Grant Agreement No.: 732078
Call: H2020-ICT-2016-2017

Topic: IOT-02-2016 – IoT Horizontal Activities
Type of action: CSA

D3.1: Ethics and Privacy Implementation Plan

Work package	3
Task	/
Due date	30/06/2017
Submission date	30/06/2017
Deliverable lead	LTU
Authors	All partners
Reviewers	Breuer, Jonas (imec) Scudiero, Lucio (Archimede Solutions) Annicchino, Pasquale (Mandat International)

Abstract	The Ethics and Privacy Implementation Plan lays down the practical guidelines that will be adhered to in the U4IoT support action. It provides necessary background information, discusses each task and its specific issues separately, and defines the general U4IoT implementation plan, complemented by templates such as for informed consent.
Keywords	User Engagement, Ethics, Privacy

Document Revision History

Version	Date	Description of change	List of contributor(s)
V0.1	27/04/2017	ToC, first input	LTU
V0.2	19/06/2017	Input of all task leaders concerning their tasks	All task leaders
V0.3	23/06/2017	Formatting and review	LTU
V0.4	27/06/2017	Internal review	imec
V.0.5	27/06/2017	Internal Review	Mandat International/Archimede Solutions
V0.6	28/06/17	Final check	Martel
V1.0	29/06/17	Submission	LTU

Disclaimer

Copyright notice

Acknowledgment

This deliverable has been written in the context of a Horizon 2020 European research project, which is co-funded by the European Commission and the Swiss State Secretariat for Education, Research and Innovation.

Co-funded by the European Union

Co-funded by the Swiss Confederation

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**Report**	
Dissemination Level		
PU	**Public, fully open, e.g. web**	☐
CI	**Classified, information as referred to in Commission Decision**	
CO	**Confidential to U4IoT project and Commission Services**	

EXECUTIVE SUMMARY

U4IoT is a CSA that supports the LSPs with user engagement by combining expertise in areas such as crowdsourcing, living labs, co-creative workshops, meetups and personal data protection to actively engage end-users and citizens in large scale pilots.

Also as a support action, U4IoT involves the collection, aggregation, storage, use, disclosure (and ultimately destruction) of data, which inevitably gives rise to privacy and security concerns.

As requested by the European Commission, U4Iot composed this concise and practical *Ethics and Privacy Implementation plan* to draw out and remedy the potential privacy and ethic related risks. It outlines how U4IoT will implement processes for ethics and privacy which include e.g. informed consent procedures for the participation of humans, on the procedures that will be implemented for data collection, storage, protection, retention and destruction and confirmation that they comply with national and EU legislation.

General concepts and aspects relating to ethics and privacy in user engagement and related research are presented, as well as related definition and applicable EU laws and norms.

In addition, each task of U4IoT is discussed regarding its specific ethics and privacy issues, or why it has none. Measures to remedy the specific issues are defined in direct relation. This is complemented by general rules and guidelines that will lead and inform all work conducted within the U4IoT project. These are in line with relevant legislation and include data minimisation, the installation of a Personal Data Protection Officer, defined duration of data retention, informed consent and other fundamental data protection principles.

Templates of the informed consent forms and information details on security measures to protect participants' personal data from security threats, misuse or dual use and confirm that the ethical standards and guidelines of Horizon2020 will be rigorously applied.

TABLE OF CONTENTS

1 INTRODUCTION

U4IoT supports the IoT LSPs in their user engagement processes by combining expertise in areas such as crowdsourcing, living labs, co-creative workshops, meetups and personal data protection to actively engage end-users and citizens in large scale pilots. In order to achieve this objective, U4IoT will: develop toolkit for LSPs end-user engagement; directly support to mobilize end-users; analyse ethical, societal and ecological issues and adoption barriers related to the pilots with end-users; support communication, knowledge sharing and dissemination with an online portal and interactive knowledge base gathering lessons learned.

Projects that involve the collection, aggregation, storage, use, disclosure (and ultimately destruction) of data inevitably give rise to privacy and security concerns. In fact, the cumulative effect of many such initiatives might even harm public trust and the reputations of corporations and government institutions alike.

This deliverable was requested by the European Commission. All task leaders had to consider the privacy and ethical issues related to their tasks for it. Where appropriate, measures specific to a task's issues are listed in addition to the general policy that is stipulated here in the following.

1.1 Purpose of this Deliverable

The objective for this *Deliverable D3.1 Ethics and Privacy Implementation Plan* is to draw out and remedy the potential privacy and ethic related risks.

The deliverable will outline how U4IoT will implement processes for ethics and privacy which include e.g. informed consent procedures for the participation of humans, on the procedures that will be implemented for data collection, storage, protection, retention and destruction and confirmation that they comply with national and EU legislation. Templates of the informed consent forms and information details on security measures to protect participants' personal data from security threats, misuse or dual use and confirm that the ethical standards and guidelines of Horizon2020 will be rigorously applied, in all the country in which the research is carried out.

1.2 Structure of this Deliverable

This deliverable is structured as follows. It starts with setting the scene of a general perspective on ethics and privacy in user engagement and related research. The following chapter is dedicated to the specific ethics and privacy issues in each work package and/or task. It is structured accordingly. Chapter 4 then presents the Ethics and Privacy Implementation Plan that guides our work throughout the U4IoT project. Several annexes include templates for the measures foreseen in the plan.

2 ETHICS AND PRIVACY IN USER ENGAGEMENT

In the following section, we will present an overview of the privacy and ethical frameworks that underlie this project's policy. We will give an overview of the area of privacy and also of research ethics that are important to consider in this context.

2.1 Ethics and User Engagement

There are different types of research, one can for instance distinguish between research that tries to explain why something has happened by showing that it can be subsumed under a natural law, and research that tries to increase and deepen our knowledge about events, processes or texts.

From a research ethics perspective, another distinction is interesting. One usually separates between three forms of research, basic, applied and commissioned. Basic research entails that the researcher seeks new knowledge without a certain application in mind. Applied and commissioned research both have a decided aim. The goal of these two types is to be of use to the party who has initiated or ordered the researcher. Here, commissioned research can be seen as being more directly and clearly driven by the commissioning party than applied research is. Research also entails a systematic search for knowledge. This knowledge should be new, and not simply compile what we already know, unless the aim is to confirm previous research results.

Scientific research is an important element of society to make sense of the world and to be able to explain and understand it. However, history has shown that the intended reasons for researching sometimes do not coincide with its actual effects. Research that can make it possible to develop new, faster processes can also have undesired and unexpected effects or be used for negative purposes by others. The challenge is thus to optimize the possibilities to use the positive effect of research and to minimize the negative ones. Hence, a lively ethical discourse is an important element of these attempts.

In the U4IoT project, the aim is to understand the potential effects of the LSPs by analysing the societal, ethical and ecological issues related to IoT implementations. To gain deep insights into this matter, interviews, workshops and discussion with LSP representatives will be performed following the plan developed in this document.

A central question in all scientific studies concerns the relationship between the research question and the method applied to investigate the question. Here it is important to balance between risk and benefit of the research being carried out. This always starts as a negative value, since research requires efforts from participants in terms of time and some kind of risks, even though it might be minimal. When designing a study, it is important to choose a method with the least imaginable harmful consequences on the stakeholders involved.

