



Grant Agreement No.: 732078
Call: H2020-ICT-2016-2017
Topic: IOT-02-2016 – IoT Horizontal Activities
Type of action: CSA



D1.3: Guidelines and Game for Privacy and Personal Data Protection in LSPs

Work package	WP 1
Task	Task 1.3
Due date	30/06/2018
Submission date	18/07/2018
Deliverable lead	Archimède Solutions
Version	1.0
Authors	Ana Maria Pacheco (Archimède Solutions), Cesco Reale (Archimède Solutions), Lucio Scudiero (Archimède Solutions), Pasquale Annicchino (Archimède Solutions), Sébastien Ziegler (Mandat International)
Reviewers	Dejan Drajić (DNET), Kai Zhang (Martel)

ABSTRACT & KEY WORDS

Abstract	<p>The entry into force of the GDPR (General Data Protection Regulation) poses new challenges to the IoT sector not only in the case of ensuring compliance and for the valorization of the data. The GDPR creates a complex legal framework that the different actors have to be able to master and apply. Such complexity needs to be somehow simplified, while at the same time ensuring an adequate level of security and personal data protection. Individuals shall be granted the opportunity to live in a secure and trustable IoT environment because it is only through security and the protection of privacy that end-users will rely on IoT solutions. The present document provides a set of guidelines to be used by the LSP (Large Scale Pilots) in order to ensure full compliance with the GDPR. These guidelines do not substitute to the regulation and applicable legal obligations that all pilots must respect and comply with. It is intended to provide a complementary set of information and guidance in order to ease the full implementation of GDPR obligations.</p> <p>The privacy game is a serious game meant to help the LSP stakeholders to learn the fundamental principles of data protection, to raise awareness on the main risks related to data protection with IoT deployments, translating complex legal norms into clear and easily understandable principles. It is aimed at LSP consortia, LSP end-users and large public. The game is meant to be easily understandable, enjoyable and educative, covering the IoT privacy risks and all main definitions and principles of the GDPR. It follows a clear iterative methodology of game design, playtest, analysis and improvements. The game is to be disseminated through privacy seminars, LSP events, game festivals and more.</p>
Keywords	Privacy, GDPR, LSP, IoT, serious game

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1		Initial draft of the deliverable	Ana Maria Pacheco (Archimède Solutions), Sébastien Ziegler (Mandat International)
V0.2		Serious game inputs	Cesco Reale (Archimède Solutions)
V0.3		Data Protection guidelines	Ana Maria Pacheco (Archimède Solutions), Lucio Scudiero (Archimède Solutions), Sébastien Ziegler (Mandat International)
V0.4		Data Protection guidelines revision	Pasquale Annicchino (Archimède Solutions)
V0.5	June 2018	Consolidated version	Ana Maria Pacheco (Archimède Solutions), Sébastien Ziegler (Mandat International), Cesco Reale (Archimède Solutions), Pasquale Annicchino (Archimède Solutions)
V0.6	June 2018	Complete version	Ana Maria Pacheco Huamani
V0.7	4.7.2018.	DNET review	Dejan Drajić (DNET)
V0.8	6.7.2018	Martel review	Kai Zhang (Martel)
V1.0	18.7.2018	Final version	Ana Maria Pacheco (AS), Cesco Reale (AS), Sébastien Ziegler (MI).

DISCLAIMER

The information, documentation and figures available in this deliverable are written by the User Engagement for LSPs in the Internet of Things, U4IoT; project's consortium under EC grant agreement 732078 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

COPYRIGHT NOTICE

© 2017 - 2019 U4IoT Consortium

ACKNOWLEDGMENTS

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. The opinions expressed and arguments employed do not engage the supporting parties.

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:		R, DEM
Dissemination Level		
PU	Public, fully open, e.g. web	*
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to FLAME project and Commission Services	

EXECUTIVE SUMMARY

The entry into force of the European General Data Protection Regulation (GDPR) poses new challenges to the Internet of Things (IoT) sector. The GDPR creates a complex legal framework that different actors have to master and apply. Such complexity needs to be communicated in simple terms, while ensuring an accurate level of compliance with security and personal data protection obligations.

Complying with the GDPR is particularly important for the five Large Scale Pilots (LSPs) on IoT. The LSPs are expected to interact with a large variety of end-users and should apply a privacy by design approach for their implementation and deployment in order to respect and protect the data subject rights. This is even more important in the context of projects being financed by the European Commission. In this context, we should expect exemplarity from the five LSPs. That is why this deliverable has been prepared by U4IoT.

This deliverable presents two complementary outputs of the U4IoT project:

- Guidelines for LSPs Projects to comply with the GDPR;
- A serious game on data protection.

The guidelines are meant to be used by the LSPs in order to ensure full compliance with the GDPR. These guidelines do not substitute the regulation and applicable legal obligations that all LSPs must respect and comply with. It is intended to provide a complementary set of information and guidance to better understand the GDPR obligations.

The serious game is meant to help the LSPs to learn the fundamental principles of data protection and privacy, to translate complex legal norms into clear and easily understandable and operational principles, to raise awareness on the main privacy risks with IoT deployments, especially reducing the risks of non-compliance to the GDPR and fines.

Both sections aim at supporting end-user engagement in the five LSPs in the field of the Internet of Things (IoT).

TABLE OF CONTENTS

Abstract & Key Words.....	2
Document Revision History	2
Disclaimer.....	3
Copyright notice	3
Acknowledgments.....	3
1.1 U4IoT Purpose	9
1.2 Deliverable D1.3.....	10
2 PRIVACY GUIDELINES.....	11
2.1 Introduction to personal data protection in IoT LSPs	11
2.2 Key Definitions	12
2.3 Key Data Protection Principles	13
2.3.1 List of Key GDPR Principles.....	13
2.3.2 List of Key ePrivacy Directive Principles	16
2.4 Consortia's Data Protection Strategy and compliance	17
2.4.1 Data Protection Officer (DPO) function	19
2.4.2 Adopting formal data protection policies and rules	20
2.4.3 Records of processing	20
2.5 Privacy BY DESIGN Approach in the LSPs	21
2.6 co-creation processes (where foreseen)	24
2.7 Open Calls	25
2.8 Complaints Management.....	26
2.9 DATA BREACH POLICY	27
2.10 Privacy APP	28
2.11 projects' technical and security measures overview	28
2.12 DATA recommendations for different stakeholders in the IoT Domain.....	28
3 PRIVACY GAME – A SERIOUS GAME ON DATA PROTECTION	29
3.1 introduction.....	29
3.2 Objectives of the serious game.....	30
3.3 Target groups of users.....	31
3.4 Requirements of the serious game	31
3.5 Planning and methodology	33

3.5.1	Importance of concepts to communicate	34
3.5.2	Playability	35
3.6	Key concepts to communicate	36
3.6.1	Key definitions.....	37
3.6.2	Key principles.....	37
3.7	Methodological Approach for question design	38
3.8	Matrix of Questions per Domain	40
3.9	First test and validation at the IoT week in june 2017	41
3.9.1	Sets of cards and team game.....	41
3.9.2	The questionnaire for the play-testers	42
3.9.3	Analysis of the answers.....	43
3.9.4	General conclusions about the test and new version.....	47
3.10	Second test at LSP Meeting in october 2017	48
3.10.1	The improved questionnaire	48
3.10.2	Analysis of the answers.....	48
3.11	Assessment and validation of the questions.....	49
3.12	Rules of the game "Privacy Quiz"	50
3.13	Expansion of the game	52
3.14	Tests and dissemination in the first semester of 2018.....	52
3.15	Online game.....	54
3.16	Conclusion on the Serious Game.....	57
ANNEX A – ORGANIZATIONAL AND SECURITY MEASURES		61
ANNEX B – RECOMMENDATIONS FOR DIFFERENT STAKEHOLDERS IN THE IOT DOMAIN		66
ANNEX C – RECOMMENDATIONS FOR DIFFERENT STAKEHOLDERS IN THE IOT DOMAIN		68
ANNEX D – QUESTIONNAIRE FOR THE PLAY TESTERS – VERSION 1		71
ANNEX E – QUESTIONNAIRE FOR THE PLAY TESTERS – VERSION 2		72

LIST OF FIGURES

FIGURE 1: DATA FLOW SCHEME IN A SMART CITY USE CASE.....	18
FIGURE 2: PRIVACY BY DESIGN APPROACH	21
FIGURE 3: METHODOLOGY OF END-USER DRIVEN DESIGN AND DEVELOPMENT.....	34
FIGURE 4: MATRIX OF QUESTIONS PER DOMAIN.....	40
FIGURE 5: HOW LONG DID YOU PLAY THE GAME?	43
FIGURE 6: HOW MANY CARDS DID YOU PLAY?	44
FIGURE 7: DID YOU LEARN SOMETHING NEW ABOUT PRIVACY?	45
FIGURE 8: IS THE GAME USEFUL FOR PRIVACY AWARENESS?	46
FIGURE 9: IS THE GAME EASY TO UNDERSTAND AND TO PLAY?	46
FIGURE 10: ARE THE QUESTIONS CLEAR AND EASY TO UNDERSTAND?	47
FIGURE 11: EXAMPLE OF CARD FRONT WITH A QUESTION.....	51
FIGURE 12: EXAMPLE OF CARD BACK WITH ANSWER AND EXPLANATION	51
FIGURE 13: PROVISIONAL ENTRY PAGE OF THE PRIVACY QUIZ.....	55
FIGURE 14: QUESTION IN THE ONLINE GAME	55
FIGURE 15: QUESTION WITH ITS ANSWER AND EXPLANATION IN THE ONLINE GAME	55
FIGURE 16: PROVISIONAL PAGE OF THE ENDGAME IN THE ONLINE GAME	56

ABBREVIATIONS

AS	Archimède Solutions
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
IoT	Internet of Things
LSP	Large Scale Pilot

GENERAL INTRODUCTION

The entry into force of the European General Data Protection Regulation (GDPR) poses new challenges to the Internet of Things (IoT) sector. The GDPR creates a complex legal framework that different actors have to master and apply. Such complexity needs to be communicated in simple terms, while ensuring an accurate level of compliance with security and personal data protection obligations.

Complying with the GDPR is particularly important for the five Large Scale Pilots (LSPs) on IoT. The LSPs are expected to interact with a large variety of end-users and should apply a privacy by design approach for their implementation and deployment in order to respect and protect the data subject rights. This is even more important in the context of projects being financed by the European Commission. In this context, we should expect exemplarity from the five LSPs. That is why this deliverable has been prepared by U4IoT.

1.1 U4IOT PURPOSE

U4IoT (User Engagement for Large Scale Pilots in the Internet of Things) is a H2020 European research project that brings together 9 partners from 5 European countries. The objectives of U4IoT are to support the end-user participation in the five European Large Scale Pilots on IoT.

U4IoT is in charge of developing a set of resources to be used by the LSPs such as: toolkit for LSPs end-user engagement and adoption, online resources, privacy-compliant crowdsourcing tools, guidelines and an innovative privacy game for personal data protection risk assessment and awareness, and online training modules.

The project provides direct support to mobilize end-user engagement with co-creative workshops and meetups, trainings, Living Labs support, and an online pool of experts to address LSPs specific questions.

The project also analyses societal, ethical and ecological issues and adoption barriers related to the pilots with end-users and make recommendations for tackling IoT adoption barriers, including educational needs and sustainability models for LSPs and future IoT pilots deployment in Europe.

The activities comprise communication support, knowledge sharing and dissemination with an online portal and interactive knowledge base gathering the lessons learned, FAQ, tools, solutions and end-user feedbacks.

1.2 DELIVERABLE D1.3

This deliverable D1.3 is part of Work Package 1 and is led by Archimede Solutions (AS). It is structured in two parts presenting two complementary outputs of the U4IoT project:

- Guidelines for LSPs Projects to comply with the GDPR;
- A presentation of the serious game on data protection.

The guidelines are meant to be used by the LSPs in order to ensure full compliance with the GDPR. These guidelines do not substitute the regulation and applicable legal obligations that all LSPs must respect and comply with. It is intended to provide a complementary set of information and guidance to better understand the GDPR obligations.

The serious game is meant to help the LSPs to learn the fundamental principles of data protection and privacy, to translate complex legal norms into clear and easily understandable and operational principles, to raise awareness on the main privacy risks with IoT deployments, especially reducing the risks of non-compliance to the GDPR and fines.

The serious game intends to address the following target users:

- a) the consortia members of the LSPs that have to deal with privacy issues in the development of their projects;
- b) the LSPs' end-users, that will interact with the IoT deployments provided by the 5 LSPs;
- c) the large public in general.

The serious game has been conceived in order to:

- raise awareness on the risks related to data protection obligations in the context of the five LSPs, and more generally in the context of IoT deployments;
- encompass the main definitions and key principles of the GDPR;
- reduce the risks of non-compliance with the GDPR;
- be easily scalable with reduced marginal costs;
- be easily understandable by players that have no legal background;
- be short and enjoyable.

Both sections aim at supporting end-user engagement in the five LSPs in the field of the Internet of Things (IoT).

2 PRIVACY GUIDELINES

2.1 INTRODUCTION TO PERSONAL DATA PROTECTION IN IOT LSPS

The adoption of the GDPR by the European Union enables to consolidate, clarify and homogenize the data protection rules to be respected by any data controller in Europe. It entered into force in May 2016 and became fully applicable from 25 May 2018¹.

In this regard, IoT does pose specific challenges that must be addressed. Sensors, mobile phones, wearable objects, RFID tags, cameras, middleware components, among others, have a common feature: they are all points of entrance of data, which can include personal data. As the players of the Internet of Things (IoT) landscape heavily leverage on personal data to deliver services and increase consumers' user experience, personal data protection and security are key elements in the "value creation chain" of IoT. It also escalates and multiplies existing challenges. For example, data subject's control on personal data becomes more difficult due to the dispersed number of data sources and entities processing personal data; as the chain of providers of IoT services stretches, allocation of responsibilities and enforcement of data protection law become more complex than before; and the same can be said with regards to compliance to the principles of purpose limitation and data minimization. Moreover, it is not easy to identify in each case what the viable legal ground for personal data processing is. The data subject's consent is not always a reliable one; in some cases – especially in the Smart Cities domain – Union or Member State law may constitute the legal basis for personal data processing through IoT deployments.

Such complexity needs – therefore – to be somehow simplified, while at the same time ensuring an adequate level of security and personal data protection. Individuals shall be granted the opportunity to live in a secure and trustable IoT environment.

The prime objective of the GDPR is to protect the individuals and to ensure that their rights, as data subjects, are fully respected. In doing so the GDPR produces a major shift from documental compliance to substantive safeguards, which need to be applied to personal data during their entire lifecycle, with a clear allocation of roles between the entities involved and higher legal and financial responsibility; in fact, on one hand, the GDPR provides for greater accountability, but on the other hand, it may lead to very high fines for the lack thereof, according to a double layer system of administrative fines, which exposes infringing entities to up to 10 million EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, or up to 20 million EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover.

This document provides a set of guidelines to be used by the LSPs in order to ensure full compliance with the GDPR. These guidelines do not substitute the regulation and applicable legal obligations that all pilots must respect and comply with. It is intended to provide a complementary set of information and guidance in order to ease the full implementation of GDPR obligations.

¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

2.2 KEY DEFINITIONS

The following section clarifies in simple words some important and key terms and definitions used in the GDPR²

Personal Data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. In other words, you should consider as personal data, any data that is linkable to individuals, such as for instance: pictures, email addresses, phone numbers, full name, postal address, IP or MAC addresses of their personal device.

Data Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In other words, the data controller is the entity which takes the decision to collect data and decides on how these data will be processed.

Data Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. In other words, the data processor is the entity that is processing data on behalf of a data controller.

Data Subject: an identified or identifiable natural person. In other words, all individuals are data subjects.

Prior Informed Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her, before the actual processing of personal data takes place. In other words, it is a two steps process through which at first the data subject is informed on the purpose for which his data are requested and afterward he freely provides his express consent to the processing and use of his personal data.

Purpose limitation: an overarching privacy principle, according to which personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. In other words, any personal data collection should be collected for a clear and specific purpose.

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Special categories of data: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data and biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. There are very strict limitation to the collection and processing of any special categories of data.

General Data Protection Regulation: Regulation EU/679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

² Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

data.

ePrivacy Directive: Directive 2002/58/EC³ concerning the processing of personal data and the protection of privacy in the electronic communications sector. This Directive complements the rules set forth by the GDPR in the field of, for example, unsolicited calls, cookies, phone traffic data and so on.

2.3 KEY DATA PROTECTION PRINCIPLES

The LSPs will have to comply with the European regulation and norms related to personal data protection and privacy. The two main normative sources that will be considered and focus on are:

- Regulation EU/679/2016 (GDPR)
- Directive 2002/58/EC (ePrivacy Directive)

Here is a short introduction on the key principles enshrined in these two norms. This introduction constitutes an overview and general introduction and does not substitute to the detailed obligations contained in the official regulations.

