accessible to all partners of SYSTEM. As the project unfolds, new documents concerning the management of the ethical and legal aspects of the project activities, will be included in this deliverable. Project partners are invited to consult this document as they look for templates, relevant authorites, or forms.

1.4. REFERENCE DOCUMENTS

In order to set a framework in matter of a hierarchical conflict between the Legal and ethics support package (D10.4) and other documents such as the Description of Actions (DoA) in 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, the hierarchy of the documents is mandatory.

1.5. PURPOSE OF THE DOCUMENT

The Legal and ethics support package (D10.4) provides a repository of documents that are or might be relevant to the SYSTEM project in order address the legal and ethical questions resulting from the project research activities.

1.6. STRUCTURE OF THE DOCUMENT

The document is structured in the following way:

1. **Introduction**
2. **Communication Form From Partners To The Legal And Ethical Manager (LEM)** is a template for communicating doubt or issue regarding legal or ethical matters to the LEM;
3. **Communication Form From The Lem To The Partners** is a template for communication from the LEM to the project partners;
4. **Non-Disclosure Agreement (NDA)** is a model of agreement regarding non-disclosure of information by third parties or external experts;
5. **Statement On Criminal Records** is a model of statement to declare no relevant criminal records concerning the illegal production of drugs and/or explosives;
6. **Data Protection Officer Designation Form** is the model of appointment letter of a partner organisation DPO for the project;
7. **Incidental Findings Policy** is the proposed policy in matter of incidental finding to apply in case of criminally relevant evidencies;
8. **Information To Be Provided To Participants In Tests Or Demonstrations** is provided to human participants involved in therein;
9. **Consent Form For Participation in Research** is a form to submit to human participants in case the law requires such declaration;
10. **Registry Of Personal Data Processing Activities** is a model record to keep of all the processing activities of personal data;
11. **Confidentiality Statement For Researchers Directly Involved With Research Participants And Personal Data** is a model that assure confidentialy about personal information processed by researchers;
12. **National Data Protection Authorities** is a list of NSA responsible of data protection in the member states;
13. **National Licenses Offices Ex. Regulation (Ec) No 428/2009** is a list of National offices in charge of licenses in a specific regulatory framework.

2. COMMUNICATION FORM FROM PARTNERS TO THE LEGAL AND ETHICAL MANAGER (LEM)

SYSTEM partners are strongly encouraged to sue this communication to address the Legal and Ethical manager (LEM) about questions or doubts or any legal and ethical matter raised or emerging during project activities. The information exchanged throught this form shall remain confidential and used exclusively within the SYSTEM project.

SYSTEM PARTNER COMMUNICATION FORM

Partner(s) issuing the inquiry	
Related WP and Task	
Area of compliance	Please identify the area of compliance to which your inquiry relates for instance data Protection/privacy, technical and organisational measures, security, ethical issues etc.
Date of communication	
Date of reply	

Explanation in detail and lay terms of the issue and question:
Answer from the legal and ethical manager:

Figure 1 System Partner Communication Form

3. COMMUNICATION FORM FROM THE LEM TO THE PARTNERS

This Communication form will be used by the Legal and Ethical Manager (LEM) to communicate or to ask questions to partners concerning the impacts of SYSTEM project activities and SYSTEM technologies on the Legal ethical social acceptance framework (LESA) developed in "Report on legal and ethical compliance of SYSTEM research activities" (D10.1). By way of example, we hereby provide an example of a communication enquiring about the registry of data processing activities concerning the personal data collected during a test.

SYSTEM LEGAL AND ETHICAL MANAGER COMMUNICATION FORM

Compliance Area of the Form	Data Protection / Human Particpants/ Safety/ Security/Dual Use/Communication with third parties/or…
Related Work Package, Task and Deliverable	
Partner(s) addressing the question	
Date of communication	
Date of reply	

Issue nº 1: Data collected during real-life pilot

Explanation and question:

The principle of accountability mandates on data controllers to keep a registry of personal data processing activities.

Q: Please indicate which research data you have collected, specifying in detail which types of data subjects (children employees, adults) and the categories of data (e.g. identification data, data collected via sensorial components, such as images).

If you have retained data but subsequently sent it to another partner, you are still kindly requested to indicate which data you have temporarily processed and during which period.

Please indicate the indicative size of the data processed/collected

Answer from partner:

Figure 2 System Legal And Ethical Manager Communication Form

4. Non-Disclosure Agreement (NDA)

The Non-Disclosure Agreement is a contract that binds legally two or more persons, e.g., the SYSTEM consortium and external stakeholders or a partner from SYSTEM and a third person invited as expert, to treat specific information that may be disclosed in the course of the interaction between the parties confidentially or not disclose it to others without proper authorization. In short, the NDA commits the parties not to disclose information with regard to the object of their transactions.