Regarding how the research should be performed and who has the responsibility for it being carried out in a scientifically and ethically satisfactory way, it can be helpful to distinguish between the responsibilities between the individual researcher, the project leader, the department head and the head of research. In certain types of research, the responsibility of the funding institution is also relevant to consider.

For the individual researcher, it is important to consider the research question. Here, those responsible for the academic merit system should give the right signals so that a researcher can avoid the temptation of defining his or her research based more on the merit possibilities than on the importance of the research question.

Hence, in research one must, in a reasonable way, compare the importance of many types of interests – all of which are legitimate but in some situations, can conflict with each other: the researcher's interest in obtaining new knowledge, the interest of participants and those affected by the research to have their integrity and private life protected. How this weighing

of interests is done depends on aspects including what type of research is being conducted. But in any type of research, the collected material is not the private property of the researcher or research group, something they own and can do with as they wish. It must be stored and archived according to the general regulations issued by the various authorities.

Four important concepts in the debate that are sometimes confused with each other or used synonymously are *secrecy, professional secrecy, anonymity, pseudonymity* and *confidentiality*.

Information can be covered by *secrecy* only if it is defined as such by an applicable law. Standards for *professional secrecy* apply to some professions through law as well as ethical rules. *Anonymizing* or de-identifying involves eliminating the connection between samples or questionnaire answers and a certain individual so that neither unauthorized individuals nor the research group can re-establish it; thus, for example, no one should be able to combine a certain piece of information with a specific person's identity. The code list is destroyed.

Anonymity can also be achieved by collecting material without noting specific individuals' identity. *Pseudonymity* is defined by Regulation 679/2016 (hereinafter the "*GDPR*") as the result of the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Confidentiality entails protection from unauthorized individuals gaining access to the information, but the research group can use code keys to associate information or samples with specific individuals. The question of who is and is not authorized, however, is not something for the researcher to ultimately determine.

The Declaration of Helsinki puts emphasis on the importance that researchers must take measures to protect research subjects´ integrity and right to protect their private life. In Article 23 of the Declaration from 2008 this is expressed as *"Every precaution must be taken to protect the privacy of the research subjects and the confidentiality of their personal information and to minimize the impact of the study on their physical, mental and social integrity".*

Important to keep in mind here is that no researcher can promise that no one outside a research group will ever have access to the material or information being collected. There might emerge situations in which access to research material is justified and necessary. For instance, an opponent requesting access to the basic data, or other researchers wanting to test the strength of the scientific results. It is also in the interest of the society that collected material can be used as much as possible in research. For this to be possible, it requires that the new research project is ethically reviewed and that the new researchers adopt the previous researchers´ promise of confidentiality and safe storage of material.

In addition, the landscape of research ethics is dynamic and lively. When researchers ask new questions, or use new methods and tools, new research ethics issues arise. When using methods such as questionnaires and interviews, the requirement that the participants´ identities are protected is met through the use of code keys and by masking and anonymizing their answers. However, this is not possible when using, for instance, video recordings. In the U4IoT project, we will not use methods such as video recordings or participant observations, hence keeping the participants' personal identity protected is less challenging.

2.2 Privacy and User Engagement

"Privacy (from Latin: privatus "separated from the rest, deprived of something, esp. office, participation in the government", from privo "to deprive") is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively."

Other related relevant definitions are:

Personal information: Information that identifies a person or can be used in conjunction with other information to identify a person

Private information: Information that an individual would prefer not be known to the public because of its intimate nature.

Privacy: is one´s ability to control information about oneself (Bélanger & Crossler, 2011). Four dimensions of privacy has been identified: privacy of a person; personal behaviour privacy; personal communication privacy; personal data privacy.

Privacy is thought of as a human right that can be seen from both a moral and legal perspective. In general, definitional approaches to privacy, found in various disciplines, can according to Smith et al. (2011), be classified as either value-based or cognate-based. Here the value-based perspective refers to general privacy as a human right that is vital to the moral value system in the society and this is the first definition of general privacy.

However, when the privacy as a human right perspective was related to consumer behaviour, a privacy paradox was discovered. This is expressed as even though consumers have privacy concerns, they still readily share personal information in various situations. Based on that, the privacy as a commodity was conceptualized. In this perspective, privacy is still an individual and societal value, but it can be given an economic value which can be considered in a privacy calculus of costs and benefits (Smith et al., 2011).

For example, many consumers seem to feel that a reduced price of a product is a fair exchange for the data collected (Hough, 2009). The cognate-based conceptualization of general privacy relates to the individual's mind, perception, and cognition rather than to an absolute moral value or norm. This means that privacy can be viewed as state and/or as control of physical space and information. Adding to these dimensions of privacy, another set of types of privacy has been identified by Pedersen (1999).

These types are "intimacy with family (being alone with family), intimacy with friends (being alone with friends), solitude (freedom from observation by others), isolation (being geographically removed from and free from observation by others), anonymity (being seen not identified or identifiable by others), and reserve (not revealing personal aspects of one's self to others)" (Pedersen, 1999 p. 398).

The European Union has adopted two major treaties containing legal obligations related to privacy: the Charter of Fundamental Rights of the European Union adopted in 2000 and the Treaty of Lisbon. Those two texts focus more on the protection of personal data, which require:

- The consent of the persons concerned
- The right to access and to rectify collected data
- The control of an independent authority

2.2.1 Charter of Fundamental Rights of the European Union, 2000[1]

Article 7 "Respect for private and family life": Everyone has the right to respect for his or her private and family life, home and communications.

Article 8 "Protection of personal data": 1. Everyone has the right to the protection of personal data concerning him or her; 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified; 3. Compliance with these rules shall be subject to control

[1] Entry into force: Dec 7, 2000

by an independent authority."

2.2.2 Lisbon Treaty[2]

It is also worth mentioning that the Lisbon Treaty, which states that the European Union has its foundations in the amended Treaty on the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) which together with the Charter for Fundamental Rights complete the institutional and constitutional European legal framework, and in so doing they provide EU institutions with a legal basis to adopt data protection rules.

Accordingly**, Article 16 TFEU** states that: "Everyone has the right to the protection of personal data concerning them. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities [...]".

2.2.3 European Union – secondary norms

2.2.3.1 DIRECTIVE 95/46/EC[3]

This Directive applies to data processed by automated means (e.g. a computer database of customers) and data contained in or intended to be part of non-automated filing systems (traditional paper files). These legal requirements will be supplemented with the changes reflected in the GDPR, which will have to be taken into account in May 2018.

The Directive **aims to protect the rights and freedoms of persons** with respect to the processing of personal data by laying down guidelines determining when this processing is lawful. The guidelines relate to:

Data minimization, meaning that the processing of personal data must be the least intrusive possible, and that only personal data that are necessary for the envisaged purposes shall be collected and processed;

Quality of the data: personal data must be processed fairly and lawfully, and collected for specified, explicit and legitimate purposes. They must also be accurate and, where necessary, kept up to date.