2.3.1 List of Key GDPR Principles

- 1) The GDPR intends to protect **personal data processed by legal entities**. As a consequence:
 - a. It does not apply to personal data collected by individuals for their private use.
 - b. It does not apply to data that cannot be linked to individuals. For instance, data provided by a temperature sensor fixed on a street light will not be considered as personal data (there is no link with a natural person), while the geolocation data and sensors data collected from a smart phone will be considered as a personal data, because they can be linked to a person.
- 2) The GDPR applies to the **processing of personal data regardless of the means used, whether automated** (e.g. an app, a website, a network of sensors) **or not automated** (e.g. a filing system based on paper).
- 3) The GDPR has 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 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 .

- 4) **Personal data cannot be processed without a legal ground or the agreement of the data subject.** This usually entails that the data subject has to give his/her consent to the processing of his or her personal data for one or more specific purposes; however, different legal grounds may apply, in different instances, which could exempt controllers or processors from collecting the data subject's consent. This holds true when personal data processing:
 - a. is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (e.g. when transferring connected cars' data to an external provider of maintenance services, as agreed with the car's owner through a contract);
 - b. is necessary for compliance with a legal obligation to which the controller is subject (e.g. a Union, national or regional law setting out rules and obligations for cities within smart cities' programs);
 - c. is necessary in order to protect the vital interests of the data subject or of another natural person (e.g. when deploying IoT devices for emergency health care purposes);
 - d. 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 (e.g. when personal data processing is necessary to manage a tax system);
 - e. is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child (the discipline of the legitimate interest still vary across EU Member States and needs a case by case assessment).
- 5) **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).
- 6) 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 foreseen (e.g. in a smart city context, by complete information notices published on the cities' websites, by icons displayed on the users' devices, by signs on the street in correspondence of IoT sensors or cameras).
- 7) **Data protection principles** (i.e. 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**.

- 8) **Risky processing** for the data subjects require a **Data Protection Impact Assessment (DPIA)**. In particular, the DPIA shall be carried out in the case of:
- a. *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. when an insurance company uses data drawn from collected cars to build customers' profiles and premiums);*
 - b. *processing on a large scale of special categories of data (e.g. in the case of provision of e-health services);*
 - c. **a systematic monitoring of a publicly accessible area on a large scale** (e.g. smart cities deploying cameras on the streets).

However, it is recommended to perform a DPIA before starting any data collection from data subjects in any pilots.

- 9) Clear procedures must be in place to ensure **data subjects' rights**, namely:
- a. Right of access to their data and to receive any important information on what it is done with the data;
 - b. Right to rectification, when the personal data are processed in a non-accurate way;
 - c. Right to erasure, under certain conditions, in particular when data have been processed unlawfully or are no longer necessary;
 - d. Right to restriction, meaning the right to "freeze" data and obtain that they are not processed for a certain period of time, for example when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data);
 - e. Right to data portability;
 - f. Right to object.
- 10) Procedures to handle and notify Data Breaches to Data Protection Authorities and Data Subjects concerned must be in place.
- 11) Data collected on the data subject should be strictly necessary for the specific purpose previously determined by the data controller (the "**data minimization**" principle). Data that is unnecessary for that purpose should not be collected and stored "just in case" or because "it might be useful later". For example, if a large scale event organizer needs generic data of people attending a concert, in order to issue tickets and organize the space in the venue, it would be not necessary and therefore disproportionate to collect information on the attendees' relatives in order to derive fine insights on the socio-economic cluster to which the attendees belong, which can

then be used for targeted advertising.

- 12) Data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.
- 13) The purpose for which the data were collected or further processed determines the length of time for which the data should be kept. Once the data are no longer needed they should either be deleted or kept in anonymous form if they serve historical, statistical or scientific uses.
- 14) In cases of secondary processing of research and scientific data previously obtained for other research purposes can be used in so far as they are not incompatible. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations.

2.3.2 List of Key ePrivacy Directive Principles

- 1) Where the ePrivacy Directive provides for a specific rule applicable to natural and legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks, it prevails over the general rule set out by the GDPR ("Lex Specialis derogat generali"- **Principle of Specialty**).
- 2) Electronic Communication Services and Networks must be secured through appropriate technical and organizational measures. (**Security**)
- 3) The confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, must be ensured (**Confidentiality**)
- 4) Access to, or storage of, information into the users' devices must be authorized by the users with a specific consent, unless it is "*strictly necessary in order to provide a service explicitly requested by the subscriber or user*" (so called "cookie law", **Prior Consent**) In other words, any website, or app should provide clear information on its the cookies it deploys into the users' devices and collect the prior consent, where necessary
- 5) **Principles applicable to Traffic Data**
 - a. Traffic data **must be erased or made anonymous** when it is no longer needed for the purpose of the transmission of a communication or for the purposes of processing subscriber's billing and interconnection payments (**Traffic data erasure**)
 - b. Traffic data can be processed for marketing and/or for the provision of value added services **only upon specific consent** of the user concerned (**Consent for Marketing purposes**)

- c. **Specific information on traffic data processing and its duration** must be provided (**Specific Information**);
- d. **Traffic data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary** (e.g. handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service – **Authorization profiles**)

6) Principles applicable to **Location Data**:

- a. Location data can be processed for the provision of value added services **only anonymously or upon specific consent** of the user concerned (**Consent for Location Data**)
- b. Users must be given the opportunity to easily refuse such processing at each connection (**Updated Consent**)
- c. Location data must be processed only by persons under the authority of the service provider that are dedicated to the function or unit for which such data are necessary (**Authorization profiles**)

2.4 CONSORTIA'S DATA PROTECTION STRATEGY AND COMPLIANCE

The first task to complete, by each Consortium running an IoT LSP project, is to clarify who is in charge of what, and more specifically, who are the data controller(s) and the data processor(s). This requires to clarify and to define the Consortium's Privacy Organisational Scheme. Be aware that a LSP may involve several Data Controllers and Several Data Processors. The Scheme should clarify:

What personal data are/will be collected: by listing the various data sets that will be collected and assessing their potential qualification as "personal data";

If the Consortium legally exists with a distinct legal personality (established as a society) and who endorses the responsibility for the consortium acts. If there is not a specific legal entity assuming the responsibility for the project, the responsibility will be shared by the consortium members who act as de facto data controllers, alone or jointly;

Who are the various stakeholders / entities involved in data processing for the project, by making a detailed list and drawing a map of data flows among these entities. It is suggested to distinguish non-personal data flows from data flows that include personal data (Figure 1 provides a simple example of Data Flow Scheme in a smart city use case)

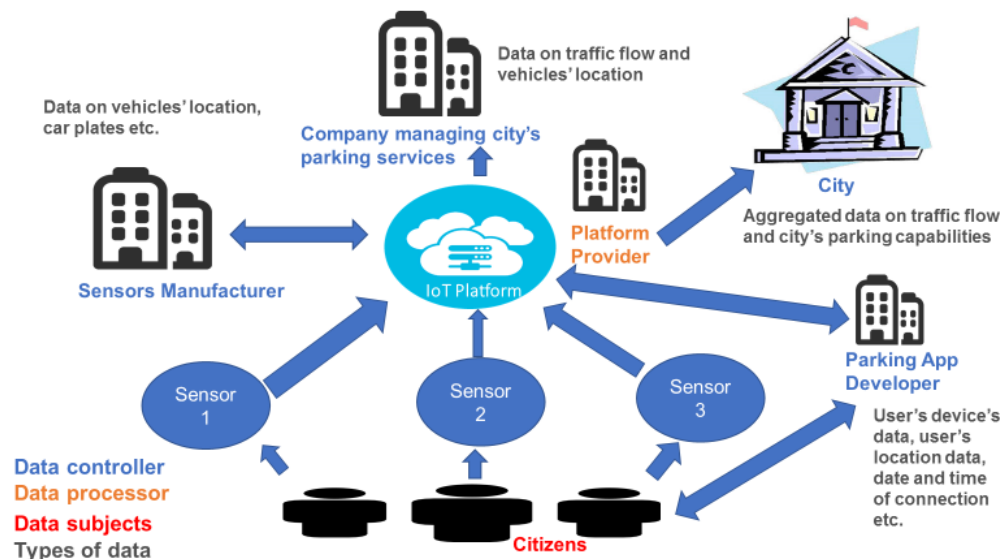


Figure 1: Data Flow Scheme in a Smart City Use Case

Who is/are the Data controller(s): The analysis should encompass each category of collected data.

Who is/are the Data Processor(s):

- If the Consortium acts as a sole data controller (e.g. Website management, processing of personal data for administrative purposes etc.);
- If and when a Partner has to be considered as a joint data controller together with other relevant Partners (e.g. in the creation call process, in the design and management of the project's facilities, during the experiments);
- If and when the Consortium (or one of its partners) will act as a data processor (e.g. As a provider of technological services in the course of an experiment);

Where (in which countries) the projects' systems and the databases should be located (of course it will depend also on the involved third parties).

If the project centralizes the facility or distribute it among Partners.

If any cloud computing solutions are expected to be adopted and, if yes, provided by whom.

In order to achieve this objective, it is preliminary to map exactly who does what within the Consortium, and to clarify the relevant roles in relation to the phases of the project that may be defined as "data-protection critical", in that they entail the collection and processing of personal data.

Each Consortium should carry out this thorough exercise.

2.4.1 Data Protection Officer (DPO) function

The GDPR defines the role and responsibility of a Data Protection Officer (DPO). The DPO is in charge of monitoring the application of the GDPR within an organization and providing strategic advice to it on how to process personal data while respecting individuals' rights.

LSPs are usually involving several testbeds or deployments controlled by different partners. Each Data Controller (the partner who has the effective control on the data collection) should have a clearly identified DPO.

At the overall project level, **each Consortium should also appoint a Project DPO**, which will be in charge of:

- Establishing common rules and requirements for the consortium data protection policy;
- Coordinating the action and information among the various DPOs;
- Serving as an entry point to answer questions and complaints from third parties when addressed to the project as a whole.
- Providing guidance on how to implement the privacy by design and by default principles

The appointment of a DPO represents a valuable step towards a better protection for personal data within the projects and puts the Consortia in line with the forthcoming rules on data protection established by the GDPR expected to be approved by the end of the year.

For Public Authorities and Bodies within the Consortia the designation of a DPO is mandatory according to the General Data Protection Regulation.

The DPO may be a staff member of the controller or processor, or fulfill the tasks on the basis of a service contract.

For LSPs it is recommended to designate:

1. A General DPO at the consortium level
2. Local DPOs for each individual partner controlling one or more pilot sites

The Local DPOs should report and work in close coordination with the General DPO.

2.4.1.1 Roles and missions of the DPO

The roles and mission of the DPO are:

- to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to data protection law;
- to monitor compliance with data protection law and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authority;
- to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation when required by data protection law, and to consult, where appropriate, with regard to any other matter.

Principles to respect:

- The DPO should be autonomous and in a position to freely raise issues and relay them internally without any limitations.
- The DPO shall be provided with the resources necessary to carry out his/her tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

As part and parcel of the above-mentioned Privacy Policy **each Consortium should establish an internal procedure for the management of the data subjects' requests**, in order to smoothly let data subjects exercise their data protection rights and promptly reply to them.

2.4.2 Adopting formal data protection policies and rules

Furthermore, **each Consortium should adopt an internal Data Protection Policy, that may be added to the Consortium Agreement**; all Partners should sign it so as to be contractually bound to abide its provisions.

Any person who is likely to have access to personal data should be contractually bound to respect and protect personal data. If the contractual clauses do not yet include specific and comprehensive clauses to protect personal data in line with the GDPR, these persons who have access to the data should sign a contractual agreement including a formal commitment to respect the project's Data Protection Policy and Rules before accessing the data.

As part and parcel of the above-mentioned Privacy Policy **each Consortium should establish clear procedures for the management of the data subjects' requests**, in order to smoothly let data subjects exercise their data protection rights and promptly reply to them. The users (data subjects) involved in the project should be informed on these procedures and should have an easy access to the Data Protection Officer(s), for instance through the website.

2.4.3 Records of processing

Records of processing activities can be defined as a repository of all the personal data processing carried out by data controllers and data processors, a map of what they do, for what purpose, on whose behalf and under what safeguards. They are a mandatory tool for companies above 250 employees or for companies which are anyway engaged in risky processing. Records of processing are regarded as a crucial proof of accountability on the side of complex organizations.

Each of the LSPs should adopt a tool similar to the records of processing provided for by Article 30 GDPR ⁴, in order to map the processing activities taking place within the project and understand the privacy implications. The DPO of each project should be entrusted with the coordination of the relevant partners and stakeholders which have to assist him/her in compiling, updating and maintaining the records.

2.5 PRIVACY BY DESIGN APPROACH IN THE LSPS

Every time there is a need to deploy an IT facility, sensors, or start processes (hereinafter "Target") which may even only potentially entail the collection and processing of personal data of users, citizens, employees, steps should be taken to ensure that the privacy by design principle is followed. The following diagram guides the relevant project manager through the steps of an horizontal Privacy By Design approach, which can be applied to any personal data processing envisaged by any of the 5 IoT LSPs.

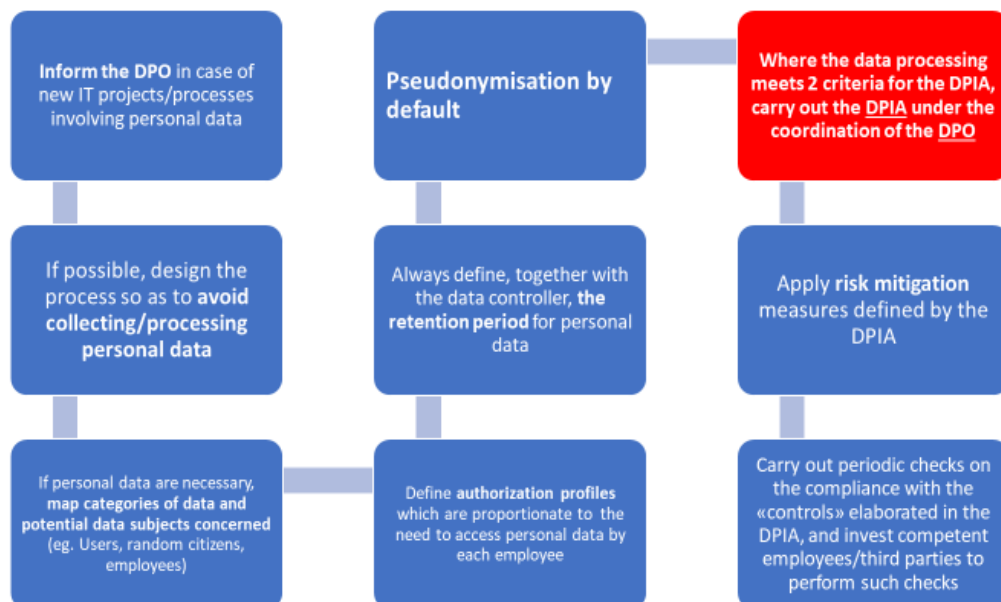


Figure 2: Privacy by Design Approach

- 1. Data Protection Impact Assessment** for each of the envisaged target, if two or more of the criteria listed in ANNEX C are met. The DPIA is compulsory for projects using new technologies, in particular when implying the monitoring of large spaces accessible to the public (such as smart cities project). The result of the DPIAs should be documented and kept available. It may be incorporated in the relevant Deliverables related to each of the target. The assessment should contain:

⁴ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

- a general description of the envisaged processing operations;
- an assessment of the risks to the rights and freedoms of data subjects;
- the measures envisaged to address the risks; safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with applicable policies and law.

By carrying out a DPIA in advance, the projects will anticipate the effect of the provisions of the GDPR that require data controllers to carry out a DPIA for risky processing of personal data. The DPIAs are crucial to ascertain if and where the targets are vulnerable to threats, what are those threats and how to reduce risks for the personal data processed therein. The DPIA is the first step taken by the data controllers in the application of the privacy by design approach.

2. Compliance with fundamental data protection principles

Transparency: the projects' managers, and each stakeholder working within, or associated to, the project will inform data subjects about all (data protection) relevant aspects of the targets; in particular, data subjects should be informed about all entities (including potential subcontractors) contributing to the provision of the respective target and all locations in which data may be stored or processed by the target manager or its subcontractors (notably, if some or all locations are outside of the European Economic Area (EEA)); the data subjects should be provided with meaningful information about technical and organizational measures implemented by within the target;

Purpose specification and limitation: each stakeholder working within, or associated to, the project, should ensure compliance with purpose specification and limitation principles and ensure that no data is processed for further purposes by the target provider or any subcontractors. Commitments in this respect may be captured in appropriate contractual measures (including technical and organizational safeguards);

Data retention: each stakeholder working within, or associated to, the project should be made responsible for ensuring that personal data are erased (by the target provider and any subcontractors) from wherever they are stored as soon as they are no longer necessary for the specific purposes; secure erasure mechanisms (destruction, demagnetisation, overwriting) will be provided for contractually.