NON-DISCLOSURE AGREEMENT SYSTEM PROJECT

This Non-Disclosure and Confidentiality Agreement (the "Agreement"), is executed as of the ______ day of __________________________, 20_____ (the "Effective Date"),

BY AND BETWEEN:

Vrije Universiteit Brussel (VUB), with offices at Pleinlaan 2, 1050 Brussel, herein represented by Eugenio Mantovani, acting as legal and ethical manager of project **SYnergy of integrated Sensors and Technologies for urban sEcured environment** and who is co-signing this agreement for acknowledgement and acceptance,

hereinafter called "**SYSTEM**";

AND

[Name of the stakeholder or external experts], with offices at [.................] represented by [..................] hereinafter called "**Disclosing Party**" or "**Receiving Party**" as the case may be;

Each party shall hereinafter jointly referred to as "Parties" or each separately as "Party",

WHEREAS, the Parties have acquired and/or developed a substantial amount of valuable Confidential Information, as hereinafter defined, which the Parties acknowledge to be of a confidential character, requiring suitable security and protection;

WHEREAS, the Parties desire to enter into discussions and exchange information for the sole purpose as described hereunder and desire to ensure that the Confidential Information, as hereinafter defined, revealed during such discussions will be protected from disclosure;

NOW, THEREFORE, in consideration of the premises and mutual covenants contained herein, the Parties hereto agree as follows:

1. For the purpose of this Agreement, "Confidential Information" shall mean all information, relating to the research, development, business, affairs, strategies, operations, technology, processes, algorithms, computer programs, services and other relevant data, of the Disclosing Party, provided to the Receiving Party in connection with the Purpose, in a form that may be transmitted in writing,

orally, visually or by any other form or medium, which (a) is identified in writing as being confidential at the time of its disclosure or within fifteen (15) days following its disclosure, or (b) would reasonably be expected by a recipient to be confidential or proprietary, based on the nature of the information contained therein and the circumstances in which the materials are provided. Any work product or portion thereof relating to or derived from any Confidential Information, in whatever form contained, generated by the Receiving Party which discloses Confidential Information shall also be deemed to be Confidential Information.

2. Disclosing Party agrees to make known to Receiving Party, and Receiving Party agrees to receive, Confidential Information for the sole purpose of: [the purpose should be described as clearly as possible] (hereinafter referred to as the "Purpose").

3. All Confidential Information delivered pursuant to this Agreement:
   a. shall be held and maintained in strict confidence by Receiving Party using the same degree of care that they use with respect to comparable, highly confidential information relating to its own business or activities; Receiving Party shall be liable for disclosure of Confidential Information of the Disclosing Party only if such care is not used; the burden shall be upon Receiving Party to show that such care was used;
   b. shall not be used by Receiving Party for any other purpose than the Purpose as described above, without the express prior written permission of Disclosing Party;
   c. shall not be made, in any form or manner whatsoever, available to any other third party;
   d. shall remain the property of Disclosing Party (along with all copies thereof) and shall be returned to Disclosing Party or destroyed, at Disclosing Party's sole option, within thirty (30) days of receipt by Receiving Party of a written request from Disclosing Party setting forth the Confidential Information to be returned or destroyed. Such request shall be made not later than three (3) months after termination of this Agreement. The Receiving Party shall be allowed to retain one copy for legal purposes in order to evidence compliance with the obligations of this Agreement.
4. The Receiving Party agrees to restrict circulation of Confidential Information to those researchers, directors, employees, advisors (including, without limitation, financial advisors and legal counsel) and agents, who (i) need to know the Confidential Information for the Purpose; (ii) are informed by the Receiving Party of the confidential nature of the Confidential Information; and (iii) agree with the Receiving Party to be bound by the terms of this Agreement or terms similar thereto, but not less restrictive.

5. The obligations of clauses 3 and 4 shall not apply, however, to any information which:
   a. is already in the public domain at the time of disclosure or becomes available to the public through no breach of this Agreement by Receiving Party;
   b. was in Receiving Party's possession prior to receipt from Disclosing Party as proven by its written records;
   c. is received by Receiving Party independently from a third party free to disclose such information to the Receiving Party;
   d. is subsequently independently developed by Receiving Party as proven by its written records.