Legitimacy of data processing: personal data may be processed only if the data subject has unambiguously given his/her consent or processing is necessary or if another legal basis apply:

- for the performance of a contract to which the data subject is party or;
- for compliance with a legal obligation to which the controller is subject or;
- in order to protect the vital interests of the data subject or;
- for the performance of a task carried out in the public interest or;
- for the purposes of the legitimate interests pursued by the controller. (art. 8)

Information to be given to the data subject: the controller must provide the data subject from whom data are collected with certain information relating to himself/herself (the identity of the controller, the purposes of the processing, recipients of the data etc.) (art. 10).

[2] Entry into force: December 1 2009

[3] Entry into force: Oct 25 1995

Right of access to data of data subject: every data subject should have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information relating to the purpose of processing, the identity of the controller, the third parties to which data are disclosed etc. (art. 12)

Right to object to the processing of data: the data subject should have the right to object, on legitimate grounds, to the processing of data relating to him/her. (art. 14)

The confidentiality and security of processing: any person acting under the authority of the controller or of the processor, including the processor himself, who has access to personal data must not process them except on instructions from the controller (art. 15 and 16)

Notification of processing to a supervisory authority: the controller must notify the national supervisory authority before carrying out any processing operation" (art. 18)

Special categories of data (so-called "sensitive personal data"): data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership" and "health or sex-life" can only be processed in exceptional circumstances (art. 8).

2.2.3.2 General Data Protection Regulation (GDPR)[4]

Following Article 16 TFEU, which is the legal basis for the adoption of data protection rules in the EU, the European Union legislator adopted the General Data Protection Regulation. The aim of the GDPR is to protect the fundamental right to data protection and to guarantee the free flow of personal data between Member States. The logic of the adoption of a GDPR was to prevent disparities between Member States in terms of procedures and sanctions, harmonizing the data protection in the EU.

The GDPR strengthens the data protection legal framework in the EU, by means of the following novelties:

1. The GDPR applies to the **processing of personal data wholly or partly by automated means** and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
2. The GDPR have an **extra-territorial reach**, meaning that its rules apply not only to controllers or processors established in the European Union, but also to entities having their establishment in a third country, if they:
    a. Offer goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the Union (e.g. a US-based social network); or
    b. Monitor the data subjects' behavior, as far as their behavior takes place within the Union (e.g. email tracking service providers)
3. **Consent should be free, unambiguous, informed, prior and demonstrable by the data controller**, meaning that it must be documented somehow (also electronically, e.g. by means of a log).
4. In any event, **data subjects must be informed** about the processing undergone by their personal data before the processing starts or, when data are not collected from the data subjects themselves, within a reasonable period, in any event no later than the first communication or the first disclosure to the public, when such activities are

[4] Regulation (EU) 2016/679

foreseen.

5. **Data protection principles** (*ie* data minimization, purpose limitation, data accuracy, storage limitation etc.) **must always be respected**; a data controller may have a legal ground to process personal data (e.g. the data subject's consent), yet it may still run the processing in breach of one of the key data protection principles, which would make the personal data processing unlawful and, potentially, trigger a sanction by competent authorities. This is the essence of the principle of **accountability**.
6. The principle of **data protection-by-design is now set in law.** It requires the controller to implement "*technical and organizational measures appropriate to the processing activity being carried out and its objectives, such as data minimization and pseudonymisation, in such a way that the processing will meet the requirements of* [the] *Regulation and protect the rights of (...) data subjects*";
7. Same goes for the principle of **data protection-by-default**, that refers to the amount of data collected, retention period, extent of the processing, data accessibility etc. Essentially, "*the controller shall implement appropriate measures for ensuring that, by default, only (...) personal data (...) which are necessary for each specific purpose of the processing are processed*".
8. Procedures to handle and notify **Data Breaches** to Data Protection Authorities and Data Subjects concerned must be in place.
9. A **Data Protection Officer** (DPO) shall be appointed in certain case provided for by law (e.g by Public Sector and by private entities carrying out risky processing activities on a large scale)

3 ETHICS AND PRIVACY IN U4IOT

The following section describes the potential ethics and privacy issues per work package and task if applicable. As not all tasks deal with the engagement of users, not all deal with such issues in the same way, or might not have to deal with it at all. Where applicable, the task leaders add concrete measures to be implemented as they deem necessary for conducting their concrete tasks.

3.1 WP1 End-user Engagement Toolkit

3.1.1 T1.1 End-User Engagement Toolkit

3.1.1.1 Privacy

Concerning the first deliverable of T1.1, the privacy issues are not taken into account in the first release of the toolkit (D1.1 with methods and tools on end-user engagement), as only a set of tools is provided to be used by use cases of LSP projects and any possible privacy issues are to be handled by the people using the tools.

At the later stage the toolkit will be completed with the outcomes of T1.3 with guidelines, resources and a game on personal data protection in Internet of Things deployments.

In planning the toolkit's first release as well as in later in collecting feedback about the services, questionnaires, interviews and surveys have and will be used in order to collect information from LSP projects. The process and measures are explained more in detail in section concerning WP2, as this contact to LSP projects is mainly done in collaboration between these two WPs.

In general, concerning the data collected, it is only used for information purposes project-internally, and any specific information of respondents will be anonymised for public deliverables of WP1.

3.1.1.2 Ethics

As WP1 provides a toolkit for the use of LSP projects, no ethical issues are foreseen for this activity. The usage of the different tools and methods provided might require some considerations of ethical issues, but this is not within the scope of WP1 activities.

3.1.2 T1.2 Crowdsourcing and survey tools

3.1.2.1 Privacy

This task will gather and customise crowdsourcing and survey tools for enabling LSPs to asses and monitor the end-user acceptance and perception of the pilots. The task leverages on the European IoT Lab platform of testbeds as a service and crowdsourcing tool. It will also select and provide access to resources developed by WP4, namely tools for collaboration, outreach and dissemination.

From a personal data protection point of view this tasks entails the potential collection of users's personal data and their sharing amongst providers of resources within the projects.

Measures

In order to perform such activities in compliance with applicable data protection law, certain safeguards will be applied.

First of all, collection of users' personal data will be avoided since the beginning; users' will not be required to provide personal details when assessing the LSPs, and their online navigation

data, which may be automatically collected by the LSPs, will be deleted after at short intervals so as to not store any potential personal information. Once the feedback from users is collected, it will be processed so as to provide interested stakeholders within the LSPs only with aggregated results and metrics of users' acceptance; personal data will therefore not appear in those reports. LSPs, by means of their coordinators, will have to enter into a data processing agreement, pursuant to Article 28 of GDPR and to APPENDIX D: SPECIFIC COMMITMENTS OF THE DATA PROFCESSORS, with:

- The entity responsible of the provision of the European IoT Lab platform of testbeds;
- DNET, as leader of WP4 in U4IoT.