3. Security Measures to be implemented in the target (see also paragraph 6 below for further details)

- Physical security policy/measures (backup power, physical access control protection measures, etc.);
- Network redundancy, geographic spread, availability zones, access control;
- Backups and failover mechanisms;
- Disaster recovery plans/Recovery time objectives;

- Service continuity in case of legal issues, administrative disputes, confiscation by law enforcement, etc.;
- General policy and approach to managing security risks;
- Contact point for security incidents;
- Compliance with best practices or industry standard on governance or risk management (Supporting evidence/guarantees);
- Certification against information security risk management standards (for example ISO/IEC 27001⁵), including scope statement;
- Self-assessment against an industry standard or best practice;
- Third-party audits;
- Logical access control protection (roles, permissions, privilege minimization, privilege segregation);
- Authentication/Authorization mechanisms;
- Protection measures for administrator interfaces;
- Authentication for administration interface;
- IP restrictions, administrator roles and privileges;
- Incident classification and response/recovery time objectives;
- Encryption of data;
- Anonymization or Pseudonymization by default, unless personal identifiable data are necessary;
- Adoption of Secure Protocols for data communication against the risk of data breaches.

4. The targets and the projects should ensure data subject's rights, through:

- Clear and easy contact procedures;
- Prompt replies to data subject's requests;
- Privacy dashboard/control panel so as to allow data subjects to keep control over their personal data.

⁵ ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements

2.6 CO-CREATION PROCESSES (WHERE FORESEEN)

A key ambition of some of the LSPs is to make the creation and design of technologies and services more inclusive for citizens and communities. In Synchronicity, for example, the co-creation process aims to tackle the question of how smart cities can be organically grown from citizens and communities instead of being engineered by the vision of large corporates and city governments alone.

In order to achieve this objective projects engage citizens, researchers, technology and service providers, to jointly participate in a co-creation process, in order to look for more effective and affordable solutions, through a better exploitation of already-available resources.

On top of the ones applicable to the project as a whole, the co-creation call phases should be accompanied by further measures taken by the Consortia as a way to protect the personal data of the involved stakeholders.

1. *Clear information to participants of the co-creation phase should be provided, also by means of context-tailored privacy policies, icons and short descriptive texts on social networks.*
2. *The participants should be asked a prior consent before being contacted; in fact, contacting and targeting potential participants beforehand is normally not allowed without consent.*
3. *Personal information should be separated from opinions/ideas expressed by participants during the procedure;*
4. *When the process will entail interviews of the participants in order to collect, for example, information regarding lifestyles, personal information collected should be aggregated as soon as possible.*

2.7 OPEN CALLS

The open calls phase is crucial for the projects and for the level of data protection safeguards going to be implemented during the subsequent stages. On one hand, the Consortia should make sure that personal data are protected during the open call procedure, by means of the following safeguards:

1. A dedicated privacy policy should be embedded in the notice of call (defining roles, communication of data, data retention, participants' privacy rights, consequences of participation/consent)
2. A helpdesk should be kept open during the call period;
3. Participants' withdrawals and data protection rights should be enforced during the open call period. This should include the enforcement of their right to be forgotten, as the case may be, after having performed the assessment prescribed by the Court of Justice of the European Union In case C-131-12.

On the other hand, the need to protect personal data must be a criterion through which proposals are assessed, in order for the project to run experiments that best suit the primary objective of enhancing data protection. In order to do so, the **notice of call/criteria** should contain the following elements:

1. A definition of the ethics/privacy criteria that should be taken into account during the evaluation phase, such as:
 - Clear and trustworthy identification of the privacy and other fundamental rights risks entailed by the proposal;
 - Clear and sound remediation measures to the identified risks;
 - Privacy by design and Privacy by default solutions;
 - Effectiveness of security measures (protection against third parties' intrusion, anonymisation etc.)
2. Each element of the proposal (amongst which privacy) could have a weight which could be predetermined beforehand in the notice of call itself (for example, privacy may account for 1 third of the overall total score attributed to a given proposal);
3. Criteria to evaluate procedures for the enforcement of data subjects' rights (priority could be given to innovative/user-centric solutions, such as dashboards and control panels, push up alerts to data subjects of «extraordinary» processing of data)
4. A clause that clearly mandates the participants to identify the legal basis on which data processing take place.

2.8 COMPLAINTS MANAGEMENT

Each LSP should have in place a policy to manage the complaints and/or the requests lodged by users, citizens and other people concerned by the processing of personal data.

The policy should be shared with all the partners of each LSP and be legally signed and accepted by them, with at least the following elements:

1. Need to have a clear contact page on the LSP website with a description of the complaint procedure;
2. List of the various DPOs for each pilot, with relevant contact details;
3. The LSP partners shall not refuse to act on the request of the users, citizens and other concerned people for exercising their rights;
4. If the users, citizens and other concerned people exercising their privacy rights are not identifiable, the DPO of the Consortium or the DPOs of each partner concerned should inform the requesting party that it is not possible to identify them;
5. LSPs and their partners should not be obliged to request additional information to identify the users, citizens and other concerned people, but if they provide those details voluntarily, LSPs and their partners shall act upon the request;
6. Requests shall be dealt with by no later than one month from the date they are lodged, regardless of when they are actually seen by the LSPs or partners' DPO. It is therefore very important to actively monitor the communication channels through which such requests can be sent.
7. If necessary, relevant people of the LSPs' staff shall be involved in replying to the requests (e.g. IT people, Directors etc).
8. Replies to the requests shall be clear, concise and complete; if the request is ill founded, LSPs should provide explanations on why they cannot react upon it.

2.9 DATA BREACH POLICY

Each LSP should have in place a policy to manage the data breaches. The policy should be shared with all the partners of each LSP and be legally signed and accepted by them, with at least the following elements:

1. Once discovered, the data breach should be immediately communicated to the competent DPO;
2. The DPO will perform a first assessment of the case in order to appraise whether:
The breach poses a risk to the rights and freedoms of users, citizens and other people concerned by the processing of personal data;
The breach poses a high risk to the rights and freedoms of users, citizens and other people concerned by the processing of personal data;
3. In each of the case sub 2), the DPO shall swiftly involve and inform the LSP's hierarchy, in order to take the appropriate measures;
4. In the case sub 2 let. a) above, the LSP, with the support of the DPO, shall notify the breach to the competent supervisory authority, within 72 hours from the time they became aware of the breach
5. The notification shall:
 - describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - describe the likely consequences of the personal data breach;
 - describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
6. In the case sub 2 let. b) above, the LSP, with the support of the DPO, shall communicate the breach to the affected users, citizens, and people concerned without undue delay.
7. The communication shall describe in clear and plain language the nature of the personal data breach, and in particular the elements listed under 5, let. b), c) and d) above;
8. In case of a breach, remediation measures shall be applied as soon as possible, with the help of IT experts and with the involvement of the LSPs hierarchy;
9. In case the LSPs or the LSPs partners have engaged data processors for the purpose of carrying out the project's activities, they shall be bound to notify the data breach to the LSPs without delay;

10. The LSPs shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with the GDPR.

2.10 PRIVACY APP

The use of ad hoc tools, such as the Privacy App developed in the context of the Synchronicity LSP can constitute useful tools to comply with the obligation of transparency and information towards the data subjects. More information is available on the Privacy App website.

2.11 PROJECTS' TECHNICAL AND SECURITY MEASURES OVERVIEW

Technical Measures should be implemented by the Consortia as described in this paragraph. They could form part of the projects' privacy policy, and be published on their websites.

The Consortia should implement measures with a view to minimize the security risks in the course of processing personal data by means of the facility and throughout the projects. The Consortia's security policies should be designed so as to cope with the obligation to process data in a secure fashion, as provided for by Articles 17 of Directive 95/46/EC and 32 of Regulation 679/2016⁶. In order to do so, the Consortia should apply the list of safeguards detailed in Annex A.

2.12 DATA RECOMMENDATIONS FOR DIFFERENTS STAKEHOLDERS IN THE IOT DOMAIN

A set of recommendations can be drawn by Article 29 Working Party's Opinion 8/2014 on Recent Developments on the IoT. Recommendations are divided in the following categories:

1. **Recommendations common to all stakeholders**
2. **Application developers**
3. **Social platforms**
4. **IoT device owners and additional recipients**

Extract in Annex B.

⁶ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

3 PRIVACY GAME – A SERIOUS GAME ON DATA PROTECTION

3.1 INTRODUCTION

In this section the privacy game is presented: objectives, requirements, target users, planning and methodology, key concepts to communicate, question design, tests and validations, game rules, expansion, dissemination and online game.

Serious games are used more and more often by companies [15], institutions and organisations as an excellent tool to raise awareness about important topics. They are used to encourage reflexions on very different subjects such as ecology, migrations, racism, homophobia, democracy and others [1-21]. There is now a vast literature on serious games, and also a precise classification was proposed [1]. The learning objectives are integrated in the games, so that the players can learn during the ludic experience.

The newly adopted GDPR imposes complex rules and obligations that must be respected by the 5 LSPs. Beyond the legal and financial risks for those who would not respect them, LSPs have the duty to prevent any reputational risk that could indirectly impact the European Commission, the H2020 research programme and the aim of the LSPs that intends to promote the adoptions of IoT technologies by the end-users and the market in general.

U4IoT aims at promoting a GDPR-compliant end-user engagement in the LSPs. It intends to contribute to the respect of end-user data protection rights, and to reduce the risks of non-compliance by the LSPs. The support encompasses end-user engagement in the five LSPs financed by the European Commission and other partners, such as the Swiss Ministry for Research and Education.

In this context, Archimede Solutions (AS) has led the development of a serious game to raise awareness and assimilate GDPR rules, principles and obligations in connection with the LSPs. This privacy game is meant to help the LSPs stakeholders to learn the fundamental principles of data protection, to raise awareness on the main risks related to data protection with IoT deployments, translating complex legal norms into clear and easily understandable principles. It is aimed at LSP consortia, LSP end-users and large public. The game is meant to be easily understandable, enjoyable and educative, covering the IoT privacy risks and all main definitions and principles of the GDPR. It follows a clear iterative methodology of game design, playtest, analysis and improvements. The game is to be disseminated through privacy seminars, LSP events, game festivals and more.

3.2 OBJECTIVES OF THE SERIOUS GAME

The aims of the serious game on data protection are fully aligned with the U4IoT goals. More specifically, the serious game targets the following objectives:

- To help the LSPs stakeholders to learn the key principles of data protection, as indicated by the General Data Protection Regulation. The LSPs are mainly focused on the technical aspects to realise and implement their projects. However, all partner that work in these projects should be aware of the privacy and data protection issues that raise in the IoT field, and they do not necessarily have a legal background, so one of the tasks of U4IoT is to help the LSPs to know the privacy aspects of the new GDPR.
- To raise awareness on the main risks related to data protection with IoT deployments. In fact, the IoT deployments present not neglectable data protection risks, such as the absence of legal ground or prior informed consent, a lack of data minimisation and purpose limitation, etc. The risks are particularly higher with the GDPR new obligations in the domain of management of data protection, such as the new rules on extraterritoriality, on sensitive data, on data controllers and data processors, etc.
- To serve as a useful tool for the LSPs. The aim is to meet the needs of the LSPs and from this point of view, the privacy game could not only be used by the LSP collaborators, but also by the LSP end users, in other words the LSPs will be able to use it in order to raise awareness about privacy and data protection issues among their users. Therefore, the game could be a useful tool that the LSPs themselves could use when they will need to launch their solutions and to address their potential users.
- To translate complex legal norms into clear and easily understandable operational principles. The legal language is often difficult to understand, and it implies technicalities. For these reasons it is important to explain with an easy language and through practical examples the privacy and data protection concepts to be communicated. Many examples will be integrated in real situations in which the players will have to take a role and try to understand which their rights or obligations are.
- To reduce the risks of non-compliance with the GDPR in the five LSPs. Non-compliance with the norms of the GDPR could mean stiff fines for the entity who did not respect the law. Fines up to 20 million € or (for companies) 4% of the annual turnover, whichever is higher, will be a risk that many entities could be unbearable. For this reason, for many stakeholders in the LSPs, it will be important to understand and minimise these risks, distinguishing to which aspects will be most important to pay attention.
- To demonstrate successful adoption and use by a significant number of players in the five LSPs. The fact that many LSP stakeholders will use the game among their collaborators and end-users will show the usefulness of the game and the efficacy of this ludic approach.

Finally, the task will evaluate and demonstrate the achievement of the above-mentioned objectives. Surveys and tests will be run to check at which degree these goals will be met. Statistical analysis will be provided for the measurable parameters and qualitative analysis will be provided for the non-measurable parameters, such as judgements and general comments of the play-testers.

The task will also extract learnt experiences to improve and guide the development of future serious games on privacy. At the end of the projects the positive and negative feedback will be collected to show suggestions for future improvements and developments, or for other projects that would like to analyze this work, taking inspiration for other similar serious games.

3.3 TARGET GROUPS OF USERS

It is important to clarify the target groups of users, this allows to determine the focus of the serious game and the following development. This focus is essential in order to evaluate the content of the serious game, the level of difficulty, the level of interaction, the keys to stimulate participation, the means of dissemination and the ways in which the serious game will be played.

It is also important to estimate for each group of users, which is their level of knowledge and education about privacy. This allows to create a game that is adapted to the users' needs and expectations. It is important to estimate the range of the levels of education of the users, in order to satisfy all these different levels, so that some parts of the game will be challenging for some users and other parts of the game will be challenging for other users.

The game intends to serve and address the following groups of users, in decreasing priority:

- LSP consortia: the members of the consortia in charge of implementing and deploying the LSPs are the top priority group. It is assumed that they are likely to have a high level of education, but probably no previous education in law. They therefore shall learn the key principles of data protection, as defined in the GDPR.
- The end-users of the 5 LSPs who will be exposed to the IoT pilots. They can benefit from the game to better understand the risks related to IoT deployments and the means to mitigate these risks. The LSPs include very heterogeneous end users: farmers, event organisers, engineers, physicians, health carers, etc. It is assumed that they do not necessarily have a superior education.
- The public in general. We make the assumption that all users do not necessarily have a superior education, and probably no legal education at all.

3.4 REQUIREMENTS OF THE SERIOUS GAME

It is key to understand and follow the requirements of the serious game. This allows focusing the development of the game on the aims and takes into consideration the target groups of users. The set of the requirements gives the framework in which the game will be developed and guides the process of creation of the serious game.

The game must comply with the following requirements:

- **Be understandable to players** with limited Knowledge and no previous legal background at all. Although some target players will be partners of the LSPs that have already a legal background, most target players will not have a legal background, so the game must present legal concept integrated in real situations and explaining the context. Every adult player should be able to understand the game.
- **Encompass the main principles and obligations** related to the data protection obligations. We will identify the main definitions and principles and we will cover all of them through different sections of the game, so that each concept will be covered at least once, and many concepts will be covered more than once.
- **Cover specific risks related to the 5 LSPs.** In order to do so, for each LSP there will be a dedicated section of the game, that will represent scenarios for that LSP. In each LSP section there will be different scenarios that will address different privacy risks for that LSP.
- **Be effectively educative:** players must learn the key concepts related to the GDPR. The game scenarios and questions will allow the players to understand the main definitions and legal principles of the GDPR. After each question there will be an answer with an explanation, so that the participants will be able not only to identify themselves in the situation, trying to find an answer or a solution, but also to read some details in the answer that will clarify the law, referring to the GDPR articles.
- **Conform with the GDPR** and other relevant and applicable European personal data protection rules and regulations. All legal details, questions, answers and scenarios will be reviewed by lawyers specialised in privacy, so that every detail, theoretical question or practical situation, will be correctly analysed.
- **Be user friendly:** the game must be easy to understand and to play. The game is aimed at being playable in small sessions from 5-15 minutes on, so that will be playable also in short breaks. Also, the texts and the rules will be straightforward in order to guarantee an optimal playability, also for people not used to play games.
- **Be enjoyable:** the game must be enjoyable to be played and adopted by users that will play it with pleasure. The challenge of the task is to make enjoyable a subject that is normally considered quite unfriendly and complicated. For this aim, the game will present concrete scenarios in order to allow the players to identify themselves in real situations.
- **Be cost effective:** the project did not allocate any substantial budget to implement the game and it must be effectively accessible to all the LSPs in a cost-efficient manner. For example, the question game will be playable with cards or online.
- **Be scalable:** the game must be scalable in terms of number of users/players, with a minimal marginal cost. It must be taken into consideration the possibility to receive interest from a larger public, and in this case it should be possible to satisfy the requests.
- **Be easily accessible:** to remote users without costly distribution channels. The online version of the game will allow to make the game accessible on the internet. The online game will be the same as the physical game, it will be just adapted to be played on the internet.

3.5 PLANNING AND METHODOLOGY

A clear methodology is also a fundamental element that allows to follow a well determined path in the creation of the serious game. The methodology consists of, on the one hand, the collection of empirical data under the guidance of hypotheses and theories to be tested; on the other hand, the rigorous analysis of these data.

The choice of a method derives from a decision-making process. It not only affects the assessment of the nature of the practical problems, but also the need to respect the requirements. It is important to establish a balance between these different limits.

