Grant Agreement N°: 825082
Call: H2020-ICT-2018-2
Topic: ICT-27-2018-2020, Internet of Things
Type of action: CSA

Next Generation Internet of Things

Deliverable number	D2.1
Deliverable title	End-user engagement and trust building report
WP number	WP2
Lead beneficiary	3 - IIP
Deliverable type	Report
Dissemination level	PU
Delivery due month	M6
Actual submission month	M14 (Ver2)
Authors	Luca Bolognini – Francesco Capparelli – Claudia Bonari – Antonio Landi (IIP) - Pasquale Annichino (AS)
Internal reviewers	Federico Michele Facca (Martel) – Benoît Dalbert (AU)
Document version	Ver2 (Ver1 was rejected with the technical review 18.09.2019)
Project start date	01.11.2018
Project end date	31.10.2021
Duration in months	36 months

This report is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 825082.

Executive Summary

This is the project's D2.1 Deliverable addressing the Task 2.1 "End-user engagement and trust strategies" along with the work that has been performed under this Task. The report starts with an extensive study that has been performed by IIP about what arises from IoT-related projects in the H2020 framework. Among others, this study includes information about the scientific and academic publications in the IoT field. As has been identified, the new technology trends include how to properly address the relationship between government and companies and the end-users. In addition, the increasing number of devices connected via the Internet create new opportunities to enhance the abovementioned relationship reaching the potential for more rapid spread of the technology through an active participation and engagement of end-users.

The report is structured as follows:

1. *The 1st part "Introduction" describes the context of the project illustrating the scope, objectives and methodology pursued and analysing the ethical challenges related to the incorporation of AI-related tools in the IoT devices.*
2. *The 2nd part "Elements" is focused on the end-users engagement, with an overview on who are the end-users, why and how engage them in IoT environments analysing the elements that increase end-user's engagement with new technologies.*
3. *The 3rd part "End-users engagement measures" evaluates different measures that should be adopted in order to increase end-users trust and reliance with the IoT context, to make them opened to the adaptation of this new technology.*
4. *The last paragraphs ("Conclusions" and "References") contain the conclusions achieved through the research carried out and the references contained within the report.*

Abbreviations

D	Deliverable
EC	European Commission
ENoLL	European Network of Living Labs
GDPR	Regulation 2016/679 (EU) - General Data Protection Regulation
IoT	Internet of Things
LSP	Large-Scale Pilots
RFID	Radio-Frequency IDentification
TAM	Technology acceptance model
TTF	Task-technology fit
UTAUT	Unified theory of acceptance and use of technology
WP	Work Package
WP29	Article 29 Working Party
WT	Work Task

Contents

List of tables

1 INTRODUCTION

This section introduces the context and methodology of this report.

1.1 Context

During the last decade, the Internet of Things (IoT) has gained huge importance as it aims to provide people with innovative and intelligent technologies and services, in which all of the physical objects around them are linked to the Internet and are able to communicate with each other. We have witnessed the evolution of the traditional Internet into a global network of an enormous number of devices which are currently available to collect data that not only gather information from the physical environment but are designed to interact with people. Citizens have become sources of information and, at the same time, users of the information elaborated and provided by smart objects[1]. Different security challenges could face the adoption of the IoT. First, data anonymity, confidentiality and integrity are desirable to ensure the basic security concerns of end-users. Moreover, access controls, which control authentication and authorization, is required to prevent unauthorized access to the system. In this scenario, concerns with security and privacy regarding computer networks are always increasing. This kind of data processing has led to numerous discussions about the trade-off between the risks for the data protection of individuals and opportunities for the industry that arise from the analysis of such data sets. Those kinds of concerns have to be tackled in a trust-oriented approach, to fulfil the gap between the expectation in efficiency and the lack of information about the elaboration process and data usage that could lead citizens to lose interest and do not behave naturally in the interaction with IoT. The challenge is to develop technologies that are inherently privacy-preserving and may offer the basis for empowering the end-users (and more in general, the end-targets) to understand and be informed of (and, where appropriate, control over) the use of their personal data (within the meaning of Article 4.1) of the GDPR). Technology acceptance is a first step to beneficially use the IoT. Once accepted, the IoT potentially offers several benefits as it enables individuals to make better decisions to adequately address the matter, we have to consider not only end-users but also data subjects, whose data are being collected and processed through IoT even if not in an interactive usage.