The data processing agreement will be binding on the appointed entities (data processors) and will stipulate, at least, that the processor:

(a) processes the personal data only on documented instructions from the controller;

(b) ensures that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

(c) takes all security measures required by the GDPR, including when necessary pseudonymysation;

(d) does not engage another processor without written authorization by the controller;

(e) taking into account the nature of the processing, assists the controller by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;

(f) assists the controller in ensuring compliance with the security and breach-reporting obligations pursuant to the GDPR;

(g) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data;

(h) makes available to the controller all information necessary to demonstrate compliance with the obligations laid down in the contract and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

3.1.2.2 Ethics

Ethical issues in the context of this activity coincide with potential data protection issues, which will be tacked according to what has been explained above in section 3.1.2.1.

3.1.3 T1.3 Guidelines and game for privacy and personal data protection

3.1.3.1 Privacy

D.1.3. will develop some Privacy Guidelines and Game on Privacy whose aim is to raise awareness on privacy issues amongst the LSPs users. The only potential implication for personal data protection arising from this task derives from the fact that the game will be put online and require the users' interaction.

Measures

The web platform hosting the game will not require personal data to start it and will only serve technical, non-profiling cookies, to allow the functioning of the game. For these cookies users' consent will not be necessary, pursuant to Article 5(3) of Directive 2002/58/EC.

3.1.3.2 Ethics

There are not ethics implications for this task.

3.2 WP2 End-user Engagement Support

3.2.1 General Ethical and Privacy Issues in WP2

All support services in WP2 rely on information from a questionnaire and interviews. This information is therefore applicable to all the more in details described support services underneath.

Research on LSP needs concerning the support services provided in WP2 will be performed through a questionnaire and individual / group interviews.

Measures

The information that is collected through the questionnaire and interviews will only be stored, processed and distributed for project purposes. In general, there is no need to use personal data in order to draw conclusions on a project level. Respondents of the questionnaire (LSP partners) will be communicated to the U4IoT as contact person of the LSP projects. The data in the interviews will solely be used to inform the work within U4IoT and will be used anonymized for the deliverables of WP2.

3.2.2 T2.1 Co-Creative Workshop Support

Initially, research on LSP needs concerning Co-Creative Workshops will be performed through a questionnaire and individual/group interviews. Based on the results from these studies the support will be customized.

Workshops will be organized during the IoT Week in Geneva, LSP partners will be targeted, other participants of the workshops are attendees of the IoT Week in Geneva.

In coordination with the LSP projects facilitated Co-Creative Workshop trainings will be provided. Moreover, guided Co-Creative Workshop trainings will be provided. There is strived to have one facilitated and one guided workshop training per LSP project.

3.2.2.1 Privacy

The general issues mentioned above concerning the questionnaire and interviews are among others envisioned.

During a Co-Creative Workshops an extensive amount of data is gathered, in the form of notes, photographs, voice and video recordings. In general, there is no need to use personal data in order to complete the task objectives (D2.1). These data, however will be used to complete research report D2.3 and will be used for U4IoT promotion purposes. Possibly they will also be added to the knowledge base (WP4).

Also during the workshop trainings, an extensive amount of data will be gathered. Participants of these workshops are stakeholders, end-users and LSP partners. In this situation however, responsibility to treat the data gathered with care, lies with the LSP partners organizing the workshops.

Measures

The above described general measures concerning the questionnaire and interviews will be taken.

The information that is collected for T2.1 will only be stored, processed and distributed for project purposes. All people participating in the workshop will be asked for their informed

consent to use the data gathered in the form of photographs and video recordings to include in research reports and for U4IoT promotion purposes. Where possible any other personal data will be anonymized and used in the form of e.g. quotes, that can e.g. be included in research reports or in the U4IoT knowledge base.

In communication about the organization of the workshops, privacy and data protection issues will be raised, also during the hands-on training this will be communicated. Moreover, attention for this issue will be raised in deliverable D2.1: Co-Creative Methodology Handbook, also there a consent template will be included that can be used by the LSP projects to ask participants for their informed consent.

3.2.2.2 Ethics

Concerning the questionnaire and the interviews with the LSP partners, no ethical issues are expected.

Conflicts concerning intellectual property rights could however possibly arise between participants (stakeholders, end-users and LSP partner) who participated in the Co-Creative Workshops and who collaboratively co-created the resulting solutions.

For each of the workshops a representative selection of participants has to be invited to the workshops in order to draw relevant conclusions. Participants in general should be treated with care, and participants possibly belonging to a vulnerable population should be treated with extra care.

Measures

In the consent form a section concerning intellectual property rights will be included, stating that all solution co-created during a Co-Creative Workshop belong to the organizer of the workshop.

In deliverable D2.1: Co-Creative Methodology Handbook and the Co-Creative Workshop trainings, there will be promoted to select representative participants, to treat participants with respect and to take extra care of participants possibly belonging to a vulnerable population.

3.2.3 T2.2 Living Lab methodology support

The task T2.2 Living Lab methodology support will provide the LSP projects with a handbook to apply Living Lab methodologies in IoT pilots as well as advisory and support services to LSPs (through specialized webinars). Thus, the activities in this task are mainly about providing the projects with tools/methodologies and webinars.

3.2.3.1 Privacy and Ethics

In the planning of the activities, the general ethical and privacy issues for WP2 apply (described in section 3.2.1), concerning the communication and collaboration with LSP project partners. For the collection of feedback from LSP projects on the usage of the Living Lab handbook and the webinars, the information gathered will not include any personal data. In general, all the data gathered from the LSP projects for T2.2 is for project-internal use only and when reported in deliverables, will be handled confidential without revealing sensitive information. Any specific information of respondents will be anonymized for public deliverables related to inputs coming from T2.2 (related to measuring the performance).

3.2.4 T2.3 Online pool of experts for end-user engagement

This task consists of three different support services. In the following, they are explained

separately before the ethics and privacy issues are addressed for each of the support services.

Interactive Flow-Diagram

To develop the Interactive Flow-Diagram the following process will be followed. Research on LSP needs concerning the Interactive Flow-Diagram will be performed through a questionnaire. Based on these results, the interactive flow-diagram will be developed iteratively, by mapping the support provided by the partners of U4IoT and selecting relevant parameters. A card sorting test will be prepared and held with consortium partners. Based on the results of this exploratory test a static version of the flow-diagram will be designed and developed. This version will be evaluated and findings of this test will be incorporated in an interactive iteration of the flow-diagram. Finally, the interactive flow-diagram will be published online and performance will be measured. Findings will be documented in D2.3 and D2.4.

E-Courses

To develop the E-Courses, the efforts undertaken in other WPs during the progression of U4IoT will be inventoried and have to be documented, recorded and gathered to enable reuse. Research on e-support will be performed through a questionnaire and group interviews to elicit the needs of the LSPs and make a definite choice on the number, objective and content of the E-Courses. Moreover, currently available e-support approaches will be studied. Based on insights from these research efforts, the material created during U4Iot will be converted into E-Courses and example material. Performance will be measured and findings will be documented in D2.3 and D2.4.