The development of the serious game follows a clear methodology of end-user driven design and development. Several iterative cycles of development of the game enabled to test, refine and validate the game. The methodology was sequenced in three distinct phases:

- The Requirements Analysis (M1-M6). During this phase, the requirements were studied, in parallel with an examination of the GDPR, and the extraction and selection of the key definitions and principles. Moreover, a thorough analysis of serious games was performed, and this will allow to compare this kind of games in the domain of privacy and in other domains, extracting the best ideas and characteristics of these games.
- Game Development (M4-M18), with several iteration cycles, including:
 - a. *Game design*. Creation of a version of the game, integrating the requirement analysis in a concrete ludic mechanism that allowed the communication of the key concepts of the GDPR.
 - b. *End-user tests and validation*, with a clearly defined methodology on the key dimensions to be tested and validated. These tests were followed by questionnaires that asked the play-testers their appreciation, comments and suggestions on different aspects of the game
 - c. *End-user tests results analysis*. For the quantitative answers, statistical analysis is provided, and for the qualitative answers, a general overview is provided, summarizing the key elements.
 - d. *Identified adaptations and improvements* that retro-fed the game design process in order to improve it. The analysis of the tests was implemented in the following version of the game, taking into account whenever possible the feedbacks of the play-testers.
- The Privacy Game dissemination (M19-M36) towards LSPs ecosystems and other potential users. The game was and will be presented in LSP meetings (such as IoT Week Geneva in June 2017, LSP meeting Brussels in October 2017, IoT Week Bilbao in June 2018) and in game festivals (such as Ludesco 2017, Ludesco 2018, Game Creators Meeting 2018), and seminars about privacy (including the privacy guidelines and the privacy game) will be proposed to LSPs.

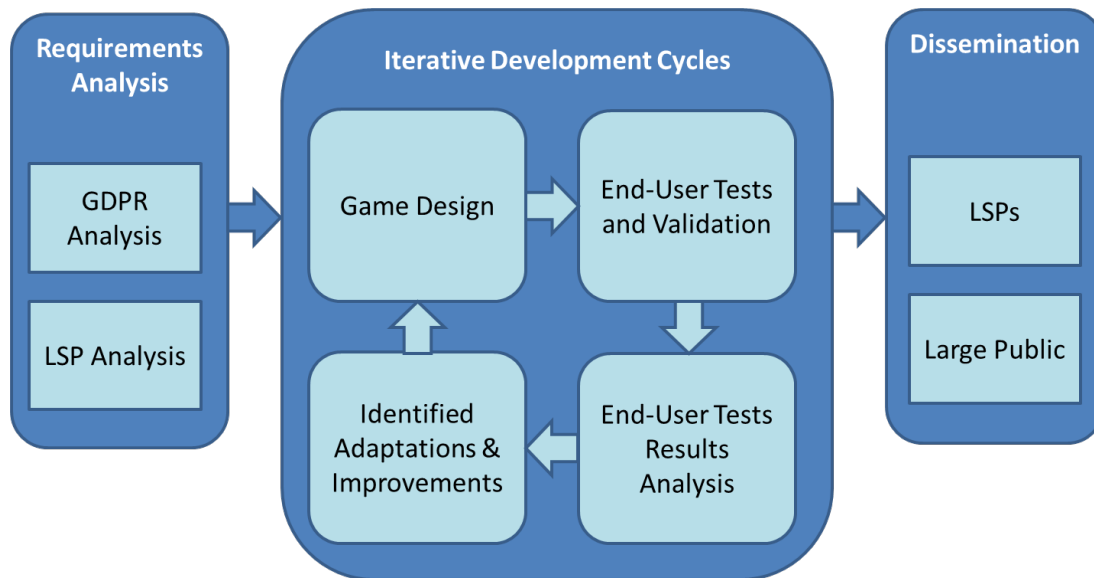


Figure 3: Methodology of end-user driven design and development

Concerning the game design, the key concepts to communicate (see section 2.6) were chosen by taking into consideration primarily the relevance to the LSPs and secondarily their playability.

3.5.1 Importance of concepts to communicate

Importance means that some topics are of particular interest for the IoT applications of the LSPs. For example, the difference between pseudonymisation and anonymisation, or that one between data controllers and data processors, are particularly important for the LSP because they have to collect, process and store large data sets.

Here some examples are presented.

Increased territorial scope

The extra-EU jurisdiction provided for by the GDPR applies to all companies processing the personal data of data subjects living in the EU, independently of where the company is based. Previously, territorial reach of the EU Data Protection directive 95/46/EC was unclear and talked about data process 'in context of an establishment'. This issue has arisen in several important court cases⁷. GDPR makes its territorial scope very clear - it will apply to the processing of personal data by controllers and processors in the EU, independently of whether the processing is done in the EU or not. The GDPR will also apply to the processing of personal data of data subjects in the EU by a controller or processor not based in the EU, if the activities relate to: offering goods or

⁷ CJEU ruling: Google Spain SL v. Costeja, C-131/12, 13th of May 2014 – in which the Court had confirmed a broad application of territorial scope of the Directive 95/46/EC with regard to the definition of establishment. CJEU ruling: Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, 1st October 2015 – in which the Court had confirmed that if a data controller exercises "a real and effective activity – even a minimal one" through "stable arrangements" in the territory of a Member State, it will be considered to have an "establishment" in that Member State, thus the Directive 95/46/EC applies.

services to EU citizens (even without payment) and the monitoring of behaviour that is done within the EU. Companies outside EU processing the data of EU citizens will also have to appoint a representative in the EU.

Fines

Companies in breach of GDPR can be fined up to 4% of annual global turnover or €20 Million (whichever is greater). This is the highest fine that can be imposed for the most serious breaches, e.g. not having adequate client consent to process information or disregarding the Privacy by Design concepts. Depending on the type of the breach the fines can be lower, e.g. 2% of annual global turnover or €10 Million (whichever is greater) if the company did not conduct a privacy impact assessment. These norms apply not only to controllers but now also to processors, so also to web clouds.

Consent

The conditions for consent have been reinforced, and organizations will not have any more the possibility to use long obscure terms and conditions with difficult legal words, as the demand for consent must be given in a clear form⁸ attaching to the description of the aims of the data processing⁹.

Notification of breaches

Controllers must report data breaches to their supervisory authority (unless the breach is unlikely to be a risk for individuals) within 72 hours after having become aware of the breach¹⁰.

3.5.2 Playability

With “playability” we mean that some concepts are more fit than others to be converted in an interesting question for the game. Some questions may also be too complex and beyond the priority objectives of the serious game.

Questions were tailored to enable multiple answers. For example, the age until which the consent from a child concerning online services is valid only if authorized by a parent is a piece of information that easily allows to create a question with multiple choices in which only one is the right answer as illustrated below:

“In the GDPR (General Data Protection Regulation) the consent from a child concerning online services will be valid only if authorized by a parent. Until which age of the child?”

A) 10 B) 11 C) 12 D) 16 E) 18”

⁸ References: Art. 4 (11) GDPR

⁹References: Art. 6 (1) (a) GDPR

¹⁰ References: Art. 33 GDPR

3.6 KEY CONCEPTS TO COMMUNICATE

The educational aim of the Privacy Game is to allow the players to learn some serious concepts in an entertaining way. These concepts are related to general privacy and data protection notions, to specific privacy theories contained in the new European GDPR, to their application to IoT and more specifically to the IoT issues present in the 5 LSPs.

More specifically, the Privacy Game should explain:

- **The key definitions** in simple terms: personal data, data subject, data controller, data processor, prior informed consent, etc. The analysis of these definitions will be essential to provide the language used in the privacy domain, in order to clarify terms that may be known, but that sometimes are not fully and precisely understood.
- **The key principles and obligations of the GDPR:** territorial scope¹¹, purpose limitation¹², data minimisation¹³, etc. The analysis of the principles is based on that of the definitions and using the terms and the language learnt will introduce the main ideas that the players will learn through the different sections and scenarios.
- **The main risks related to data protection with the IoT pilots.** It is very important to raise awareness about the risks that both the LSPs, and their end-users run in the framework of the IoT pilots. For the LSPs it will be also particularly important become aware of the financial risks connected to the potential fines they could receive in cases of non-compliance to the GDPR.
- **The distinction between the various categories of data.** For example, the difference between personal data and non-personal data (linked to the identifiability of the data subject), the difference between sensitive and non-sensitive data, the difference between sensors that can collect personal data and other that cannot.

The Privacy Game should **cover both general requirements and LSP-specific requirements**. These explanations will happen in two ways: first, through some introduction texts or cards that will present these concepts as general knowledge useful for the game; second, through the explanations to the questions and to the presented scenarios.

After analysing the GDPR and extracting the main obligations, we have established a list of key topics to be presented and explained through the game:

¹¹ Reference: art. 3 GDPR, Recital 22-25 GDPR

¹² Reference: art. 5(1)(b) GDPR, Recital 39 GDPR

¹³ Reference: art. 5 (1)(c) GDPR, Recital 39 GDPR

3.6.1 Key definitions

- | | |
|---------------------|-------------------|
| 1) Personal data | 6) Sensitive data |
| 2) Anonymisation | 7) Genetic data |
| 3) Pseudonymisation | 8) Biometric data |
| 4) Data controllers | 9) Data subject |
| 5) Data processors | 10) Profiling |

3.6.2 Key principles

- | | |
|---|---|
| 1) Territorial scope | 12) Right to restriction of processing |
| 2) Purpose limitation | 13) Right of the user to withdraw his/her consent |
| 3) Data minimisation | 14) Right to data portability |
| 4) Prior informed consent - Conditions for consent | 15) Notification of a personal data breach to the supervisory authority |
| 5) Child's consent | 16) Data protection impact assessment |
| 6) Processing of personal data relating to criminal convictions | 17) Data protection officer |
| 7) Transparency | 18) General conditions for imposing administrative fines |
| 8) Right to access | 19) National derogations |
| 9) Right to rectification | 20) Transfer of personal data outside the EU |
| 10) Right to erasure | |
| 11) Right to object to data processing | |

As explained in section 2.5, these topics were chosen taking into consideration primarily their importance for LSPs and secondarily their playability.

3.7 METHODOLOGICAL APPROACH FOR QUESTION DESIGN

In order to create a game that takes into account the described objectives, target users, requirements and key concepts to be communicated, three main options were analysed:

- a board game
- a card game
- and a quiz

Compared with the other options, the board game would include more graphic design (for the board), higher production costs and a bigger duration. Therefore, considering the stated goals, it seemed a less interesting option.

The card game would be a game without board and with cards to be collected or exchanged among the players, e.g. cards representing data, LSP stakeholders and/or end-users.

A quiz would include only question cards. It was decided to create a quiz, because it allows to focus directly on the main goal, i.e. to analyse a situation understanding how GDPR applies. In this way the players can play even if they have only a few minutes, the rules are straightforward, and most of the time is used to learn. Being a fast and flexible game, the quiz is also best suited for the dissemination of the privacy game.

The card game would be slower, but it would be also lighter and more playful, and it was decided to leave it as a possible expansion of the quiz. Indeed in 2018 it was begun the development of a card game as expansion of the quiz, it will be described in paragraph 2.14. Now the quiz game will be analysed.

In order to develop a set of questions that are aligned with the objectives of the game and with the key concepts to be communicated, we decided to split the questions in two categories:

- General: this section contains questions about GDPR in general applied to different domains.
- Domain specific: these questions are conceived for the 5 domains of the 5 LSPs, and propose situations contextualised in these fields.

For the domain specific questions, we decided to focus on the thematic application domains of the five LSPs, namely:

- Smart cars: Autopilot, developing IoT autonomous driving vehicles.
- Smart cities: SynchroniCity, developing a European IoT-enabled city market.
- Smart events: MONICA - Management of Networked IoT Wearables.
- Smart farming: IoF2020 - Internet of Food and Farm.
- Smart health: ACTIVAGE, developing an active & healthy ageing IoT based solutions.

We planned to develop 60 questions distributed as follow:

- 30 questions on generic GDPR topics
- 6 questions on smart cities
- 6 questions on smart farming
- 6 questions on smart cars
- 6 questions on smart events
- 6 questions on smart health

The objective was to distribute the questions in order to cover all the list of identified key topics and definitions.

The questions were formulated to be illustrative, with a simple context that the user can understand, and kept short. It has been decided to focus on the key principles and to avoid questions that relates to too complex cases.

3.8 MATRIX OF QUESTIONS PER DOMAIN

It was decided to have one section dedicated to the GDPR in general and then one section for each LSP. The initial plan was to have 30 general questions and 30 domain specific questions (5 times 6 questions). However, the effective number of questions was slightly adapted to address the specificities of each application domain. Here is the table of the questions:

In the following matrix, vertically it shows the key concepts communicate (definitions and principles) and horizontally the 6 sections of the game. In each field of the table, the quantity of the questions related to that concept and that section are written. Some questions cover more than one topic, so in some columns, adding up the values, the result is bigger than the actual number of questions of that section.

Topic	General Questions	Domain Specific Questions					Total
		Smart cars	Smart cities	Smart events	Smart Farming	Smart Health	
Definitions							
Personal data	5			1	2		8
Anonymisation vs pseudonymisation	2				1		3
Data controller vs data processors	5			2	3		10
Sensitive data	5					2	7
Genetic data	1					1	2
Biometric data	1					1	2
Data subject			1				1
Profiling		2	1				3
Principles							
Territorial scope	7						7
Purpose limitation			1	1			2
Data minimisation				2			2
Prior informed consent	1		1				2
Child's consent	1						1
Criminal convictions processing	4						4
Transparency		1					1
Right to access			1				1
Right to rectification		1					1
Right to erasure		1	1			1	3
Object to data processing			1			1	2
Restriction of processing						1	1
Consent withdraw	1	1					2
Data portability		1				1	2
Notification of personal data breach	1						1
Impact assessment		1				1	2
Total	34	8	7	6	6	9	70

Figure 4: Matrix of questions per domain

3.9 FIRST TEST AND VALIDATION AT THE IOT WEEK IN JUNE 2017

It was decided that it was an excellent opportunity to test the first version of the game at the IoT Week 2017 (Geneva, 6-9 June 2017).

The IoT Week is a “leading conference on IoT research and emerging technologies. It is organized under the umbrella of the IoT Forum to promote international dialogue and cooperation for IoT innovation, as well as to discuss technical, societal and market issues related to the IoT.”¹⁴

In this event, most participants are highly interested in privacy issues related to the IoT, among them lawyers and privacy experts. Also, U4IoT and the five LSPs participated in the event, so AS had the possibility to show the game to the key partners of the LSPs. U4IoT had a booth to show the current status of the project, managed by several partners, among them AS, and the first version of the privacy game was proposed to the public at the booth.

The playtest protocol was the following. The booth visitors were invited to play a quick game about privacy. The aims of the game in the framework of U4IoT were explained, then the rules were presented and the participants were divided into two teams (if a visitor was alone s/he tested the game alone). Each team was given a piece of paper and a pencil to write the answer and a limit in time or in number of questions was agreed. Then a question card was randomly chosen and read, and each team had 2 minutes to agree upon an answer. After each team answered, the answer was read and the points were assigned, then the following question card was sorted. Before leaving the play-testers were given the questionnaire to be answered and their answers were collected in anonymised form.

3.9.1 Sets of cards and team game

Two sets of cards were presented: one set with multiple questions in each card and one set with only one question per card. In the following lines it is going to be explained why two sets of cards were presented.

At the beginning it was decided to create cards with multiple questions, e.g. :

“Card 1 Which of the following are in general data controllers?”

- | | |
|--------------------|---|
| A) dentist | D) provider hosting encrypted personal data |
| B) payroll company | E) health insurance” |
| C) accountant | |

In such cards every line can be true or false, so the player can reason about the different possibilities, learning by comparing them. But after internal tests it was seen that this kind of cards has too much text to be read, and so it was decided to test cards with single questions, e.g.

¹⁴ (source: <http://iot-week.eu/>)

Card 1

"Is a dentist in general a data controller?"

Card 2

"Is a payroll company in general a data controller?"

Etc., so that the cards are lighter and can be read more quickly.

At the IoT Week both sets of cards were proposed, to test this characteristic also through the external public. When there were at least 2 people at the same time, it was proposed to them to play in 2 opponent teams. Playing with at least 2 opponent parties allows the participants to be challenged by a little competition and having teams of at least 2 people allows the players to discuss in each team about the questions; this makes the game more playful and stimulating.

3.9.2 The questionnaire for the play-testers¹⁵

After playing the game, a questionnaire was proposed to the play-testers (see Annex D).

The questions were chosen because we wanted to understand the level of acceptance among play-testers, analysing the averages of how many minutes each play-tester played and how many questions s/he tried to answer. We wanted to understand their degree of appreciation concerning the most liked and disliked things in the game, the clarity of the questions, the learning of new privacy concepts and the perceived usefulness of the game as a tool to raise privacy awareness. Moreover, we wanted to receive feedback and suggestions to improve the game through new ideas of the play-testers.

It was decided to ask open questions and closed questions, and among the open questions there were quantitative questions and evaluation questions.