In this context NGIoT project will lead to unlocking the growth potential of the Internet of Things (IoT) while respecting core European values, supporting key EU policies, leveraging the key associations, and establishing a Strategy Board. The project ambition is to create a human-centred IoT environment, through an inclusive and innovative approach developing research and innovation in this field.

1.2 Scope and Objectives

The purpose of this report is to provide elements and measures that have been identified in several European projects and through academic research to increase trust in end-users ensuring a privacy by design approach, in compliance with Article 25 of the GDPR. This report provides a synthetic view by

[1] "IoT systems are based on distributed software services that, through the Internet, enable the access to functionality and data provided by physical devices. These are the so-called smart objects [Atzori et al. 2010], i.e., devices generally equipped with sensors (able to detect different types of events occurring in an observed environment) and/or actuators (able to enact some actions determining a state change in the environment or in the IoT system itself)" in *Smart Objects to Smart Experiences: an End-User Development Approach – Ardito , Buono , Desolda , Matera.*

aggregating the know-how developed in European projects taking into consideration, as a main factor, data protection and security, considered as conditions that increase trustworthiness in the usage of IoT.

End-user engagement through trust building has been identified as one approach to address some of the challenges of the IoT by enabling people to set-up and use technology in line with their specific needs and preferences in a data protection by design approach. In order to achieve this goal, end-users need appropriate tools aimed at supporting them and in turn, in order to build such tools, developers need a deeper understanding of the elements and measures that have to be part of the designing process to increase acceptance in end-users.

1.3 Methodology

Through the collection of academic sources and the results of researches carried out by European projects, a division in two macro-categories has been elaborated. The first category concerns the elements, intended as social prerequisites relative to the context in which the end user interfaces with the IoT. The second category regards the measures, intended as methods which are likely to engage end-users in a conscious use of IoT.

1.4 Ethical challenges related to the incorporation of AI - related tools in IoT devices.

One of the main issue that shall be examined in the development of new technologies is related to the ethical aspects concerning their use. Several questions may be addressed in this field. In 2011, for example, the European Commissioner, Gerald Santucci, head of Internet of Things and Future Internet Enterprise Systems Unit from the European Committee underlined the fact that *"The Internet of Things does not refer only to things, but also to the relationship between the objects which surround the people daily and the people themselves"* and he was wondering: *"What place will the human beings have in a world in which 7 billions of people live together with 70 billion cars and a few thousand of billions of objects connected to an infrastructure of global networking, having the ability of self-coordination, self-configuring and self-diagnosis*[2]*"?*

The abovementioned questions are strictly connected with ethical issues that arise with the adoption of new technologies having a strong impact on daily life of individuals. As we will continuously deploy AI models in the wild we will be forced to re-examine the effects of such automation on the conditions of human life. Although these systems bring myriad benefits, they also contain inherent risks, such as privacy breach, codifying and entrenching biases, reducing accountability and hindering due process and increasing the information asymmetry between data producers and data holders.

Keeping track of every unethical or security breach incident will be difficult. Any failure or bugs in the software or hardware will have serious consequences. Even power failure can cause a lot of inconvenience. So, we may need another AI system on top of such AI enabled IoT to monitor its whereabouts each instant. But the main issue is related to the fact that we may need a democracy of such systems which will prevent themselves from not doing irrational things. Our lives will go on to be

[2] Santucci, G. (2011), *"The Internet of Things: A Window to Our Future"*, la http://www.theinternetofthings.eu/content/g%C3%A9rald-santucci-internet-things-window-our-future.

increasingly controlled by technology, and we will depend on them for everything[3]. Whatever be the case, humans should still have supremacy over all the man-made smartness. Only then we can control this revolution without getting enslaved by it.