Expert Pool

To develop the Expert Pool the following process will be followed. Research on LSP needs concerning the Expert Pool will be performed through a questionnaire. All partners will be requested to contribute to the potential list of experts, a selection will be made to invite to the expert pool. To contact the experts, templates with an invitation letter according to the expertise clusters will be made. Possible questions of the experts will be answered. When an expert confirms his/her interest, they will be asked for a short biography and one or more URLs to their work. Their name will be moved to a list with confirmed experts, the online expert pool based on this spreadsheet will be published on the U4IoT website. The online performance of the expert pool will from then on be monitored and evaluated. LSPs contacting experts from the expert pool outside of the LSP scope or for extensive consultancy moving beyond the initial scope of U4IoT and receiving advice through consultancy are themselves responsible for the payment of the fee charged by the consulted expert.

3.2.4.1 Privacy

Interactive Flow-Diagram;

The underlying research for the Interactive Flow-Diagram will be based on the questionnaire and interviews mentioned earlier. On this the WP2 general issues are envisioned.

Concerning the design and development of the Interactive Flow-Diagram, no issues are expected. Tests will mainly take place with members of the consortium. Possibly LSP partners will be invited to join in the last test phase. There is no need to use personal data in order to complete the task objectives, all data used to complete research reports D2.3 and D2.4 will be in an aggregated fashion.

To measure the KPI for WP2, the use of the Interactive Flow-Diagram will be monitored via the U4IoT website (that is part of the LSP-programme website). Moreover, visitors of the website who made use of the flow-diagram are asked to fill-out a mini-survey to indicate their satisfaction with the support. This processing will take place according to a Privacy Policy which regulates the way personal data – including online navigation data – are processed by the website.

E-Courses

Concerning the design and development of the E-Courses, no issues are expected. In terms of the questionnaire and interviews, the WP2 general issues are envisioned.

To measure the KPI for WP2, the use of the Interactive Flow-Diagram will be monitored via the U4IoT website (that is part of the LSP-programme website). Moreover, visitors of the website who made use of the flow-diagram are asked to fill-out a mini-survey to indicate their satisfaction with the support.

Expert Pool

In terms of the underlying research used to determine the need for the Expert Pool, the general issues described above are envisioned. Concerning the design and development of the E-Courses no privacy issues are expected.

When publishing the Expert Pool, experts their picture, biography and links to their work will be used for the Expert Pool on the U4IoT website. This will be done with the consent of the experts or without consent when the publication is the provision of a service explicitly requested by them.

To measure the KPI for WP2, the use of the Expert Pool will be monitored via the U4IoT website (that is part of the LSP-programme website). Moreover, visitors of the website who made use of the Expert Pool are asked to fill-out a mini-survey to indicate their satisfaction with the support.

Measures

Interactive Flow-Diagram

Any information that is collected will only be stored, processed and distributed for the design and developed of the interactive flow-diagram. Although privacy issues are not expected, all people participating in the exploratory and evaluative tests will be asked for their informed consent to use the data gathered during the test, in anonymized format, for research purposes.

The information gathered on the performance of the Interactive Flow-Diagram will not contain any personal data, its will be solely used for the measurement of the KPI of WP2 and research report D2.3 and D2.4.

E-Courses

The information gathered on the performance of the E-Courses will not contain any personal data, its will be solely used for the measurement of the KPI of WP2 and research report D2.3 and D2.4.

Expert Pool

Each of the experts who confirmed their interest to be included in the Expert Pool will be asked for their informed consent to use their picture, biography and links to their work for the Expert Pool on the U4IoT website; information will be anyway published when the request to do so comes from the expert himself.

The information gathered on the performance of the Expert Pool will not contain any personal data, its will be solely used for the measurement of the KPI of WP2 and research report D2.3 and D2.4.

3.2.4.2 Ethics

For the design, development and implementation of the Interactive Flow-Diagram, no ethical issues are expected. In terms of the E-Courses and the Expert Pool the following issues are identified and the measures described underneath will be taken.

E-Courses

Materials of consortium partners and other WPs will be used to convert into E-Courses. The property rights of the knowledge communicated in the E-Courses should be guaranteed.

Expert Pool

The first ethical issue to take into account in terms of the Expert Pool, is that the experts in the Expert Pool should reflect a balanced research society. The second issue that arises concerns the fact that it is not in the capacity of U4IoT to interact as an intermediary between the LSP partners and the experts in the Expert Pool. LSP partners and experts have to make their own agreements and U4IoT cannot be hold reliable for possible misunderstandings between LSP partners and experts.

Measures

E-Courses

The intellectual property rights will be visualized in the E-Courses, e.g. in webinars, videos, assignments, the name and logo of the partner who developed the content will be included.

Expert Pool

In order to reflect a balanced research society, U4IoT will make sure to include a wide variety of end-user engagement experts. Taking into account not only expertise but also gender, background, etc. in order to reflect the end-user engagement research and design society.

On the U4IoT website will be made clear that U4IoT will not act as an intermediary, and agreements have to be made between LSP partners and the experts themselves, U4IoT cannot be held responsible for any misunderstandings. Moreover, on the website there has to be communicated that it would be decent to reward experts according to their efforts and that possible agreements concerning intellectual property rights should be made between LSP partners and experts themselves.

3.3 WP3 Analysis and Recommendations

This chapter is not structured according to its tasks. This is the case because the work done and foreseen within the three tasks is very similar in terms of ethics- and privacy related issues. A distinction was thus not deemed necessary.

3.3.1 Privacy

No personal data is crucial for the work in WP3. All the objectives of the work package can be achieved with anonymised data. We will not work with citizens or end-users, our research objects are the LSPs and thus the project partners of the LSPs, who will take part in the interviews in that role, not as private persons. Their personal information is hence not important for the studies to be conducted. The information we will be seeking relates to the LSPs. The LSPs are, however, expected to establish their own sound privacy policy.

When we do interact with end-users, they will be given an information letter and an informed consent form to ensure that they are duly informed about how and what data that is collected and for which purpose.

In **T3.1** the aim is to analyse societal, ethical and ecological issues related to IoT implementation in the LSPs. In this task, primary data from workshops and discussions as well as interviews will be used in combination with secondary data such as project deliverables from the LSPs.

In **T3.2** we will develop recommendations for tackling IoT adoption barriers from an end-user perspective. We will analyse end-users needs and values related to IoT with the aim to

understand these barriers in depth. In this task, anonymised end-user data will be gathered, stored and analysed.

In **T3.3**, we are turning towards target audiences of specific pilots. These may include companies, public organisations, civil society, other organisations or citizens depending on the pilot. Also here, anonymised data will be sufficient for us to reach the task's objectives.

Measures

When interacting directly with private persons, we will ensure to have their informed consent in using information they provide us, following the informed consent agreement as expressed in appendix 1.

Any information that is collected in the course of the work for T3.1, T3.2 and T3.3 will only be stored, processed and distributed for project and research purposes.

The data from these processes will be stored, managed and processed following the principle of data minimization and not for longer time that what is needed.

Anonymized data will be considered out of the scope of Directive 95/46/EC and the GDPR.

If we encounter an uncertainty in this regard during our work within T3.3, or we see a risk of potential privacy infringement, we will assess whether further privacy impact assessment is required. This preliminary assessment can be achieved through several screening questions (see Appendix C). These questions serve to form a crude first view of the privacy impact of a use case. Questions are answered on a yes/no basis. In the unlikely case this preliminary assessment is positive we can rely on the privacy impact assessment methodology of imec.