The open quantitative questions required a numerical answer, like Q1-Q2, and their aim was to have a clear idea of how reliable the judgements of the play-testers were.

The closed evaluation questions (Q5 to Q8) offered 5 different appreciations, numerically converted in 1 to 5:

- | | |
|------------------|------------------|
| [1] not at all | [4] rather yes |
| [2] rather not | [5] very much |
| [3] more or less | [N] no opinion). |

We prepared these closed questions in order to have statistics on the opinions of the play-testers, having homogeneous answers and a common measure.

Finally, the open evaluation questions (Q3, Q4 and Q9) were probably the most important ones, because they allowed the play-testers to describe their opinions and to suggest new ideas to improve the game.

¹⁵ <https://en.wikipedia.org/wiki/Playtest>

3.9.3 Analysis of the answers

Because the participants were very busy with the intense programme of talks of the conference, we had the possibility to invite them only during the short pauses. We were able to engage only 27 participants that filled the questionnaire, so this small sample served only for a preliminary analysis. It was proposed to the first 6 participants to play with the set of multiple questions cards, then it was proposed to the following participants to play with the set of single question cards. Then it was decided to keep proposing this version because many of the first evaluations showed that the participants preferred shorter texts.

Here some analysis of the answers is provided, through the classical statistical parameters of average, standard deviation, median, mode, skewness and Kurtosis.

These parameters allow to synthesize the numerical results, checking at which degree these results are biased by outliers, sparse or asymmetric in the histogram.

Q1) How long did you play the game? (please insert 1 number: the estimated number of minutes)

The participants played approximately 5 ± 3 minutes (average \pm standard deviation), the median and the mode are also 5 minutes, so this average is not affected by outliers.

This average was the goal set before the test, because it was considered that 5 minutes are sufficient to evaluate the game idea.

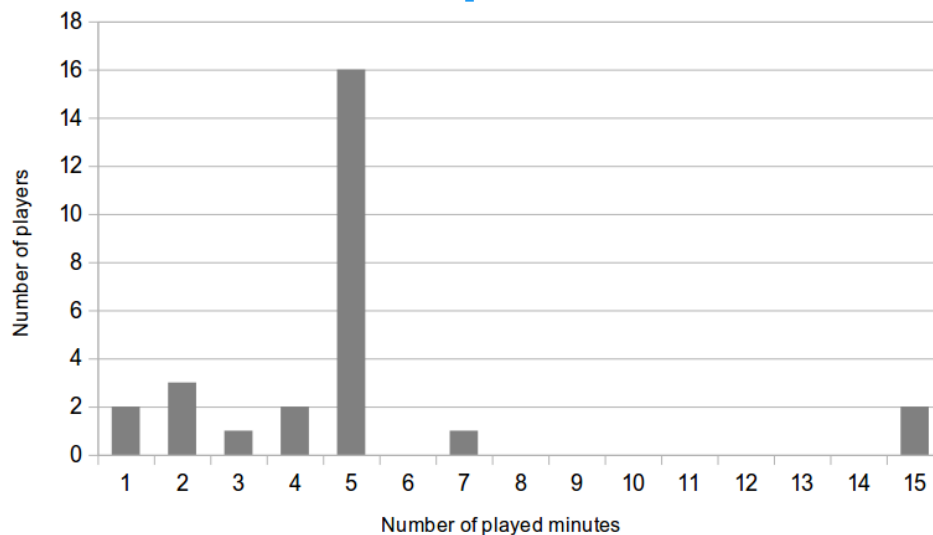


Figure 5: How long did you play the game?

Q2) How many cards did you play? (please insert only 1 number)

The participants answered approximately to 2 ± 1 cards (average \pm standard deviation). Because the first 6 participants tested the version with multiple questions, for them each card had several questions, so the number of answered questions does not correspond to the number of played cards. The participants answered approximately to 3.67 ± 3.52 questions (average \pm standard deviation), with a median of 3 and a mode of 2. The skewness of 2.66 shows an asymmetry on the right of the histogram, and a Kurtosis of 7.15 indicates heavy tails of the histogram. This is due to 2 participants that answered 15 questions, many more than the other participants. This average was the goal set before the test, because it was considered that 3-4 questions are sufficient to evaluate the game idea.

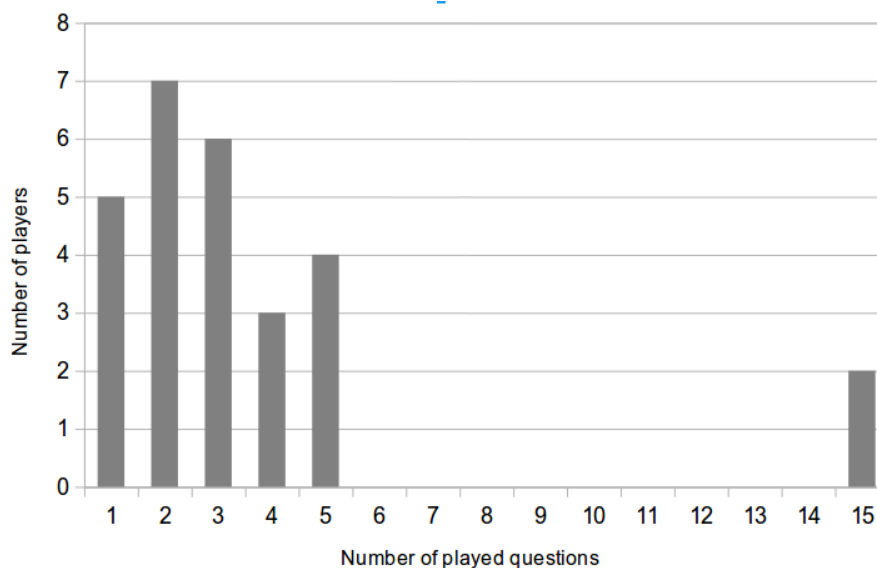


Figure 6: How many cards did you play?

Q3) What did you like in the game?

The most liked thing is that people can learn playing, so the participants can understand privacy concepts in a pleasant way (80% of the play-testers liked this point). Moreover, some people (15%) liked the precise use cases and that it is a simple game even when there is a difficult content.

Q4) What did you dislike in the game?

Among the disliked things there were: some unclear questions or answers (15% of the play-testers), some tricky questions (about 8%), some technical words (15%). For example, some questions considered tricky were related to specific numbers, like

“Question: Is it true that in the GDPR (General Data Protection Regulation) the consent from a minor in relation to online services will only be valid if authorised by a parent?

Answer: No. This norm applies not to minors but to children under 16 years old, though Member States can reduce this age to 13 years old.”

Here the question plays on the notion of minor that corresponds typically to the age of 18

years, so the sentence is almost entirely correct unless this detail.

Concerning the technical words, an example was the word “derogation” that was unknown to many play-testers.

Q5) Did you learn something new about privacy?

The average result was 3.69 ± 0.97 (average \pm standard deviation), approximated to 4, so “rather yes”. Median and mode are also 4, and it confirms that the result is robust. Some play-testers answered “not at all” or “rather not”, this is easily explainable considering that among the play-testers there were a few privacy experts, they liked the game but they knew already the answers because they work in this domain.

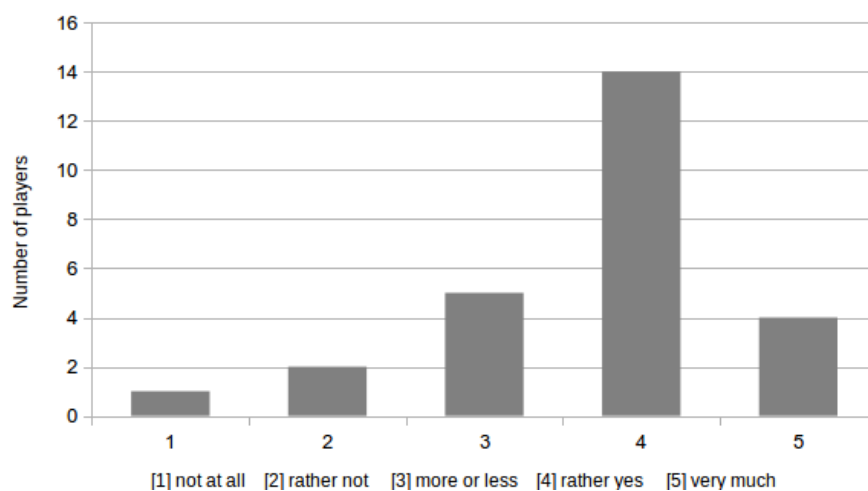


Figure 7: Did you learn something new about privacy?

Q6) Is the game useful for privacy awareness?

The average result was 4.42 ± 0.64 (average \pm standard deviation), approximated to 4, so “rather yes”. The median of 4.5 and the mode of 5 confirm this very positive result. The negative skewness of -0.67 indicates an asymmetry towards the left, this is due to the fact that the mode is also the maximum possible value.

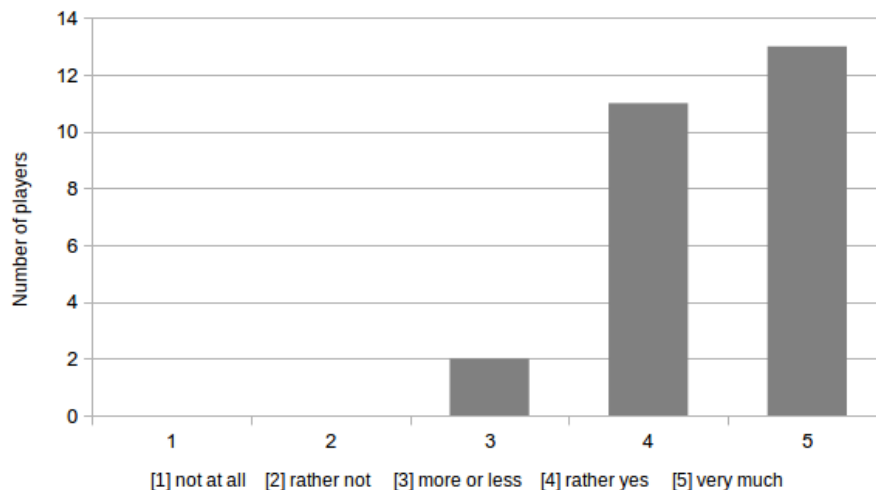


Figure 8: Is the game useful for privacy awareness?

Q7) Is the game easy to understand and to play?

The average result was 4.41 ± 0.80 (average \pm standard deviation), approximated to 4, so “rather yes”.

The result is even more positive considering that both median and mode are 5, so “very much”. The negative skewness of -0.90 indicates an asymmetry towards the left, this is due to the fact that the mode is also the maximum value.

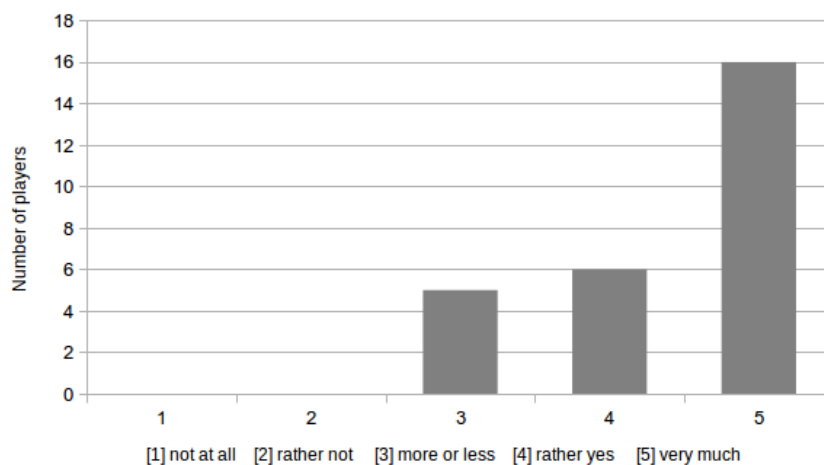


Figure 9: Is the game easy to understand and to play?

Q8) Are the questions clear and easy to understand?

The average result was 3.70 ± 0.82 (average \pm standard deviation), approximated to 4, so “rather yes”. This is the only case in which median and mode are 3, showing that the clarity was the most important point to improve. A Kurtosis of -1.20 shows significantly smaller tails compared to a Gaussian distribution, so the results are well grouped around the average.

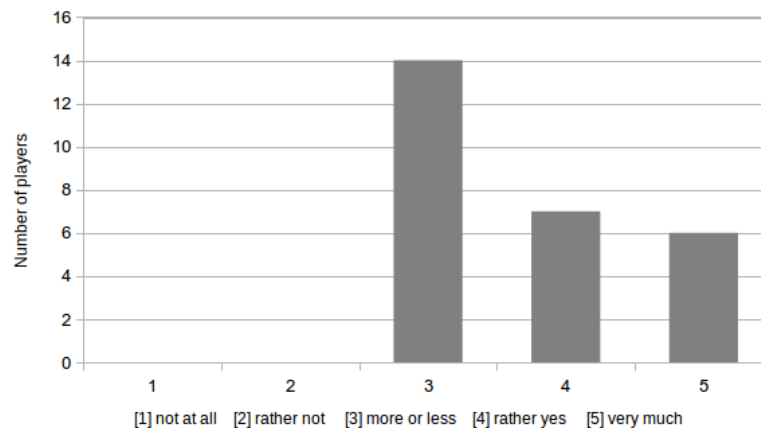


Figure 10: Are the questions clear and easy to understand?

Q9) Which are your suggestions and comments to improve the game?

Among the suggestions, there were: to add graphics and pictures, to create an online version, to have clearer questions and answers, to add general questions on privacy (not necessarily on GDPR and LSPs), to add real cases, to show the risks of not compliance.

3.9.4 General conclusions about the test and new version

Here a few specific feedbacks will be analysed.

1. The comments about the tricky questions were related to questions like the following one:

According to GDPR (General Data Protection Regulation), is it true that supervisory authorities will be able to issue fines to public institutions up to 2 million €?

and the answer is: no, up to 20 million €.

In fact, for these cases it is better a question with multiple answers so that the players can reason comparing them.

In the previous example, the new question was modified in the following way:

According to GDPR (General Data Protection Regulation), supervisory authorities will be able to issue fines to public institutions up to which amount of € ?

A) half million

B) 1 million

C) 2 millions

E) 20 millions

D) 10 millions

2. Regarding the suggestion to have clearer questions and answers, there were for example some questions about derogations of the GDPR, and many people did not know the word "derogation", so a synonym between parentheses was added: derogations (exceptions).
3. The addition of a graphic design and the online version were already planned.
4. Concerning the idea to add general questions on privacy (not necessarily on GDPR for the LSPs) from everyday life, Google, Facebook, etc, AS already thought about it. Even if AS agrees that this part would make the game more attractive and closer to the public, these comments will probably have to be disregarded, because such a part is not foreseen in the approved proposal of U4IoT. The approved proposal aims specifically at a game for privacy and personal data protection in LSPs.

As general conclusions, the game had a very positive feedbacks and the play-testers liked the idea to create a game that allows to learn about a complex theme like privacy and data protection. A new version of the game was created, taking into account these results. Moreover, in the new version the contextualisation of the questions was improved, creating for each question a very specific and concrete situation to be analysed.

3.10 SECOND TEST AT LSP MEETING IN OCTOBER 2017

From the new version of the game a selection of 15 questions was extrapolated in order to present it at the LSP meeting in Brussels 25-27 October 2017.

The selection was composed by 10 questions of the general section and 1 question per LSP. In Brussels the opportunities to privately interact with potential play-testers were rarer than in Geneva, and only 5 people tested the new game, so we will not provide statistics but just general results.

At the same time, it was an excellent opportunity to present the concept at the Activity Group on Privacy and Security, in front of about 20 people. The game raised much interest and the comments will be included in the following analysis.

3.10.1 The improved questionnaire

The questionnaire was discussed with the rest of the U4IoT partners and it was slightly improved concerning the language and adding the distinction between the clarity of the questions and the clarity of the answers (Q8 and Q9). See annex E.

3.10.2 Analysis of the answers

The 5 play-testers played averagely 4-5 minutes, testing 2-3 questions each.

The average answer to question 5 (Did you learn something new about privacy?) was 3.9 (rather yes).

The average answer to question 6 (Do you think that the game is useful to raise awareness about privacy?) was 4.7 (very much).

The average answer to question 7 (Is the game easy to understand and to play?) was 4.6 (very much).

The average answer to question 8 (Are the questions clear and easy to understand?) and 9 (Are the answers clear and easy to understand?) was in both cases 4.4 (rather yes).

Therefore, the quantitative questions had very good results.

In question 3 (Name something you especially liked in the game) people liked the closeness to reality, the challenge of multiple answers, the research behind the game, the questions tailored on real cases and the practical approach.

In question 4 (Name something you especially disliked in the game) one tester answered "nothing" (he liked everything), others said that it is a too simple game, maybe monotone, and that some questions are too wordy.

In question 10 (Which are your suggestions and comments to improve the game?) people suggested to add a board with a path, to have shorter texts and to add points depending on the answering time.