Confidential Information shall not be deemed to be in the public domain merely because any part of said information is embodied in general disclosures or because individual features, components, or combinations thereof are now, or become, known to the public.

6. Notwithstanding any provision to the contrary contained herein, the Receiving Party shall be allowed to release Confidential Information received from the Disclosing Party if such Party is compelled to disclose such Confidential Information pursuant to any law, legal process, regulation or regulatory process, provided, however, as follows:

a. that the Receiving Party shall take all reasonable steps to preserve the confidentiality of the Confidential Information, including without limitation, requesting that the Confidential Information not be released to third parties or the public;
b. that the Receiving Party gives the Disclosing Party prompt notice of the legal process, to the extent that such notice is permissible, so that the Disclosing Party may seek an appropriate protective order or pursue such other legal action necessary to preserve the confidentiality of the Confidential Information;
c. that the Receiving Party provides reasonable assistance to and cooperates with the Disclosing Party in its efforts to preserve the confidential nature of the Confidential Information.

7. This Agreement shall be effective as of its Effective Date, first mentioned above. It may be terminated with respect to further disclosures upon thirty (30) days' prior notice in writing. This Agreement shall automatically terminate three (3) years from its Effective Date. The rights and obligations accruing prior to termination as set forth herein shall, however, survive the termination as specified in this Agreement.

8. Receiving Party's obligations hereunder with respect to each item of Confidential Information shall terminate five (5) years from the date of the receipt thereof by the Receiving Party.

9. Receiving Party shall have the right to refuse to accept any Confidential Information under this Agreement if it believes the receipt of such information would limit or restrict in any way the use of its own technology or otherwise impair its business interests and nothing herein shall obligate Disclosing Party to disclose to Receiving Party any particular information.

10. The Parties acknowledge that the disclosure of any aspect of the Confidential Information may give rise to irreparable injury to the Disclosing Party which would be inadequately compensable in damages. Accordingly, the Disclosing Party may seek to obtain injunctive relief to prevent the unauthorized use or disclosure of the Confidential Information in addition to any other legal remedies which may be available to it, and the Parties hereby consent to the obtaining of such injunctive relief in the event of unauthorized use or disclosure of the Confidential Information.

11. It is understood that no patent, copyright, trademark or other proprietary right or license is granted by this Agreement. The disclosure of Confidential Information and materials which may accompany the disclosure shall not result in any obligation to grant Receiving Party rights therein.

12. Disclosing Party warrants and represents that Disclosing Party possesses all necessary powers, rights, and authority to lawfully make the disclosure subject to this Agreement. The Parties hereto shall not be obligated to compensate each other for disclosure of any information under this Agreement and agree that no warranties of any kind are given with respect to such information, as well as any use thereof, except as otherwise provided for herein. Any information exchanged under this Agreement is provided "as is".

13. This Agreement represents the entire understanding and agreement of the Parties and supersedes all prior communications, agreements, and understandings relating to the subject matter hereof. The provisions of this Agreement may not be modified, amended, nor waived, except by a written instrument duly executed by both parties. This Agreement may not be assigned by either Party without the prior written consent of the other.

14. All disputes between the Parties in connection to this Agreement shall first be discussed in good faith between the Parties in order to try to find an amicable solution. If no solution can be found to settle the dispute within thirty (30) days after giving notice to the defaulting Party, then the dispute will be exclusively submitted to [e.g., the courts of Brussels, Belgium. This Agreement shall be governed by and construed in accordance with the laws of Belgium.]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representative on the dates specified below:

Party Signature: ....
Name: .... Date: ....
I confirm, for the project team, my agreement to participate in this research study.

Party Signature: ....
Name: .... Date: ....
Organisation: ....

Done in two copies, of which one is for the SYSTEM Consortium and one for the [party].

Done at [place] on [date]
Signature

[THIS VERSION HAS BEEN SUBMITTED FOR REVIEW TO THE SECURITY ADVISORY BOARD (JANUARY 2019)]

Figure 3 Non-Disclosure Agreement of the SYSTEM Project

5. Statement On Criminal Records

As stated in section 5.1, Proposal 787128 - SYSTEM - Part B Annex 1, the consortium commits to ensure that researchers involved in SYSTEM do not have relevant a criminal record concerning illegal production of drugs and/or explosives. Having discussed the matter at the KoM held in Rome, December 2018, the Legal and Ethical Manager has requested each partner to provide the following statement to the Coordinator.

To: the coordinator of project System
Object: statement on criminal records of SYSTEM researchers

I [............] responsible of partner [..............]

hereby confirm,

that, further to a background check, carried out in conformity with national law and with art. 10 GDPR, the researchers involved in the project under my supervision do not have a relevant criminal record that could expose the research or the research results to the risk of being misused.