3.3.2 Ethics

In WP3, we will not face ethical issues from a personal data perspective, since the data being collected will be focused on the project level, that is the LSPs, and their experiences of end-user adoption barriers. Hence, we will handle data regarding the projects according to stipulated ethical guidelines. This means that the data retrieved from the projects will be handled confidential without revealing sensitive information.

In **T3.2** we will develop recommendations for tackling IoT adoption barriers from an end-user perspective. We will analyse end-user needs and values related to IoT with the aim to understand these barriers in depth. In this task, end-user data will be gathered, stored and analysed. However, we will use anonymized data without collecting individuals' specific identity.

In **T3.3**, we are turning towards target audiences of specific pilots. These may include companies, public organisations, civil society, other organisations or citizens depending on the pilot. Also here, anonymised data will be sufficient for us to reach the task's objectives.

The work in T3.3 will be conducted in three steps. We start here by describing these different steps, as they might entail different ethical and privacy issue. We then describe potential issues accordingly and how we will address them.

The **first step** of T3.3 will be the collecting material from any business or sustainability activities that may be going on in the pilots. This will draw insight and will help us to find common and compatible approaches. These insights will be structured and complemented by our own expertise and our own frameworks. The result will be the creation of different (business) scenarios.

The **second step** of T3.3 will be the validation of those scenarios with the LSPs.

The **third step** will be the further evolvement of the validated scenarios. This will be done by including the target audiences of the particular pilots.

We thus get in touch with different groups of people and consequently we will process different

kind of information. In general, there is no need to use personal data in order to reach the task's objectives.

We do not expect to come across major ethical issues in conducting our work for T3.3.

One potential issue we are taking into account at this point might arise from the interaction with pilot target audiences and in particular with companies and public organisations in step 3.

To validate our scenarios and models, and to make them as concretely applicable as possible as is requested by the DoW, we might ask them to provide information that might count as confidential. We do not actively seek for confidential data and will try to avoid it, but it might be necessary in order to provide the best possible outcomes. This might be the case regarding some insights from a company's business model, a pricing scheme or information that relates to intellectual property (IP).

Measures

In the case that we interact with end-users, ethical issues in the context of this activity coincide with potential data protection issues, which will be tacked according to what has been explained above in section 3.3.1.

In case we seek company data for enriching our research (e.g. business model), we will make sure to establish the appropriate non-disclosure agreement. A non-disclosure agreement needs to be a specific solution for IP challenges. It includes what we will use the information for: deliverables that are public (or cannot be according to the agreement); for sharing it with the LSPs; for academic publications, etc. We have an expert at imec that can help us with non-disclosure agreements if necessary.

3.4 WP4 Collaboration, Outreach and Dissemination

3.4.1 T4.1 Cooperation strategy with LSPs and end-users outreach

T4.1 deals with the communication and dissemination strategies of U4IoT with the LSPs and end-users. As a result, no sensitive data is collected from individuals. The publication of the strategy merely outlines the plan for the LSPs and U4IoT to collaborate with each other and with CREATE-IoT.

3.4.2 T4.2 Website and Dissemination

T4.2 will set up and maintain a dynamic web portal in collaboration with CREATE-IoT which will gather and give access to the various resources of the Project and CRATE-IoT. The portal will be complemented by a social media communication strategy (e.g. LinkedIn groups, Facebook, etc.) that will ensure a broad diffusion of the project results and promote the project in online discussion communities. Complementary communication tools, such as videos, posters, white papers, flyers and other printed material will be developed. As a result, no sensitive data is collected from individuals.

3.4.3 T4.3 Online knowledge base on lessons learned, solutions and user feedback

T4.3 will develop and manage an online knowledge base platform to collect lessons learned, solutions and user feedbacks. It will constitute the interactive part of the online platform. The prime objective of this task is to enable the community to share and mutualize lessons learned and to capitalize the acquired experience in order to support and accelerate the progress on the learning curve. Platform's users will not be identified, unless it is necessary; in the latter case,

personal data will be processed for the purposes of the research activities within the project, and in accordance to a Privacy Policy regulating the platform.

4 U4IoT GENERAL ETHICS AND PRIVACY IMPLEMENTATION PLAN

4.1 General principles

By default, the project will avoid and prevent any unnecessary collection and use of personal data. Project partners will take all required steps to guarantee compliance with the provisions of the relevant EU directives related to personal data and information protection, particularly Directive 95/46/EC and EU Directive 2002/58/EC on Privacy and Electronic Communications as well as the related legislation of the Member States of the project partners and the LSPs, particularly those of the countries in which the will pilots take place.

These legal requirements will be supplemented with the changes reflected in the GDPR, which will have to be taken into account in May 2018.

Work will be carried out respecting the principles of the Charter of Fundamental Rights of the European Union. These include dignity, freedom, equality, solidarity, citizens' rights and justice. Our proposal also complies with Article 8 of the European Human Rights Convention. In particular, researchers will consider the sensitive implications of their agendas for privacy and autonomy.

4.2 Personal Data Protection under Directive 95/46/EC

According to article 2 of the **Directive 95/46/EC** of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, "'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

In case personal data would be nevertheless accessed, the research project will strictly and fully comply with the European standards for personal data protections, including Directive 95/46/EC on the protection of individuals with the regard to the processing of personal data and on the free movement of such data (the "Directive"). Other provisions from the European regulation and practice will be taken into account, where relevant, for the proper achievement of the project's aims (like, inter-alia, the provisions of the European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "ePrivacy Directive"). In addition, other essential guidelines affecting project's approach and/or realization are also to be considered like, the right to the protection of personal data as explicitly stated in Article 16 of the Treaty on the Functioning of the European Union (this has given the EU new responsibilities to protect personal data in all areas of EU law, including police and judicial cooperation, and is to be considered by the project's approach as well).

4.3 Data Minimisation

The project will comply with the principle of **data minimisation**, by limiting the collection and/or storage of sensitive data to the extent that it is necessary, and will not store data for a longer period than needed. Data will be parsed and anonymized and personal identifier will be either hashed or randomly generated. The project will abide to the "Prior informed consent" principle by providing clear and transparent information and by letting the respondents choose what information they want to provide for what purpose. The website will be fully transparent regarding the data processor and data controller. Respondents will be duly informed ahead of their acceptance to participate, on the personal data protection policy of the project. This information will be provided in a layered, readable and user friendly mode, and will be

accessible at any time from the website. Proactive actions will be undertaken to guarantee that the respondents fully understand and give their consent to the data protection policy of the project. Respondents will be granted the right to opt-out from the project at any time, in a simple and effective way.

4.4 Personal Data Protection Officer

A **Personal Data Protection Officer** (PDPO) will be nominated and will be accessible to the public through the contact page of our website. The PDPO will therefore act as a single point of contact for any data subjects participating in the project. For any query or exercise of rights the users may always address a request to the PDPO, who will act as a single point of contact. Personal data breaches or risks thereof will proactively be brought by the PDPO to the attention of the data subjects.

The project will adopt Privacy policy rules and guidelines that will be made available on the website and easily accessible from the agents. The respondents will be invited to provide a control of the interviews, workshops and discussions and to inform the PDPO on any identified risk of non-compliance with the rules and guidelines of the project.