Several people (also in the activity group on privacy) suggested to introduce FAQ about privacy like privacy issues in everyday life, more general and less technical questions, based not only on GDPR but on general basic concepts of privacy, and to ask when data are really necessary, because often data controllers want to keep data for which the related privacy risks are higher than the potential commercial use. Finally, a very good suggestion was to use the game as introduction in workshops about privacy.

3.11 ASSESSMENT AND VALIDATION OF THE QUESTIONS

The game is assessed and validated according to three dimensions:

- a. The accuracy of questions and answers: all the texts were reviewed in 2018 through 5 rounds of comments and improvements. The comments were provided by 5 lawyers (2 of AS, 2 of MI (Mandat International) and 1 of IIP (Istituto Italiano per la Privacy). Thanks to this process some references were added, several questions were made clearer and other questions were replaced.
- b. The user experience: the satisfaction of the play-testers was described in the previous paragraphs. Apart from the official tests, several informal tests were performed and over 20 complete games were played, with comments similar to those already received.
- c. Achievement of the objectives: this dimension will be able to be assessed during the dissemination phase, in the second half of the project.

3.12 RULES OF THE GAME “PRIVACY QUIZ”

Number of players: 2 or more (at least 2 teams of 1 or more players).

Age: over 13.

Duration: 5 to 60 minutes.

Introduction: This game was conceived as a serious game with the aim to raise awareness about privacy and data protection in the framework of the new EU law GDPR (General Data Protection Regulation).

Objective of the players: earning points guessing phrases and answering questions about privacy and data protection. The team with most points wins the game.

Preparing the game:

Each team can have 1 or more players and we recommend between 2 and 4 players. There can be 2 or more teams (ideally 2). At the beginning of the game, players can decide a time limit (ideally 10 to 60 minutes) or a number of question cards to play through (randomly chosen out of the 60 question cards).

Running the game:

In each turn there are 2 phases: phrase guessing and question. Each phase is timed on a separate timer (phrase timer and question timer). A player of Team 1 becomes the speaker, picks a card randomly and has max. 2 minutes in the phrase timer to give his/her teammates hints to guess the phrase (1 to 3 words) put in evidence in the card. The speaker can say neither the words to be guessed, nor any word with the same root (e.g. for “television” the speaker cannot say “telescope”), unless the team has already said that word. If Team 1 guesses, the phrase timer is stopped. If Team 1 does not guess after 2 minutes, or if it decides to skip the phrase stopping the phrase timer (not before 1 minute of trials), then Team 2 has 1 trial to guess, if Team 2 does not guess then Team 3 has 1 trial to guess, and so on. If a team guesses it receives 1 point. Then the speaker reads the question aloud. Each team has 2 minutes (timed in the question timer) to discuss and write down its answer. The official answer is read out by the speaker and discussed. Each team gets 2 points for a right answer, -1 point for a wrong answer, and 0 points if it decides not to answer. Then the next speaker of Team 1 picks a new card, reactivates the phrase timer and continues as previously explained. When the 2 minutes of the phrase timer are over, a player of Team 2 becomes the new speaker. Then the game continues in this way until the end.

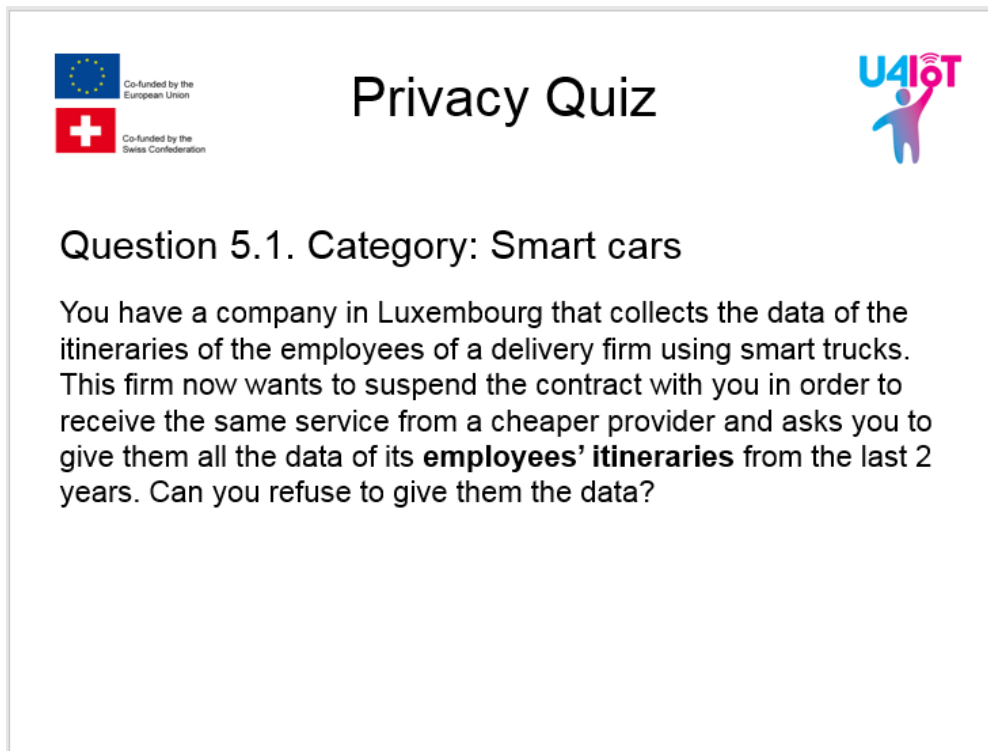


Figure 11: Example of card front with a question

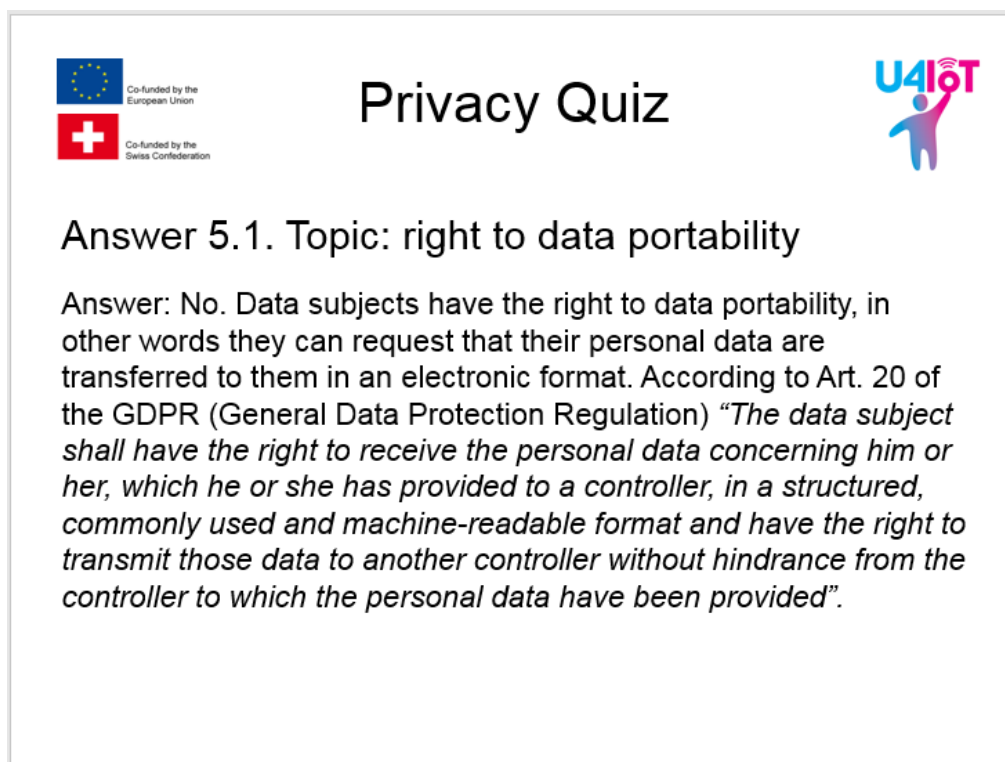


Figure 12: Example of card back with answer and explanation

3.13 EXPANSION OF THE GAME

The Privacy Quiz is more addressed to the LSP stakeholders than to LSP end-users and to the large public. In fact, it is a game conceived to give more importance to the content than to the game elements and it is tailored to be playable also in a few minutes. In order to address in a more substantial way also the LSP end-users and the large public, in 2018 an expansion of the questions game is being developed. The aim of this expansion is to have a more playful game, with a lower density of legal content, in which other game elements are present.

For this aim a collaboration was started with prof. David King (Univ. Arts London, Department of Game Design). A card game (named "Privacy Cards") is being developed where the cards represent data and the players move their markers on a grid of cards representing the internet. Navigating the internet, users leave personal data about themselves or about other users, and many companies try to collect these data to profile the users, and elaborate statistics on them. In this game some players will play as a user trying to erase his/her online accessible data, and some will play as a company trying to collect some categories of data through the internet. At each turn the players will have to answer one question from the question cards of the basic game, earning points through which they will be able to get the data cards.

3.14 TESTS AND DISSEMINATION IN THE FIRST SEMESTER OF 2018

In the first semester of 2018, AS participated in 4 more events:

- 1) Ludesco game Festival (La Chaux-de-Fonds, Switzerland, 16-18/3/2018)
- 2) Créateurs de Jeux 2018 (game creators gathering, Swiss Museum of Games, La Tour-de-Peilz, 5-6/5/2018)
- 3) U4IoT Co-Creation Workshop for Smart Cities (Carouge, Switzerland, 22-25/5/2018)
- 4) IoT Week 2018 (Bilbao, Spain, 4-8/6/2018).

Ludesco is one of the biggest Swiss game festivals and receives thousands of game lovers from Switzerland and other countries. In the last years, they have dedicated a special attention both to serious games and to game inventors, they organised a space dedicated to show and play prototypes and serious games in different domains. In this space, AS showed and tested the Privacy Quiz with a public that has only a general knowledge about privacy and IoT. Over thirty persons tested the game, showing interest in the domain. This test allowed to refine and improve the mechanism of word guessing (see the paragraph 2.14 with the rules).

Créateurs de Jeux is the Swiss gathering of game inventors, organized by the Swiss Museum of Games and by the Swiss game company GameWorks. In this event, every year participate amateur and professional game creators, and it was indeed a great opportunity to receive feedback by these experts. In this context, a first version of Privacy Cards was tested. Many positive comments and useful insights were collected to continue the development. In particular, the most interesting suggestion received from several people was to differentiate the goals of users and companies, in order to have a clearer distinction of these roles for the

players.

The **U4IoT Co-Creation Workshop for Smart Cities** was organised in Carouge, near Geneva, by U4IoT in collaboration with the City of Carouge, Mandat international, the University of Geneva (MAS on IoT), and SynchroniCity. The workshop was tailored for: smart city employees and project managers; master students in IoT and/or smart cities; LSP project Partners; citizens from Carouge; representatives of local associations. The main objective of the event was to provide the participants with tools to create services together with citizens, in this case, the inhabitants of the City of Carouge. In this scenario, AS presented a workshop about gamification and serious games and in the final part the Privacy Quiz was played by the participants. During the game the participants were very engaged discussing about the privacy issues in the scenarios proposed by the questions. The whole workshop, and particularly the part on gamification, were well received by participants.

The **IoT Week 2018** is a “leading conference on IoT research and emerging technologies”. It is organized under the umbrella of the IoT Forum to promote international dialogue and cooperation for IoT innovation, as well as to discuss technical, societal and market issues related to the IoT.”¹⁶ At the IoT Week 2018, AS managed with other U4IoT partners a booth on Privacy and Security. Moreover, AS participated in the organisation and presentation of the workshop “*End-user engagement tools and methods for IoT projects*”. In the booth and the workshop, the Privacy Quiz and the Privacy Cards games were presented, receiving great interest and requests to organise workshops with the Privacy Game (e.g. by Autopilot and Synchronicity).

16 (source: <http://iot-week.eu/>)

3.15 ONLINE GAME

In collaboration with DunavNet, an online version of the Privacy Quiz is being prepared, accessible on the U4IoT website. The user will be able to select one or more question categories, then the player will see a question randomly chosen among those of the selected categories, and after providing an answer the official answer and the explanation will be displayed. For each correct answer the user will earn points, and when the player finishes to play s/he will be able to enter a pseudonym and to save his/her score in the website ranking. Here we show some screenshots of the first provisional version (not yet online).

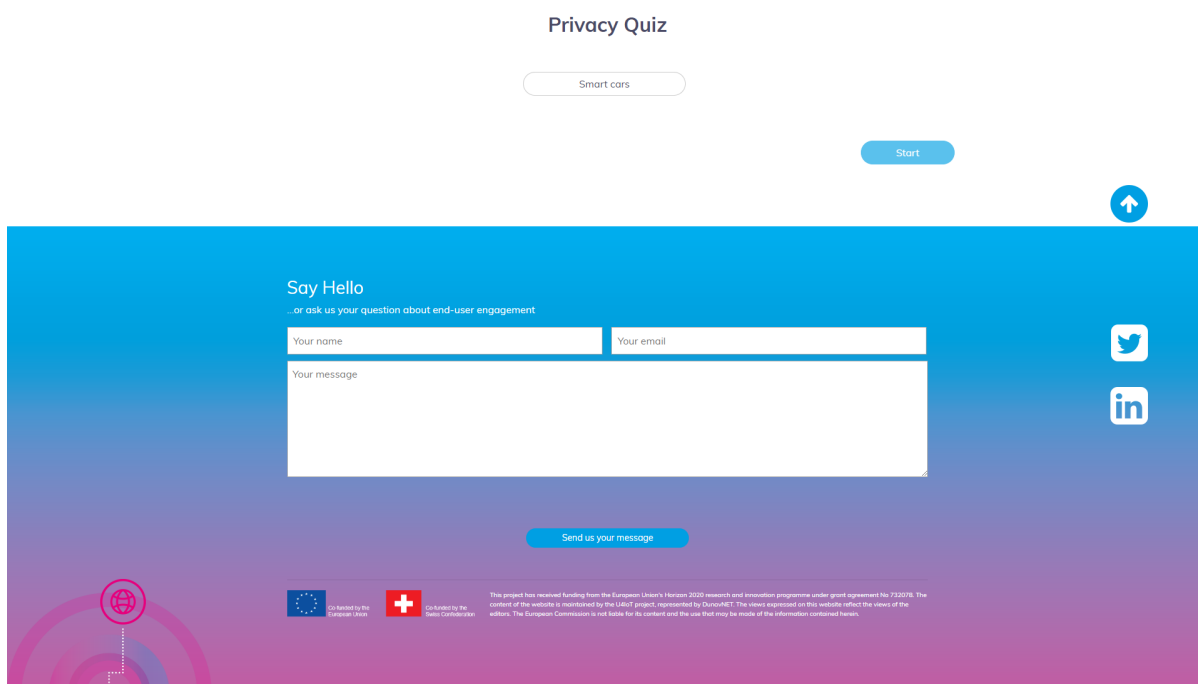
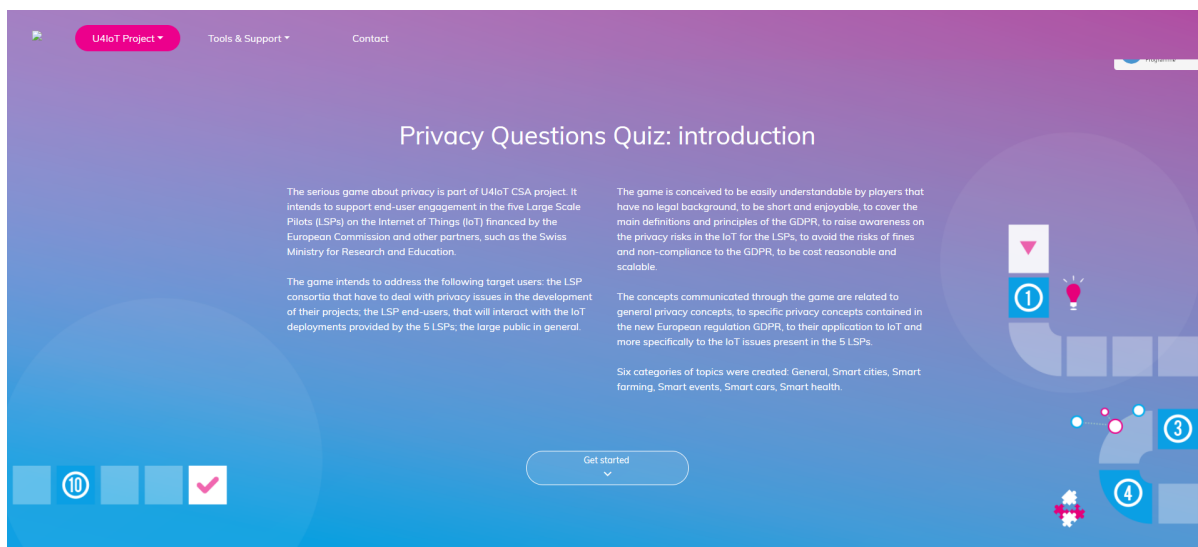
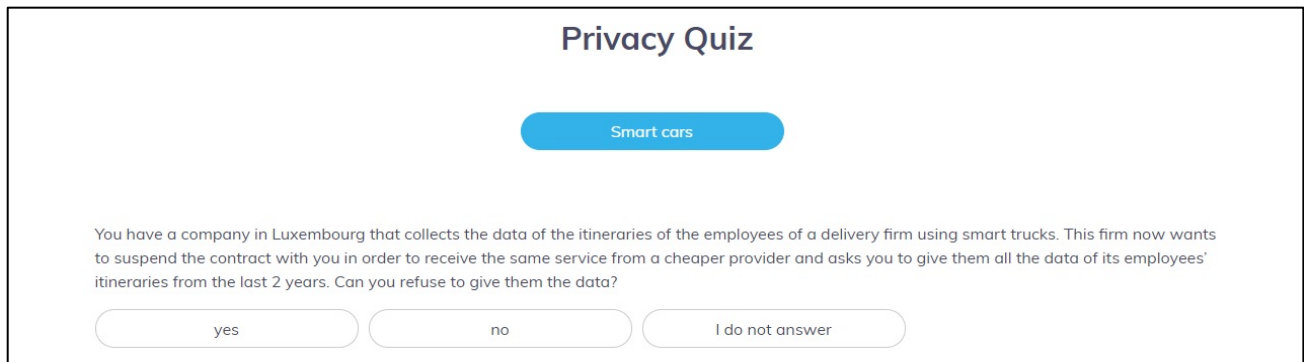