I also confirm that the same verification will be performed with regards to any researcher who may be, in the course of the project, involved in SYSTEM related activities.

Yours Faithfully

Name and Surname: .... Date: ....

Figure 4 Statement on Criminal Records

6. Data Protection Officer Designation Form

A form through which each partner involved in the SYSTEM consortium nominates a Data Protection Officer for the purposes of the project activities.

Appointment of data protection officer (DPO) for the project SYSTEM

The [Partner] has, pursuant to entry into force of Regulation (EU) 2016/679 (the General Data Protection Regulation), appointed an acting Data Protection Officer in the person of:

- NAME and SURNAME:
- Address:
- Telephone number:
- Email:

as Data Protection Officer for the SYnergy of integrated Sensors and Technologies for urban sEcured environment project (SYSTEM), granted project Number: 787128.

with the following tasks:

- to act as first contact point for the Coordinator and for VUB concerning the obligations under the GDPR and other applicable data protection provisions in SYSTEM;
- to participate in training and meetings of SYSTEM DPOs organized by VUB;
- to actively participate in the data protection impact assessment conducted by VUB, answering to queries, questionnaires.

The appointments shall take effect on the date of signature of this appointment letter and last for the duration of the project SYSTEM.

place, date

Signature of the representative of the partner in SYSTEM

Figure 5 DPO Appointment Letter

7. Incidental Findings Policy

Incidental findings are described as results that appear outside the original purpose for which a test or a procedure was conducted. In the case where incidental findings were potentially criminally relevant, this incidental finding policy will apply.

7.1. Incidental Findings Policy

In Figure 6, the version of the Incidental Findings Policy in effect at the time of the document date submission.

SYSTEM INCIDENTAL FINDINGS POLICY

Incidental findings are known to be results that appear outside the original purpose for which a test or a procedure was conducted. In light of article 19 of the H2020 Regulation (EU) No 1291/20135,[1] SYSTEM project is subject to compliance with 'ethical principles and relevant national, Union and international legislation, including the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights and its Supplementary Protocols. In particular, the SYSTEM consortium is specially compromised to respect 'the principle of proportionality, the right to privacy, the right to the protection of personal data, the right to fair trial and the right to non-discrimination.

When an incidental finding referring to potential criminal activity occur during the execution of the project, the following procedure shall be followed:

1. The responsible project partner who becomes aware of the finding, will report without delay all details of the incidental findings to the representative of the participating Law Enforcement Authority.

2. Unless the provisions of the relevant national, European Union and international legislation express it otherwise, the Law Enforcement Authority shall report on the existence of the incident to the Project Coordinator, the Ethical and Legal Managers, Eugenio Mantovani (VUB, emantovani@vub.be) and Sergi Vazquez Maymir (VUB, sergi.vazquez.maymir@vub.be).

3. The project coordinator, with the support of the Legal Ethical Managers and prior consultation to the relevant Law Enforcement Authority shall keep record of the incidental finding. The record will include the following information :

    i. The date when the incident took place

    ii. The research context in which the incidental finding was detected including: the partners involved, and the nature of the research activities performed that lead to the incidental finding.

[1] 'Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/

iii. The legal relevance of the incident with specific references to articles of law allegedly violated.

4. The Project coordinator with the support of the Legal Ethical Manager and subject to a motivated opinion by the relevant Law Enforcement Authority involved, shall decide to inform the consortium partners, the national Data Protection Supervisor and the European Commission about:

   i. The information of the incidental finding record in (3)

   ii. A proposal concerning the mitigating measures to be adopted in case the findings are such that they might cause the project to be discontinued.

   iii. If the incidental finding includes any information of public interest, the bodies mentioned in (2) will decide on the, means and timing of their communication to other relevant stakeholders.

[The incidental findings policy was approved by the members of SYSTEM Security Advisory Board on the 25/03/2021]

Figure 6 Incidental Findings Policy

7.2. Approval of the Security Advisory Board

The version of the incidental findings policy in § 7.1 has been approved by the Security Advisory Board members (FORMIT, BKA, CFLP, Min.Difesa-Carabinieri, NAKA-NCA-PPZ, RESI and VUB) through a statement.