4.5 Territoriality and normative scope

The research project is to take place mainly in EU-member states and/or in associated countries with equivalent level of privacy protection. In the case of research undertaken In other countries we will comply with applicable laws and in any case a level of protection at least equivalent to EU standards will be ensured. The data will be stored in secured servers in Europe and no personal data will be transferred abroad or stored in non-European based cloud infrastructure.

Moreover, the European personal data protection norms and ethical standards and guidelines of Horizon2020 will be rigorously applied, regardless of the country in which are located the users. The project will voluntary and universally apply and respect the European norms and standards regardless of the territorial location of the users. The project will abide by all applicable and any future EU and national legislations, as well as by the relevant international guidelines and will be conducted in accordance with the Declaration of Helsinki.

4.6 Duration of data retention

All data collected by the platform will be collected on the principle of the prior informed consent or, where applicable, on the basis of another viable legal ground (e.g. legal obligation, contract etc.). The project will differentiate amongst:

Personal data, meaning information related to an identified or identifiable individual, including IP addresses, IMEI codes, pictures, voice recordings, username, passwords, opinions etc. This personal data will be retained for as long as necessary to fulfil the envisaged objectives of the processing, and will be deleted thereafter. For example, personal data related to the usage of the websites, platforms and interactive tools developed by the project will be deleted if the users do not use the websites, platforms and interactive tools for 3 months after he/she carried out the first access to them. All the other personal data will be deleted by no later than the end of the project.

Anonymized data, meaning personal data that afterwards anonymized, with no means (once anonymized) to identify the person behind such data. Such data will be considered as non-sensitive data moving out of the scope of "personal data" as defined by the directive Directive 95/46/EC on the protection of individuals with the regard to the processing of personal data and on the free movement of such data. In the absence of any risk for personal data protection, such data can be stored as long as relevant for the research project and scientific audits, and may even be retained once the project ends ant put at disposal of other research

initiatives.

4.7 Informed consent

Examples of Informed Consent Forms and Information Sheets are appended in this deliverable. These must be in language and terms understandable to the respondents. Respondents must have, inter-alia, the right:

- To know that participation is voluntary;
- To ask questions and receive understandable answers before making a decision;
- To know the degree of risk and burden involved in participation;
- To know who will benefit from participation;
- To know the procedures that will be implemented in the case of incidental findings;
- To receive assurances that appropriate insurance cover is in place;
- To know how their data will be collected, protected during the project and either destroyed or reused at the end of the research; minors will be re-asked for their consent as soon as their reach legal majority
- To withdraw themselves and their data from the project at any time;
- To know of any potential commercial exploitation of the research;
- To know to which other countries personal data might be transferred.

4.8 Fundamental Data Protection Principles

U4IoT will have compliance with fundamental data protection principles.

Transparency: U4IoT will inform respondents (i.e. data subjects) about all (data protection) relevant aspects of the facilities; in particular, respondents should be informed about all entities (including potential subcontractors) contributing to the provision of the respective facility and all locations in which data may be stored or processed by the researchers.

Purpose specification and limitation: the researcher will have to ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes than was agreed upon. Commitments in this respect may be captured in appropriate contractual measures;

Information sharing: Sharing of datasets will be defined on a case-by-case basis. Based on the type of dataset, it will be decided which datasets can be made public, shared are have to be kept confidential. All participants in the user tests will sign an informed consent, clarifying all implications in terms of privacy and protection of their personal data.

Personal data sharing: Data sharing will be defined before data collection so that users are able to consent. If data would be shared to unanticipated parties, this data will be anonymised or be evaluated if compatible grounds for scientific research apply.

Data retention: the researchers will be made responsible for ensuring that personal data are erased from wherever they are stored as soon as they are no longer necessary for the specific purposes.

On top of the ones applicable to the project as a whole, the workshops and interviews will be accompanied by further measures taken by the Consortium as a way to protect the personal data of the involved stakeholders.

a. Clear information to participants in the data-collection process will be provided

b. The participants will be asked a prior consent before being interviewed; in fact, contacting and targeting potential participants beforehand is normally not allowed without consent

c. Personal information will be separated from opinions/ideas expressed by participants during the procedure;

d. When the process will entail interviews of the participants in order to collect, for example, information regarding, adoption barriers, personal information collected will be aggregated as soon as possible.

5 CONCLUSION

The document at hand lays down the (potential) issues regarding ethics and privacy within the U4IoT cooperation and support action. U4IoT works with and for the IoT LSPs. Collection, aggregation, storage, use, disclosure (and ultimately destruction) of data inevitably gives rise to privacy and security concerns.

As requested by the European Commission, U4Iot thus composed this concise and practical *Ethics and Privacy Implementation plan* to draw out and remedy the potential privacy and ethic related risks. It outlines how U4IoT will implement processes for ethics and privacy which include e.g. informed consent procedures for the participation of humans, on the procedures that will be implemented for data collection, storage, protection, retention and destruction and confirmation that they comply with national and EU legislation.

Chapter 2 presented general concepts and aspects relating to ethics and privacy in user engagement and related research, as well as related definition and applicable EU laws and norms. This provides the necessary foundation to consider issues specific to the U4IoT project.

In chapter 3, the task leaders went into detail concerning the specific work conducted within their tasks. They discuss the ethics- and privacy-related issues specific to their tasks. Where necessary, measures to be taken are added, which ensure the compliance to the general U4IoT data protection policy and the general *Ethics and Privacy Implementation plan.*

Chapter 4 adds the general U4IoT *Ethics and Privacy Implementation plan.* This plan has been composed based on the basic foundations and the specific tasks and issues presented in previous chapters.

It ensures that the ethical standards and guidelines of Horizon2020 will be rigorously applied, in all the country in which the research is carried out.

APPENDIX A: U4IOT INFORMED CONSENT FORM

INTRODUCTION

You are invited to join a research study to contribute to our analysis of societal, ethical and ecological issues related to IoT implementations in the Large Scale Pilots. Please take whatever time you need to discuss the study with your family and friends, or anyone else you wish to the decision to join, or not to join, is up to you.

In this research study, we are investigating plans, activities and results from the contexts of the Large Scale Pilots with the objective to identify actors, changes sought for and aspects influencing diffusion and adoption of IoT in the pilots.

WHAT IS INVOLVED IN THE STUDY?

If you decide to participate you will be asked to take part in discussions, interviews and workshops. We think this will take you between 60-120 minutes. Some of these interactions will take part in correlation with other events, e.g. IoT week, some will be carried out online via e.g. Skype and some will be in person.

The investigators may stop the study or take you out of the study at any time they judge it is in your best interest. They may also remove you from the study for various other reasons. They can do this without your consent.

You can stop participating at any time. If you stop you will not lose any benefits.

DATA CONTROLLER

The data controller is the U4IoT project, represented by its coordinator LULEA TEKNISKA UNIVERSITET (LTU), 2021002841, established in UNIVERSITETSOMRADET PORSON, LULEA 971 87, Sweden, VAT number SE202100284101, represented by Anna Ståhlbröst.