Figure 13: Provisional entry page of the Privacy Quiz



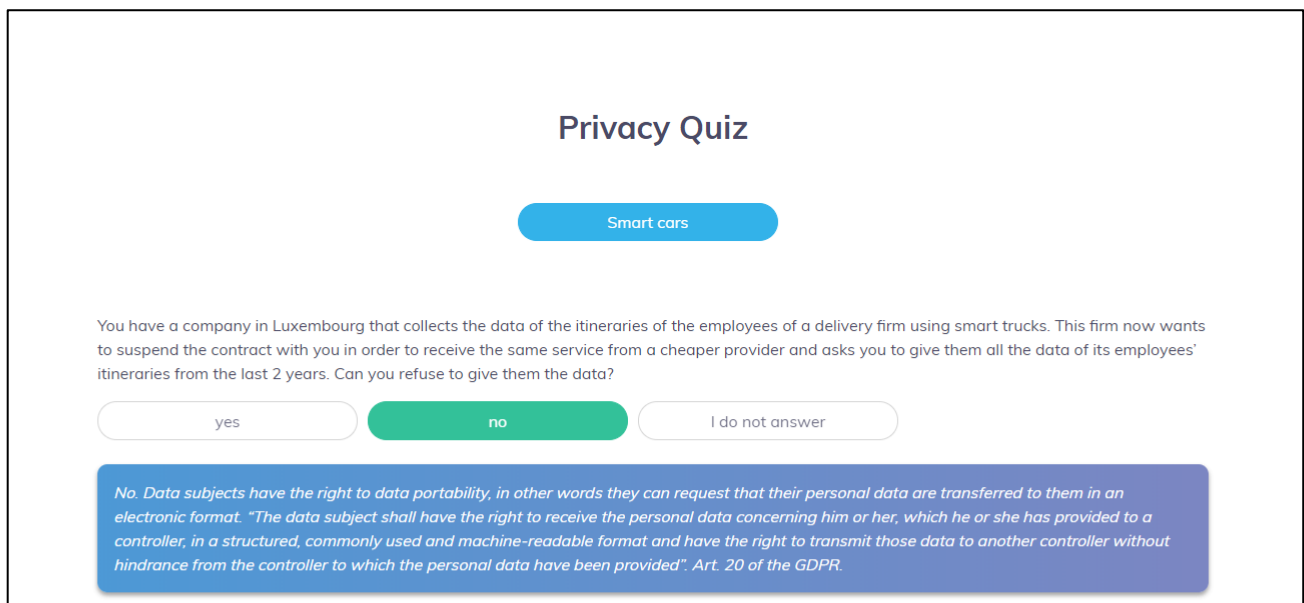
Privacy Quiz

Smart cars

You have a company in Luxembourg that collects the data of the itineraries of the employees of a delivery firm using smart trucks. This firm now wants to suspend the contract with you in order to receive the same service from a cheaper provider and asks you to give them all the data of its employees' itineraries from the last 2 years. Can you refuse to give them the data?

yes no I do not answer

Figure 14: Question in the online game



Privacy Quiz

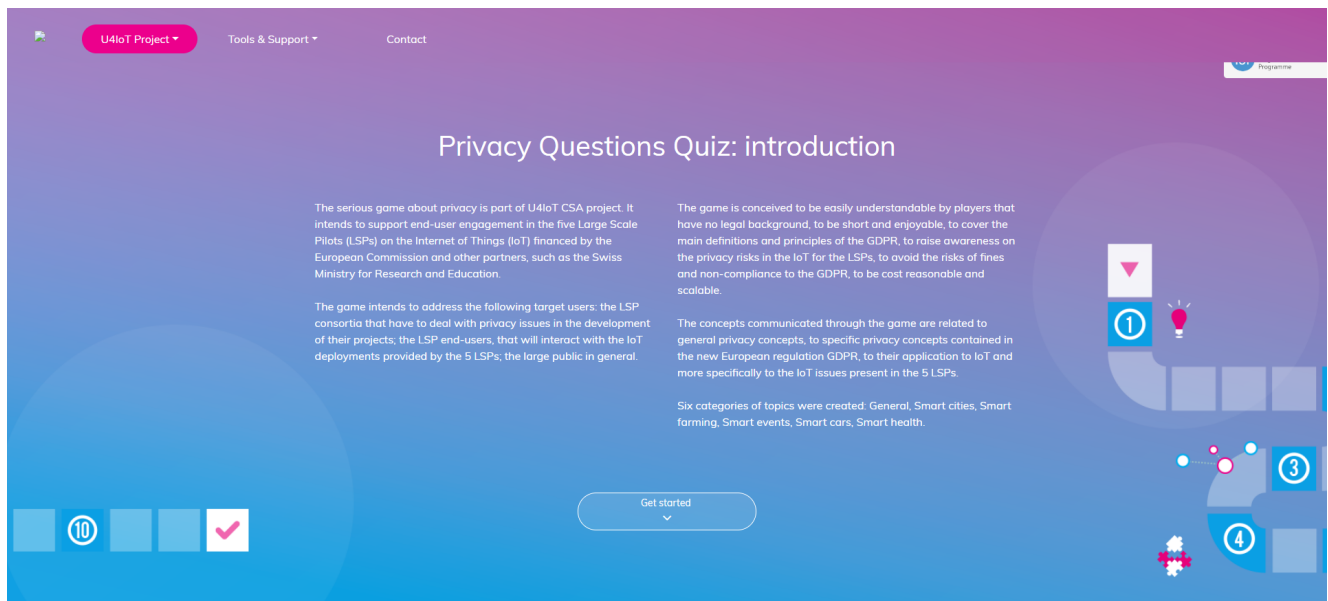
Smart cars

You have a company in Luxembourg that collects the data of the itineraries of the employees of a delivery firm using smart trucks. This firm now wants to suspend the contract with you in order to receive the same service from a cheaper provider and asks you to give them all the data of its employees' itineraries from the last 2 years. Can you refuse to give them the data?

yes **no** I do not answer

No. Data subjects have the right to data portability, in other words they can request that their personal data are transferred to them in an electronic format. "The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided". Art. 20 of the GDPR.

Figure 15: Question with its answer and explanation in the online game



Privacy Quiz

You have scored 90 points.

You can sign in with your user name if you wish to save your result.

Your user name can only be used once.

User name

Submit

Try again

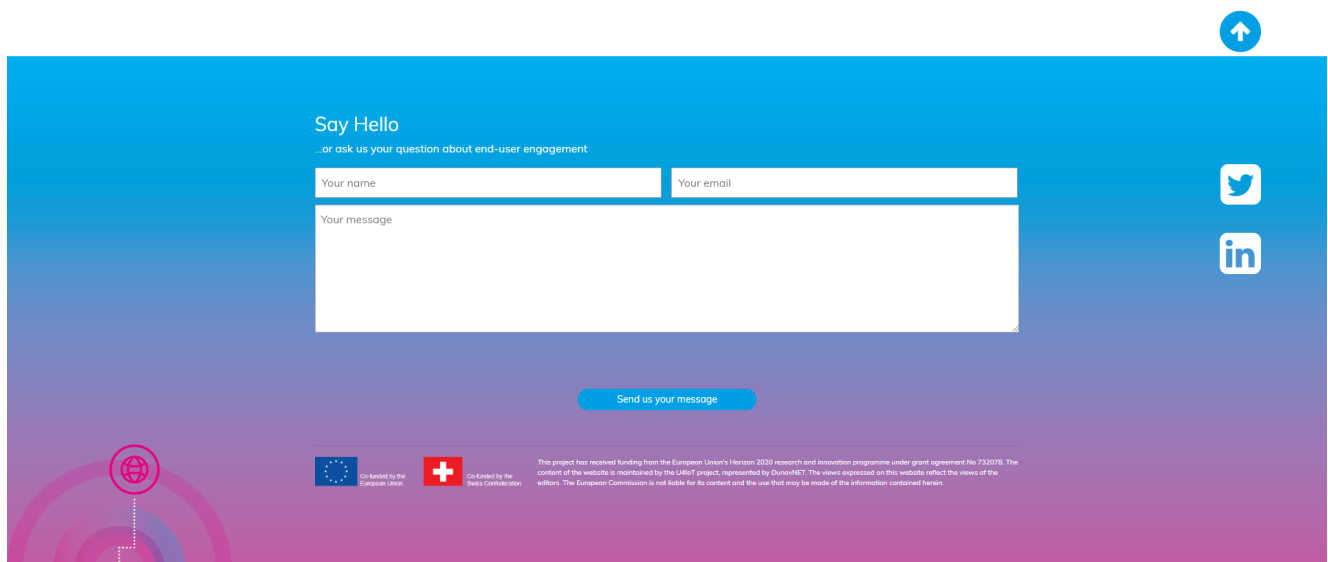


Figure 16: Provisional page of the endgame in the online game

3.16 CONCLUSION ON THE SERIOUS GAME

The privacy game was conceived as a serious game aimed at raising awareness about the main concepts of privacy, and particularly of the GDPR, in the domain of the IoT and specifically for the 5 LSPs.

In the initial part of the project, AS analysed the whole text of the GDPR and the LSP requirements, in order to understand which topics were the most important to communicate and how to adapt them in useful IoT scenarios. The main goals were set: to help the LSPs and their stakeholders to show the key principles of data protection, to raise awareness on the main risks related to data protection with IoT deployments, to create a useful tool for the LSPs, to translate complex legal norms into clear and easily understandable operational principles and to reduce the risks of non-compliance with the GDPR in the five LSPs.

The target users were defined: primarily the members of the LSP consortia, secondarily the LSP end-users and finally the large public. The requirements of the serious game were set: be easily understandable, encompass the main definitions, principles and obligations of the GDPR, cover specific risks of the LSPs, be educative, effective, cost-efficient, enjoyable, scalable and easily accessible.

A clear methodology and a planning were defined: The Requirements Analysis (M1-M6); Game Development (M4-M18), with several iteration cycles (game design, end-user tests and validation, test results analysis, adaptations and improvements); Privacy Game dissemination (M19-M36). The key definitions and principles of the GDPR were selected as main concepts to be communicated through the game.

After that, an analysis of the existing serious games was done in order to brainstorm ideas on how to create the privacy game. Three options were analysed: board game, card game and quiz. The last one was chosen, as it is the most suitable considering the game requirements.

The questions were then prepared with the support of the legal team of AS and MI that checked the precision of the legal aspects. The first external test was performed at the IoT Week 2017 in June 2017 in Geneva, after which the game was reviewed and improved. The second test was in the LSP meeting in Brussels in October 2017, followed by a second round of adaptation and improvement. The main conclusions extracted from these tests were that the texts had to be simplified and shortened, some technical words had to be explained or substituted and images should be added (as already foreseen).

In 2018, in collaboration with Univ. of London, an expansion of the quiz is being developed as a card game in which the cards represent data and users. To protect their data the users must earn points answering the questions of the Privacy Quiz.

The game was presented again in Ludesco game Festival (La Chaux-de-Fonds, Switzerland, 16-18/3/2018), in the Créateurs de Jeux 2018 (game creators gathering, Swiss Museum of Games, La Tour-de-Peilz, 5-6/5/2018), in the U4IoT Co-Creation Workshop for Smart Cities (Carouge, Switzerland, 22-25/5/2018) and in the IoT Week 2018 (Bilbao, Spain, 4-8/6/2018).

An online version of the Privacy Quiz is being developed in collaboration with DunavNet, made accessible on the U4IoT website.

The game was successfully tailored for its target users, namely LSPs and their stakeholders, end users and the general public, focussing on key concepts for communication, such as key privacy definitions and principles, covering all main concepts of the GDPR. It was tested and improved and a final test will be performed by LTU in the summer of 2018, in order to have an external judgement by another partner of the project; The game will then be finalised and the final questions will be uploaded in the online game, before disseminating it through seminars, workshops and game festivals.

REFERENCES

- [1] Ahmed, A. M., Mehid, Q. H., Moreton, R., & Elmaghra by, A. (2015). Serious games providing opportunities to empower citizen engagement and participation in e-government services. Paper presented at the 2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games, Louisville, USA. DOI: 10.1109/CGames.2015.7272971
- [2] de-Marcos, L., Domínguez, A., Saenz-de-Navarrete, J., & Pagés, C. (2015). An empirical study comparing gamification and social networking on e-learning. *Computers & Education*, 75, 82-91. DOI: 10.1016/j.compedu.2014.01.012
- [3] Djaouti, Damien; Alvarez, Julian; Jessel, Jean-Pierre. "Classifying Serious Games: the G/P/S model". (2015)
- [4] Dobrescu, L., Greiner, B., & Motta, A. (2015). Learning economics concepts through game-play: An experiment. *International Journal of Educational Research*, 69, 23-37. DOI: 10.1016/j.ijer.2014.08.005
- [5] Dubbels, B. (2013). Gamification, serious games, ludic simulation and other contentious categories. *International Journal of Gaming and Computer-Mediated Simulations*, 5(2), 1-19. DOI:10.4018/jgcms.2013040101
- [6] Gotterbarn, D. (2013). Serious games: Learning why professionalism matters can be fun. *ACM Inroads*, 4(2). DOI: 10.1145/2465085.2465091
- [7] Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game based learning. *Computers in Human Behavior*, 54, 170-179. DOI: 10.1016/j.chb.2015.07.045
- [8] Ismailović, D., Köhler, B., Haladjian, J., Pagano, D., & Brügge, B. (2012). Towards a conceptual model for adaptivity in serious games. Paper presented at the IADIS International Conferences on Interfaces and Human Computer Interaction 2012 and Game Entertainment Technologies 2012, Lisbon, Portugal. URL: <http://www.iadisportal.org/ihci-2012-proceedings>
- [9] Kapralos, B., Fisher, S., Clarkson, J., & van Oostveen, R. (2015). A course on serious game design and development using an online problem-based learning approach. *Interactive Technology and Smart Education*, 12(2), 116-136. DOI: 10.1108/ITSE-10-2014-0033
- [10] Lewis, M. A., & Maylor, H. R. (2007). Game playing and operation management education. *International Journal of Production Economics*, 105(1), 134-149. DOI: 10.1016/j.ijpe.2006.02.009
- [11] Muñoz, K., McKevitt, P., Lunney, T., Noguez, J., & Neri, L. (2011). An emotional student model for game-play adaptation. *Entertainment Computing*, 2(2), 133-141. DOI: 10.1016/j.entcom.2010.12.006



- [12] Pereira, G., Brisson, A., Prada, R., Paiva, A., Bellotti, F., Kravcik, M., & Klamma, R. (2012). Serious games for personal and social learning & ethics: Status and trends. *Procedia Computer Science*, 15, 53-65. DOI: 10.1016/j.procs.2012.10.058
- [13] Seager, W., Ruskov, M., Sasse, A. M., & Oliveira, M. (2011). Eliciting and modelling expertise for serious games in project management. *Entertainment Computing*, 2(2), 75-80. DOI: 10.1016/j.entcom.2011.01.002
- [14] Soflano, M., Connolly, T., & Hainey, T. (2015). An application of adaptive games-based learning based on learning style to teach SQL. *Computers & Education*, 86, 192-211. DOI: 10.1016/j.compedu.2015.03.015
- [15] Susi, T., Johannesson, M. & Backlund, P. (2007). Serious games – An overview. Sweden: University of Skode. Technical Report HS-IKI-TR-07-001.
- [16] ter Vrugte, J., de Jong, T., Vandercruysse, S., Wouters, P., van Oostendorp, H., & Elen, J. (2015). How competition and heterogeneous collaboration interact in prevocational game-based mathematics education. *Computers & Education*, 89, 42-52. DOI: 10.1016/j.compedu.2015.08.010
- [17] Tobias, S., & Fletcher, D. J. (2012). Reflections on 'A Review of Trends in Serious Gaming'. *Review of Educational Research*, 82(2), 233-237. DOI: 10.3102/0034654312450190
- [18] Truong, H. M. (2016). Integrating learning styles and adaptive e-learning system: Current developments, problems and opportunities. *Computers in Human Behavior*, 55, 1185-1193. DOI: 10.1016/j.chb.2015.02.014
- [19] van de Sandre, E., Segers, E., & Verhoeven, L. (2015). The role of executive control in young children's serious gaming behavior. *Computers & Education*, 82, 432-441. DOI: 10.1016/j.compedu.2014.12.004
- [20] van der Zee, D.-J., Holkenborg, B., & Robinson, S. (2012). Conceptual modeling for simulation-based serious gaming. *Decision Support Systems*, 54(1), 33-45. DOI: 10.1016/j.dss.2012.03.006
- [21] Wang, A. I. (2015). The wear out effect of a game-based student response system. *Computers & Education*, 82, 217-227. DOI: 10.1016/j.compedu.2014.11.004