Statement on the Incidental Finding Policy of the Project

I, Giampiero Gasperini, as representative of FORMIT, member of the Security Advisory Board,

hereby declare to,

acknowledge that the version of the Incidental Finding Policy for the SYSTEM project (Grant Agreement n. 787128) is available in Deliverable 10.4: Legal and Ethical Support Package elaborated by Vrije Universiteit Brussels (VUB).

acknowledge and approve the implementation of the Incidental Finding Policy as detailed in the document "Handling incidental findings" (included in D10.4), for the research activities performed in SYSTEM.

Rome, 25/03/2021

Fondazione Formit

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

Figure 7 Statement of approval - FORMIT

Statement on the Incidental Finding Policy of the Project

I, Pütz, Michael, as representative of Bundeskriminalamt (BKA), member of the Security Advisory Board,

hereby declare to,

acknowledge that the version of the Incidental Finding Policy for the SYSTEM project (Grant Agreement n. 787128) is available in Deliverable 10.4: Legal and Ethical Support Package elaborated by Vrije Universiteit Brussels (VUB).

Wiesbaden, 11/03/2021

(Signature)

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

Figure 8 Statement of approval – BKA

Statement on the Incidental Finding Policy of the Project

I, Anna Trynda, as representative of Central Forensic Laboratory of the Police, member of the Security Advisory Board,

hereby declare to,

acknowledge that the version of the Incidental Finding Policy for the SYSTEM project (Grant Agreement n. 787128) is available in Deliverable 10.4: Legal and Ethical Support Package elaborated by Vrije Universiteit Brussels (VUB).

acknowledge and approve the implementation of the Incidental Finding Policy as detailed in the document "Handling incidental findings" (included in D10.4), for the research activities performed in SYSTEM.

Warsaw, 25/03/2021

(Signature)

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

Figure 9 Statement of approval – CFLP

Statement on the Incidental Finding Policy of the Project

I, Ten.Col. ADOLFO GREGORI, as representative of RACIS , member of the Security Advisory Board,

hereby declare to,

acknowledge and approve the implementation of the Incidental Finding Policy as detailed in the document "Handling incidental findings" (included in D10.4), for the research activities performed in SYSTEM.

Rome, 25/03/2021

IL COMANDANTE
(Ten. Col. inæsc. Adolfo Gregori)

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

Figure 10 Statement of approval - Min.Difesa_Carabinieri

MINISTERSTVO VNÚTRA SR
Prezídium Policajného zboru
národná kriminálna agentúra
protidrogová centrála
Pribinova 2
812 72 Bratislava
- 1 -

SYSTEM

Statement on the Incidental Finding Policy of the Project

I, Leonard Grunský, as representative of National Crime Agency of the Presidium of the Police Force, Slovakia, member of the Security Advisory Board,

hereby declare to,

acknowledge that the version of the Incidental Finding Policy for the SYSTEM project (Grant Agreement n. 787128) is available in Deliverable 10.4: Legal and Ethical Support Package elaborated by Vrije Universiteit Brussels (VUB).

acknowledge and approve the implementation of the Incidental Finding Policy as detailed in the document "Handling incidental findings" (included in D10.4), for the research activities performed in SYSTEM.

BRATISLAVA, 22/03/2021

Ministerstvo vnútra Slovenskej republiky
868

(Signature)

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

Figure 11 Statement of approval - NCA-NAKA

Statement on the Incidental Finding Policy of the Project

I, CLAUDIO ROMANI, as representative of RESI INFORMATICA S.p.A., member of the Security Advisory Board,

hereby declare to,

acknowledge that the version of the Incidental Finding Policy for the SYSTEM project (Grant Agreement n. 787128) is available in Deliverable 10.4: Legal and Ethical Support Package elaborated by Vrije Universiteit Brussels (VUB).

acknowledge and approve the implementation of the Incidental Finding Policy as detailed in the document "Handling incidental findings" (included in D10.4), for the research activities performed in SYSTEM.

PLACE, 29/03/2021

RESI Informatica S.p.A.
Via Pontina Km 44,044
04011 APRILIA - ITALY
VAT 05633751002

(Signature)

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

Figure 12 Statement of approval - RESI

Statement on the Incidental Finding Policy of the Project

I, Sergi Vazquez Maymir, as representative of Vrije Universiteit Brussels, member of the Security Advisory Board,

hereby declare to,

acknowledge that the version of the Incidental Finding Policy for the SYSTEM project (Grant Agreement n. 787128) is available in Deliverable 10.4: Legal and Ethical Support Package elaborated by Vrije Universiteit Brussels (VUB).

acknowledge and approve the implementation of the Incidental Finding Policy as detailed in the document "Handling incidental findings" (included in D10.4), for the research activities performed in SYSTEM.