RISKS

This study involves the following risks: exposure of your personal data to the large scale pilots on IoT and their challenges. There may also be other risks that we cannot predict.

BENEFITS TO TAKING PART IN THE STUDY?

It is reasonable to expect the following benefits from this research: increased knowledge on how to design and implement IoT solutions that end-users want to adopt and use which in turn will give benefits to the Large Scale Pilots and its success. However, we can't guarantee that you will personally experience benefits from participating in this study. Others may benefit in the future from the information we find in this study.

CONFIDENTIALITY

We will take the following steps to keep information about you confidential, and to protect it from unauthorized disclosure, tampering, or damage: only partners at LTU will have access to the original data, the data will be described in general ways to ensure that individuals are not revealed or could be traced in the material. The analysis of data will be related to the Large Scale Pilots and its efforts, not on an individual level. Quotes might be used to highlight aspects of the pilots, but it will not reveal who expressed it. The data will be kept within the premises of LTU.

Scientific publications will be made based on the data from a pilot perspective, not at an individual level.

Data are kept on a computer requiring a password. Only researchers at LTU will have access to the source data.

YOUR RIGHTS AS A RESEARCH PARTICIPANT?

Participation in this study is voluntary. You have the right not to participate at all or to leave the study at any time. Deciding not to participate or choosing to leave the study will not result in any penalty or loss of benefits to which you are entitled, and it will not harm your relationship with U4IoT project.

If you want to withdraw from the study, send an email to aya.rizk@ltu.se and she will make sure that your data is excluded from the study by deleting it from her computer.

SCOPE OF CIRCULATION OF PERSONAL DATA

Your personal data may be shared with the relevant members of the LSPs and with the projects U4IoT and Create-IoT, in order to achieve the research's purposes.

For the provision of the platform and other IT services we have bound, as data processor, according to Article 28 of the GDPR and to APPENDIX D: SPECIFIC COMMITMENTS OF THE DATA PROFCESSORS, Drustvo Za Konsalting, Razvoj I Implementaciju Informacionih I Komunikacionih Tehnologija Dunavnet Doo (**DNET**), 20232145, established in Polgar Andrasa 38a, Novi Sad 21000, Serbia, VAT number RS104769297.

All the persons accessing personal data under the authority of the data controller or the data processor will do so on a need-to-know basis and are bound by confidentiality obligations.

CONTACTS FOR QUESTIONS OR PROBLEMS?

Call our [Personal Data Protection officer] if you have questions about the study, any problems, unexpected physical or psychological discomforts, any injuries, or think that something unusual or unexpected is happening.

Consent of Subject (or Legally Authorized Representative)

Signature of Subject or Representative Date

_____

Upon signing, the subject or the legally authorized representative will receive a copy of this form, and the original will be held in the subject's research record.

APPENDIX B: U4IOT INFORMATION LETTER

[Name of organisation]

Adress

Phone

e-mail address

Organization number

For the project U4IoT (User Engagement for Large Scale Pilots in the Internet of Things)[5], [Organisation name] would like you to provide certain information about the Large Scale Pilots (LSP) you are participating in, concerning your experiences with IoT implementation and adoption barriers.

The purpose of the project is to support the LSPs by providing toolkits and direct support for end-user engagement, to encourage them to participate in the LSPs and to adopt the IoT technology. In addition, we will analyse societal, ethical and ecological issues related to the implementation of IoT with the aim to develop recommendations for tackling adoption barriers. The project lasts until the end of 2019.

To be able to develop those supportive tools and handbooks, we would like to gather information about your experiences, insights, thoughts and perspectives. This will ensure the relevance of our work for the LSPs and for the stimulation of the adoption of IoT technology.

The information we will gather is your name, project you work in, your role in the project, plans, activities and results related to the project, and your experiences and insights concerning IoT development and implementation. You decide if you want to share this information with us.

The information will be accessible only to us within our organisation. Anonymised information might be shared with other actors in the form of scientific articles and related dissemination activities.

If you have any questions about the project you are free to contact [Name, phone number and email to local contact]

I agree that [Name of organisation] can use this information about be according to what is stated above.

.....

Town and date

.....

Name

[5] european-iot-pilots.eu/u4iot/

APPENDIX C: SCREENING QUESTIONS FOR PRELIMINARY PRIVACY IMPACT ASSESSMENT

Table 1: Screening questions for preliminary privacy impact assessment

1.	Will the project compel individuals to provide personal information about themselves?
2.	Will the project involve the collection of new information about individuals?
3.	Will you use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
4.	Is the information about individuals of a kind particularly sensitive and therefore likely to raise privacy concerns or expectations? For example, information about a person's health, criminal record, beliefs, race, or other information that people are likely to consider as private?
5.	Will information about individuals be disclosed to organizations or people who have not previously had routine access to the information?
6.	Are any of those organizations located outside of the European Union?
7.	Will the project result in you making decisions or taking action against individuals in ways, which could have a significant impact on them?
8.	Does the project involve using new technology, which might be perceived as being privacy intruding for example biometrics or facial recognition?
9.	Will the project require you to contact individuals in ways, which they may find intrusive to their personal life?

APPENDIX D: SPECIFIC COMMITMENTS OF THE DATA PROCESSORS

Each data processor agrees and warrants:

- To process the personal data only on behalf of the data controller, according to specific agreement, and in compliance with its instructions and these clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data controller of its inability to comply, in which case the data controller is entitled to suspend the transfer of data and/or terminate the contract;

- that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data controller and its obligations under this data processing agreement and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by these clauses, it will promptly notify the change to the data controller as soon as it is aware, in which case the data controller is entitled to suspend the transfer of data and/or terminate the contract;

- that it has implemented the technical and organisational security measures indicated in Annex 1 before processing the personal data transferred;

- that it will promptly notify the data controller about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

- to deal promptly and properly with all inquiries from the data controller relating to its processing of the personal data subject to the transfer and to abide by the advice of the competent supervisory authority with regard to the processing of the data transferred;

- at the request of the data controller to submit its data processing facilities for audit of the processing activities covered by these clauses which shall be carried out by the data controller;

- to make available to the data subject upon request a copy of the data processing agreement, or any existing contract for subprocessing, and a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data controller;

- that, in the event of subprocessing, it has previously informed the data controller and obtained its prior written authorization.

Where the data processor subcontracts its obligations under these clauses, with the written consent of the data controller, it shall do so only by way of a written agreement with the subprocessor in the name and on behalf of data controller, which imposes the same obligations on the subprocessor as are imposed on the data processor under these clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data processor shall remain fully liable to the data controller for the performance of the subprocessor's obligations under such agreement.

Each data processor in the context of the project agrees that on the termination of the provision of data processing services, the data processor and the subprocessor shall, at the choice of the data controller, return all the personal data transferred and the copies thereof

to the data controller or shall destroy all the personal data and certify to the data controller that it has done so, unless legislation imposed upon the data processor prevents it from returning or destroying all or part of the personal data transferred. In that case, the data processor warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data processor and the subprocessor warrant that upon request of the data controller and/or of a supervisory authority, it will submit its data processing facilities for an audit of the measures referred to above.