ANNEX A – ORGANIZATIONAL AND SECURITY MEASURES

1. Measures for operations concerning the management of access, accounts, and the network
 - authentication requirements to the systems for accessing data and the assignment of remote access to such data by third parties such as consultants and suppliers are formally defined;
 - the identification codes (user-id) for access to applications and the network are both individual and unique;
 - the proper management of passwords is defined by guidelines communicated to all users for the selection and use of the keyword;
 - the setting of criteria and procedures for creating passwords for network access, access to the software applications, to corporate information, assets and critical or sensitive systems (e.g. minimum password length, complexity rules, validity);
 - accesses made by the users, in any mode, to data, to systems and to the network are subject to periodic audits;
 - applications keep track of changes made to the data by users;
 - setting of the criteria and procedures for the granting, modification and deletion of user profiles with systems are defined;
 - a matrix of authorization - applications/profiles/applicants - aligned with the organizational roles is prepared;
 - periodic checks are carried out on user profiles in order to verify that they are consistent with the assigned responsibilities;
 - documents relating to each individual activity are archived or stored in order to ensure complete traceability of the same.
2. Measures for operations concerning the management of access, accounts and profiles.
 - the responsibility for the management of networks is defined;
 - security controls are implemented to ensure confidentiality of the data inside the network and in transit over public networks;
 - tracking mechanisms of security events on networks are implemented (e.g. unusual frequency of access, mode, temporality);
 - the implementation and maintenance of computer networks through the definition of responsibilities and operating procedures, periodic checks on the operation of networks and the identified deficiencies is regulated;

- the criteria and procedures for activities that provide back up for each telecommunication network, the frequency of the activity, the modality, the number of copies, and the period of data retention is established;
 - documents relating to each individual activity is archived or stored in order to ensure complete traceability of the same.
3. Measures for operations concerning the management of hardware systems, which also includes the management of the back-up and continuity of information systems and other processes that are deemed critical.
- the process is formalized in an operating procedure or internal policy;
 - the setting of the criteria and procedures for the management of hardware systems that provide for the compilation and maintenance of an updated inventory of the hardware in use and that regulate the responsibilities and operating procedures in the event of implementation and/or maintenance of the hardware is defined;
 - the setting of the criteria and procedures for activities that provide back up for each hardware application, the frequency of the methods, the number of copies and the period of data retention is defined;
 - documents relating to each individual activity are archived or stored in order to ensure complete traceability of the same.
4. Measures for operations concerning the management of physical access to the sites in which IT infrastructure is located:
- the security measures, the procedures for surveillance, the frequency, the responsibility, the process of reporting violations/burglary of local technical or safety measures, and the countermeasures to be activated are defined; login credentials to the sites in which information systems and IT infrastructure is located is defined;
5. documentation of each transaction is stored in order to ensure complete traceability of the same. Organizational measures.
- Data controllers designate, in written, data processors¹⁷ selected among entities that can appropriately ensure, on account of their experience, capabilities and reliability, thorough compliance with the provisions in force applying to processing as also related to security matters;
 - Consortia, cities and/or data controllers supervise over thorough compliance with their instructions also by means of regular controls;

¹⁷ 'data processor' shall mean any natural or legal person, public administration, body, association or other agency that processes personal data on the controller's behalf

- Processing operations are only performed by persons in charge of the processing¹⁸ that act under the direct authority of either the data controllers or their data processor by complying with the instructions received;
 - The aforementioned persons are nominated in writing by specifically referring to the scope of the processing operations that are permitted. This requirement shall be also fulfilled if a natural person is entrusted with the task of directing a department, on a documentary basis, whereby the scope of the processing operations that may be performed by the staff working in said department has been specified in writing;
 - Personal data undergoing processing are kept and controlled, also in consideration of technological innovations, of their nature and the specific features of the processing, in such a way as to minimize, by means of suitable preventative security measures, the risk of their destruction or loss, whether by accident or not, of unauthorized access to the data or of processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected;
 - Data controllers take suitable technical and organizational measures that are adequate in the light of the existing risk, in order to safeguard security of its services and integrity of traffic data, location data and electronic communications against any form of unauthorized utilization or access;
 - In case of a particular risk of a breach of network security, data controllers inform subscribers and, if possible, users concerning said risk, as well as the local DPA or other competent Authorities;
6. Processing of personal data by electronic means is allowed in accordance with the arrangements listed here below.
- Persons in charge of the processing are provided with authentication credentials such as to successfully complete an authentication procedure relating either to a specific processing operation or to a set of processing operations
 - Authentication credentials consist in an ID code for the person in charge of the processing as associated with a secret password that shall only be known to the latter person; alternatively, they shall consist in an authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password, or else in a biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.
 - One or more authentication credentials are assigned to or associated with each person in charge of the processing.
 - The instructions provided to the persons in charge of the processing lay down the obligation to take such precautions as may be necessary to ensure that the confidential component(s) in the credentials are kept secret and that the devices

¹⁸ 'persons in charge of the processing' shall mean the natural persons that have been authorized by the data controller or processor to carry out processing operations

used and held exclusively by exclusively by persons in charge of the processing are kept with due care;

- Where provided for by the relevant authentication system, a password shall consist of at least eight characters; if this is not allowed by the electronic equipment, a password shall consist of the maximum permitted number of characters. It shall not contain any item that can be easily related to the person in charge of the processing and shall be modified by the latter when it is first used as well as at least every six months thereafter. If sensitive or judicial data are processed, the password shall be modified at least every three months.
- An ID code, if used, may not be assigned to another person in charge of the processing even at a different time.
- Authentication credentials are de-activated if they have not been used for at least six months, except for those that have been authorized exclusively for technical management purposes.
- Authentication credentials are also de-activated if the person in charge of the processing is disqualified from accessing personal data.
- The persons in charge of the processing are instructed to the effect that electronic equipment should not be left unattended and made accessible during processing sessions.
- Where data and electronic equipment may only be accessed by using the confidential component(s) of the authentication credential, appropriate instructions are given in advance, in writing, to clearly specify the mechanisms by which the data controller can ensure that data or electronic equipment are available in case the person in charge of the processing is either absent or unavailable for a long time and it is indispensable to carry out certain activities without further delay exclusively for purposes related to system operability and security. In this case, copies of the credentials are kept in such a way as to ensure their confidentiality by specifying, in writing, the entities in charge of keeping such credentials. Said entities have to inform the person in charge of the processing, without delay, as to the activities carried out;
- Where authorization profiles with different scope have been set out for the persons in charge of the processing, an authorization system is used.
- Authorization profiles for each person or homogeneous set of persons in charge of the processing is set out and configured prior to start of the processing in such a way as to only enable access to the data that are necessary to perform processing operations.
- It is regularly verified, at least at yearly intervals, that the prerequisites for retaining the relevant authorization profiles still apply.
- Within the framework of the regular update — to be performed at least at yearly intervals — of the specifications concerning the scope of the processing operations that are entrusted to the individual persons in charge of the processing as well as

to the technicians responsible for management and/or maintenance of electronic equipment, the list of the persons in charge of the processing may also be drawn up by homogeneous categories of task and corresponding authorization profile.

- Personal data are protected against the risk of intrusion and the effects of programs by implementing suitable electronic means to be updated at least every six months.
- The regular update of computer programs as aimed at preventing vulnerability and removing flaws of electronic means is carried out at least annually. If sensitive or judicial data are processed, such update is carried out at least every six months.
- Organizational and technical instructions are issued such as to require at least weekly data back-ups.
- Sensitive or judicial data are protected against unauthorized access by implementing suitable electronic means.
- Organizational and technical instructions are issued with regard to keeping and using the removable media on which the data are stored in order to prevent unauthorized access and processing.
- The removable media containing sensitive or judicial data are destroyed or made unusable if they are not used; alternatively, they may be re-used by other persons in charge of the processing, who are not authorized to process the same data, if the information previously contained in them is not intelligible and cannot be re-constructed by any technical means.
- If either the data or electronic means have been damaged, suitable measures are adopted to ensure that data access is restored within a specific deadline, which must be compatible with data subjects' rights and not in excess of seven days.

ANNEX B – RECOMMENDATIONS FOR DIFFERENT STAKEHOLDERS IN THE IOT DOMAIN

[from Article 29 Working Party, [Opinion](#) 8/2014¹⁹ on the on Recent Developments on the IoT]

1. Recommendations common to all stakeholders

- Privacy Impact Assessments (PIAs) should be performed before any new applications are launched in the IoT. (..). Where appropriate/feasible, stakeholders should consider making the relevant PIA available to the public at large. Specific PIA frameworks could be developed for particular IoT ecosystems (e.g smart cities, for which check D.1.2.2. of Synchronicity).
- Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).
- Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default.
- User empowerment is essential in the context of IoT. Data subjects and users must be able to exercise their rights and thus be “in control” of the data at any time according to the principle of self determination of data.
- The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. In particular, information and consent policies must focus on information which is understandable by the user and should not be confined to a general privacy policy on the controllers' website.
- Devices and applications should also be designed so as to inform users and non-user data subjects, for instance via the device physical interface or by broadcasting a signal on a wireless channel.

2. Application developers

- Notices or warnings should be designed to frequently remind users that sensors are collecting data. When the application developer does not have a direct access to the device, the app should periodically send a notification to the user to let him know that it is still recording data.
- Applications should facilitate the exercise of data subject rights of access, modification and deletion of personal information collected by IoT devices.
- Application developers should provide tools so that data-subjects can export both raw and/or aggregated data in a standard and usable format.
- Developers should pay special attention to the types of data being processed and to

¹⁹ pp. 21-23.

the possibility of inferring sensitive personal data from them.

- Application developers should apply a data minimisation principle. When the purpose can be achieved using aggregated data, developers should not access the raw data. More generally, developers should follow a Privacy by Design approach and minimise the amount of collected data to that required to provide the service.

3. Social platforms

- Default settings of social applications based on IoT devices should ask users to review, edit and decide on information generated by their device before publication on social platforms.
- Information published by IoT devices on social platforms should, by default, not become public or be indexed by search engines.

4. IoT device owners and additional recipients

- Consent to the use of a connected device and to the resulting data processing must be informed and freely given. Users should not be economically penalized or have degraded access to the capabilities of their devices if they decide not to use the device or a specific service.
- The data subject whose data is being processed in the context of a contractual relationship with the user of a connected device (i.e. hotel, health-insurance or a car renter) should be in a position to administrate the device. Irrespective of the existence of any contractual relationship, any non-user data subject must be in a capacity to exercise his/her rights of access and opposition.
- Users of IoT devices should inform non-user data subjects whose data are collected of the presence of IoT devices and the type of collected data. They should also respect the data subject's preference not to have their data collected by the device.

ANNEX C – RECOMMENDATIONS FOR DIFFERENT STAKEHOLDERS IN THE IOT DOMAIN

In appraising whether a PIA is necessary the following criteria should be considered, as indicated by the WP29.²⁰

1. **Evaluation or scoring, including profiling and predicting**, especially from “aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements” (recitals 71 and 91 GDPR). Examples of this could include a bank that screens its customers against a credit reference database, or a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks, or a company building behavioural or marketing profiles based on usage or navigation on its website.
2. **Automated-decision making with legal or similar significant effect**: processing that aims at taking decisions on data subjects producing “legal effects concerning the natural person” or which “similarly significantly affects the natural person” (Article 35(3)(a)). For example, the processing may lead to the exclusion or discrimination against individuals. Processing with little or no effect on individuals does not match this specific criterion.
3. **Systematic monitoring**: processing used to observe, monitor or control data subjects, including data collected through “a systematic monitoring of a publicly accessible area” (Article 35(3)(c))¹³. This type of monitoring is a criterion because the personal data may be collected in circumstances where data subjects may not be aware of who is collecting their data and how they will be used. Additionally, it may be impossible for individuals to avoid being subject to such processing in frequent public (or publicly accessible) space(s).
4. **Sensitive data**: this includes special categories of data as defined in Article 9 (for example information about individuals' political opinions), as well as personal data relating to criminal convictions or offences. An example would be a general hospital keeping patients' medical records or a private investigator keeping offenders' details. This criterion also includes data which may more generally be considered as increasing the possible risk to the rights and freedoms of individuals, such as electronic communication data, location data, financial data (that might be used for payment fraud). In this regard,

²⁰ WP29, DPIA Guidelines, pp.7-9.

whether the data has already been made publicly available by the data subject or by third parties may be relevant. The fact that personal data is publicly available may be considered as a factor in the assessment if the data was expected to be further used for certain purposes. This criterion may also include information processed by a natural person in the course of purely personal or household activity (such as cloud computing services for personal document management, email services, diaries, e-readers equipped with note-taking features, and various life-logging applications that may contain very personal information), whose disclosure or processing for any other purpose than household activities can be perceived as very intrusive.

5. **Data processed on a large scale:** the GDPR does not define what constitutes large-scale, though recital 91 provides some guidance. In any event, the WP29 recommends that the following factors, in particular, be considered when determining whether the processing is carried out on a large scale:
 - i. the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;
 - ii. the volume of data and/or the range of different data items being processed;
 - iii. the duration, or permanence, of the data processing activity;
 - iv. the geographical extent of the processing activity.
6. **Datasets that have been matched or combined**, for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject.
7. **Data concerning vulnerable data subjects (recital 75 GDPR):** the processing of this type of data can require a DPIA because of the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data. For example, employees would often meet serious difficulties to oppose to the processing performed by their employer, when it is linked to human resources management. Similarly, children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data. This also concerns more vulnerable segment of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.

8. **Innovative use or applying technological or organisational solutions**, like combining use of finger print and face recognition for improved physical access control, etc. The GDPR makes it clear (Article 35(1) and recitals 89 and 91) that the use of a new technology can trigger the need to carry out a DPIA. This is because the use of such technology can involve novel forms of data collection and usage, possibly with a high risk to individuals' rights and freedoms. Indeed, the personal and social consequences of the deployment of a new technology may be unknown. A DPIA will help the data controller to understand and to treat such risks. For example, certain "IoT" applications could have a significant impact on individuals' daily lives and privacy; and therefore require a DPIA.
9. **Data transfer across borders outside the European Union (recital 116 GDPR)**, taking into consideration, amongst others, the envisaged country or countries of destination, the possibility of further transfers or the likelihood of transfers based on derogations for specific situations set forth by the GDPR.
10. **When the processing in itself "prevents data subjects from exercising a right or using a service or a contract" (Article 22 and recital 91 GDPR)**. This includes processings performed in a public area that people passing by cannot avoid, or processings that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.

The WP29 considers that the more criteria are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects, and therefore to require a DPIA. As a rule of thumb, **a processing operation meeting less than two criteria may not require a DPIA** due to the lower level of risk, and processing operations which meet at least two of these criteria will require a DPIA

ANNEX D – QUESTIONNAIRE FOR THE PLAY TESTERS – VERSION 1

Q1) How long did you play the game? (please insert 1 number: the estimated number of minutes) []

Q2) How many cards did you play? (please insert only 1 number) []

Q3) What did you like in the game?

Q4) What did you dislike in the game?

Q5) Did you learn something new about privacy?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q6) Is the game useful for privacy awareness?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q7) Is the game easy to understand and to play?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q8) Are the questions clear and easy to understand?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q9) Which are your suggestions and comments to improve the game?

ANNEX E – QUESTIONNAIRE FOR THE PLAY TESTERS – VERSION 2

Q1) How long did you play the game? (please insert 1 number: the estimated number of minutes) []

Q2) With how many questions did you play? (please insert only 1 number) []

Q3) Name something you especially liked in the game

Q4) Name something you especially disliked in the game

Q5) Did you learn something new about privacy?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q6) Do you think that the game is useful to raise awareness about privacy?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q7) Is the game easy to understand and to play?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q8) Are the questions clear and easy to understand?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q9) Are the answers clear and easy to understand?

[1] not at all	[3] more or less	[5] very much
[2] rather not	[4] rather yes	[N] no opinion

Q10) Which are your suggestions and comments to improve the game?