Brussels, 25/03/2021

(Signature)

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

Figure 13 Statement of approval - VUB

8. Information To Be Provided To Participants In Tests Or Demonstrations

The SYSTEM project and Consortium attach great importance to the ethical conduct of research. A precondition for this is that information about tests and demonstrations is provided to human participants involved in therein, in an accurate and clear fashion. This information sheet contains information with a public dissemination level to be provided to any human participants directly involved in SYSTEM tests or demonstrations, including information concerning the processing of personal data relating to them.

INFORMATION TO BE PROVIDED TO PARTICIPANTS

Prior to any involvement in the testing, workers and their representatives, as well as personnel will be informed of:

1. The research purpose of the project SYSTEM: e.g., SYSTEM attempts to develop a network of sensing devices to support the detection of illegal production of explosives and drugs. For that purpose, networks of sensing devices need to be tested across different urban areas, and their data will be fused into the SYSTEM monitoring centre.
2. The purpose of the tests and demonstrations;
3. An explanation of how research venues, e.g., monitored buildings or blocks, were selected;
4. Expected duration of the experiment/pilot, and number of participants;
5. The right to ask any questions;
6. The incidental findings policy, detailing what happens if something suspicious is detected;
7. The possibility to opt out.
8. A statement saying whether personal data will be collected, and which types of data will be collected (e.g., only non-personal data from the sewage system);
9. A description, in lay terms, of the; purpose of collection for the data
10. A description, in lay terms, of the methods of data collection and processing
11. A statement concerning the sharing of the data, which will be available only to the members of the SYSTEM Research Consortium. [if possible , pls identify which partners within the consortium, will have access to this information;
12. A statement ensuring specifically that data will be used only for the purpose related to the project and will not be used to take any measures that affect the rights of participants;
13. A statement about the right to ask any questions and the contact details of the person or persons who should address such questions (name, surname, his/her email address and functioning telephone number).
14. A statement concerning the retention period of the data collected and A simple description of the measures that will be adopted to ensure that data are kept securely;
15. The incidental findings policy detailing what would happens if something suspicious is detected;
16. A statement that data will be processed in line with European and national data protection law (to be defined for each jurisdiction).

Figure 14 Information To Be Provided To Participants In Tests Or Demonstrations

9. Consent Form For Participation In Research

When required by the law, together with the relevant information sheet associated with the test or demonstration, human participants will be asked to sign the following consent form:

CONSENT FORM

"I, undersigned [name] [date and place of birth], hereby give my consent to take part in the research carried out by the SYSTEM Consortium.

I have been informed that the SYSTEM project is a research project currently run under the Horizon 2020 Framework Programme under the grant agreement no. 787128.

I have been informed about the purposes of this demonstration, which consists in [describe in short]. I have had all my questions answered to my satisfaction.

I have been informed that information obtained during the research will be used for [describe in detail]. Personal data or data that may reaveal aspects fo my person will be made available only to the members of the SYSTEM Consortium.

I have been informed that I am free to withdraw my consent and discontinue my participation at any time without any negative consequences.

I can also request the deletion of any personal data that may pertain to me. Such a request may be made without any consequences.

I have been informed that I can also address any questions or concerns arising from this research to:
[name and surname]
[contcat details]

[I require my participation remains anonymous, i.e. all possible efforts would be made to prevent the identification of myself and I will not be identified in any research results.]

I give this consent fully informed, freely and voluntarily.

Participant Signature: ....
Name: ....   Date: ....
I confirm, for the project team, my agreement to participate in this research study.

Researcher Signature: ....
Name: ....   Date: ....
Organisation: ....

Done in two copies, of which one is for the SYSTEM Consortium and one for the participant

Done at [place] on [date]

Figure 15 Consent Form For Participation In Research

10. Registry Of Personal Data Processing Activities

European privacy and data protection legislation (the General Data Protection Regulation, or GDPR, art. 30), demands that records are kept of all the processing activities of personal data. This questionnaire will be used to enable each partner to assess whether personal data are processed during the project activities. This assessment is necessary to plan a robust and adequate framework of safeguards and checks.

Registry of personal data processing activities

Partner details	
Related WP and Task	

Am I using 'personal data'?

Information is considered 'personal data' whenever it relates to a living, *"identified or identifiable natural person"*.

These include identifiers such as a name, address, telephone number, photograph, voice recording, social security number, an internal reference number, license plate, location data, online identifiers such as an IP-address etc.

Please be aware of the fact that this question regarding personal data has to be asked on an aggregate level. Even when certain types of data may not lead to a person being identified directly, as would be the case with names or biometric data, the question still must be asked whether individuals are *identifiable* using this information.

Am I 'processing' processing data?

You are 'processing' personal data whenever you perform an operation or a set of operations on the data set, which, in the GDPR, is defined extremely broad. Operations such as collecting, consulting, structuring, storing, using, moving, or removing of data, whether or not by automated means, are all considered 'processing' of personal data.

If you **process personal data** as a part of your activities within the consortium of SYSTEM, you must file these processing activities in this document and keep it on file.

CHECKLIST

In order to comply with this privacy legislation, the following information is needed on every processing of personal data:

1. Reason for processing the data: fill in your part in the SYSTEM Consortium, specific process, using personal data that you are responsible for, and within which WP of the project)
2. Who is the controller? (The controller is whoever determines the purposes and means of the processing of personal data. This is a difficult question that VUB will probably answer)
3. Who is the processor? (This is a question that VUB will probably answer for you)
    - Name and contact details of the person working at the processing service/department…
4. Who is procedurally responsible? (Who carries out the processing?)
    - Name of the service/department that is responsible for the processing
5. In which information system is the processing executed?
    - Name of the information system
    - Location of data storage
6. What are the purposes of the processing?
7. Is the personal data an existing dataset?
    - Did you ask consent for further use? (provide form)
    - Did you inform the data subject of the further use? (Provide privacy policy)
8. What is the scale of the processing?
    - Processing on large or small scale? (give approximate number of personal data)
9. Will you anonymize the data? Y/N
    - If no, why not?
    - If yes, when and how?
10. Will you pseudonymize the data? Y/N
    - If no, why not?
    - If yes, how?
11. What will be the security measures? (i.e. encryption and how, logging and how…)….
12. Whose personal data is being processed?
    - Indicate whether or not personal data of vulnerable persons is being processed (e.g. children below the age of 16, patients, your own students, own employees, specific target group/possible stigmatization)
13. What categories of information are being processed?
    - Mark the relevant categories and feel free to add further specifications (i.e. genetic information)

A. Identification data
B. Financial information
C. Personal features
D. Data on physical properties
E. Habits
F. Mental health
G. Family composition
H. Hobbies and interests
I. Memberships
J. Judicial records
K. Consumption patterns and habits
L. Residence and the home
M. Information regarding health
N. Education
O. Occupation and employment
P. Social security numbers
Q. Racial or ethnic background
R. Information on sexual preferences or behavior
S. Political orientation or opinion
T. Membership of trade union or affiliation
U. Philosophical or spiritual orientation
V. Video footage
W. Audio records
Z. Other, namely:

14. What is the data retention period? Why?
15. What is the legal basis for the processing activity (choose one of these options that applies)? (VUB will verify this)
    - **Obligation laid down by law:** there is a law or stature that obliges the personal data to be processed - which law (link to law in English/French/Dutch/German)?
    - **Contract**: the processing of personal data is warranted by a contractual relationship – provide the contract?
    - **Consent**: the data subject has explicitly consented to the processing of his or her personal data - provide consent form
    - **Vital interest of the data subject**: the processing is necessary to protect the vital interests of the data subject
    - **Legitimate interests**: processing is necessary for the purposes of the legitimate interests of the controller (or a third party): Why?
    - processing is necessary for the performance of a task carried out in the **public interest** or **in the exercise of official authority** vested in the controller: Why? And what law gives your institution this public task?
16. What other partners/institutions is the personal data shared with (in and out of consortium)?
    - Name of the institutions
    - Is this information being shared with partners/institutions outside EU?

Remarks: Please feel free to provide additional clarification, commentary, or remarks regarding the filing of this processing activity

Figure 16 Registry of personal data processing activities

11. Confidentiality Statement For Researchers Directly Involved With Research Participants And Personal Data

Researchers themselves can be source of privacy violation if they carelessly treat or disclose personal information acquired in the course of research activities involving human participants and data subjects. For this reason, it is recommended that researchers in SYSTEM who will process personal information will sign a Confidentiality Statement specifying that the said data will be used only for specific purposes related to the project and will not be used to take any measures that affect the right of workers to privacy in the workplace.

Confidentiality statement

"I, undersigned ("Researcher"), [name] [institution] [contact details], agree to the following:

1. The sole purpose of acquiring, storing, using or in any other way processing data acquired during the demonstration is scientific research.
2. Data collected during the demonstration will be used for the purpose of the Project and will not be made publicly available or accessible in any way outside the Consortium.
3. Any information I receive in the context of the project, I will treat as confidential and I will not disclose it to anybody outside the project.
4. Only the analysis results on the dataset can be published, observing relevant privacy and data protection laws, if applicable, and citing the name of the organization providing the data for the project purposes.
5. The relevant laws of [country] shall apply.

Done in two copies, of which one is for the SYSTEM researcher and one for the person involved in the research.

Done at [place] on [date].
Signature "

[this form wll be sumbitted to teh Security Advisory Board for approval]

Figure 17 Confidentiality statement

12. National Data Protection Authorities

The research will collect aggregate data from sensors placed in sewage systems, solid waste, and urban air. As stated in the ethics self-assessment, the project will not, nor does it intend to, collect personal identifiable data. However, the self-assessment has recognized that monitoring through the sensors can link the data to identifiable persons and create the conditions for covert surveillance. For this reason, the consortium has identified the relevant Data Protection Authorities in the four countries in which the pilot demonstration will take place. The conditions under which the obligation to enter into contact with these authorities arise are defined in national and EU law with regards to data protection measures.

COUNTRY	Data Protection Legislation and authority
Germany	German Bundesdatenschutzgesetz (BDSG) or the Federal data protection act and the guidelines and the opinions of the Bavarian Data Protection Authority. https://www.lda.bayern.de/en/index.html In Bavaria, where SYSTEM plans to carry out tests and demonstrations, the data protection supervising authority is the BayLDA. With regard to data protection laws in the public sector this falls under the jurisdiction the State Commissioner on Data Protection, Dr. Thomas Petri. He is responsible for Bavarian public sector entities, e.g. state entities, municipalities and local governments. https://www.lda.bayern.de/en/index.html
Slovak Republic	Act No. 122/2013 Coll. on Protection of Personal Data and on Changing and Amending of other acts, resulting from amendments and additions executed by the Act. No. 84/2014 Coll and the guidelines and the opinions of the Office for Personal Data Protection of the Slovak Republic. https://dataprotection.gov.sk/uoou/en
Poland	The Act of 10 May 2018 on the Protection of Personal Data and the guidelines and the opinions of the supervisory authority for the protection of personal data in Poland is the Inspector General for Personal Data Protection (Polish abbreviation: GIODO). http://www.giodo.gov.pl
Italy	Law No. 675 of 31 December 1996) and regulated subsequently by the Personal Data Protection Code (Legislative Decree No. 196 of 30 June 2003) as amended by Legislative Decree No. 101 of 10 August 2018, which also established that the Italian DPA is the supervisory authority responsible for monitoring application of the General Data Protection Regulation (pursuant to Article 51 of Regulation No. 2016/679. http://www.garanteprivacy.it
The Netherlands	The General Data Protection Regulation (GDPR or Algemene Verordening Gegevensbescherming (AVG) in Dutch) has replaced the Dutch Data Protection Act (Wet bescherming persoonsgegevens,Wbp). https://autoriteitpersoonsgegevens.nl/en Te Dutch Data Protection Authority (Dutch DPA) contact details are to be found in its site(https://www.autoriteitpersoonsgegevens.nl/en/contact-dutch-dpa/contact-us)

Table 1 National Data Protection Authorities

13. National Licenses Offices Ex. Regulation (Ec) No 428/2009

The SYSTEM technology is unlikely to have dual use potential as it will be developed with the aim to work in urban environments. However, dual use risks of sensors, and of drones in particular, need to be monitored (Reg. 428/2009 (2017 Consolidated Version). Transactions involving such dual-use items are in fact subject to certain restrictions, which may affect the research project.

The following authorities have been identified as contact points to ensure that dual-use items, if so classified, can be moved across countries.

Country	Licensing Office	Web site on export of dual use items
Germany	Federal Office of Economics and Export Control (Bundesamt für Wirtschaft und Ausfuhrkontrolle) Frankfurter Strasse 29-35 65760 Eschborn GERMANY Tel. +49 6196908-0 Fax +49 6196908-900 E-mail: ausfuhrkontrolle@bafa.bund.de	http://www.ausfuhrkontrolle.info
Poland	Minister for Economy Plac Trzech Krzyży 3/5 00-950 Warszawa POLAND Tel. +48 226935171 Fax +48 226934033 E-mail: sekretariatDKE@mg.gov.pl	www.mg.gov.pl/Gospodarka/DKE, www.mg.gov.pl/DKE/EN

Source: http://trade.ec.europa.eu/doclib/docs/2011/july/tradoc_148094.pdf

Table 2 National Licenses Offices Ex. Regulation (Ec) No 428/2009