On this regard it is urgent to regulate AI relationships with power reaffirming the primacy of the human that is imperfect, of course, but exactly for this reason able of being liable. We should talk about a "human rule of law"[4] and an algorithm should not be above the law. It is important, therefore, to set-up the rules of the game in the artificial age considering the fact that algorithms and non-human objects are and will be increasingly able to make decisions with significant effects, but also to self-evolve, self-produce and self-determine.

The biggest mistake would be to consider that behind an algorithm there is always a human programmer, but in reality we know that artificial intelligence - at least the specialized one - will be able to generate other algorithms (its children made of bits[5]). Children not alive, not human, but bit. Rather than talking about artificial, it would be more correct to speak of lifeless and not human.

Where there is no humanity there is no appreciation of the goods of life. Therefore, where these values are lacking, and above all, if they are not perceived as essential by the agent, there can be no liability. Thus, according to Luca Bolognini, the biggest mistake would be to recognize the legal personality or even citizenship for tangible or intangible objects without life or humanity: they would never be held empowered because they would not fear sanctioning and depriving consequences. In other words, the ability to feel emotions (a typical characteristic of a human being) is closely connected with the ability to be responsible and liable, a capacity that lifeless intelligence will probably never have.

Hence machines are not made to completely replace humans, they have been made to help humans reducing the tasks load. Obviously, humans need to maintain supremacy over machines.

AI is most effective when it is conjoined with human intelligence, rather than replacing it. It highlights the idea that computers and humans have different strengths in the vast field of excellence: computers are much more efficient at doing arithmetic jobs and counting, while humans show a remarkable performance in logic and reasoning. These differing forms of intelligence are complimentary, not diametrically opposites. Thus, AI is the technology that can fulfil our dream to have 'things' that can 'think'[6].

But, ultimately, the ethical rules of the game in the artificial intelligence age should always be established by the human being. No decision or rule (of law, but not only) should be left in the last instance to the non-human. The fundamental principle of rule of law, for which no president or king can be said to be above the laws in a democratic society, shall apply above all to algorithms and lifeless objects. This principle should be integrated and transformed expressly in modern constitutions, making it become the rule of Human law[7].

The Internet of Things can represent, if incorrectly managed, a danger from the perspective of ethics for the contemporary individuals and organizations. Every individual needs to be ensured that he/she will be protected by effective technical solutions, re-interpreted and updated for IoT (as, for example, encryption techniques, ID management, privacy enhancing technologies, digital watermarking, electronic signature etc..), legal/regulatory mechanisms (consumers consent, legislation limiting the data

[3] Ashish Ghosh, Debasrita Chakraborty, Anwesha Law; *"Artificial Intelligence in Internet of Things"*; IET Research Journals.

[4] Luca Bolognini; *"Se gli algoritmi vanno al governo"*; Left page 58, 11 October 2019.

[5] *Ibid ut supra*, note 4.

[6] N. Gershenfeld, *When Things Start to Think: Integrating Digital Technology into the Fabric of our lives*. Henry Holt and Company, 2014.

[7] *Ibid ut supra*, note 4.

collected and used by third parties, accountability of transactions mediated by IO etc.), economical measures (self-regulation, codes of conduct, consumer education, privacy certification) and social ones (public awareness, disclosure, public advocacy, consumer rights). After these first steps of awareness, further research must be done methodically on interventions needed to prevent the turning of IoT into a feared and intrusive Big Brother[8].

But on the other hand if well managed, following the above-mentioned measures, AI and IoT systems bear great potential benefits in individuals' life in areas such as transport, health, energy consumption, public space and environmental monitoring, as well as personalised and linked-up services for them.

[8] Daniela Popescul, Mircea Georgescu; "*Internet of Things – Some Ethical Issues*"; Article December 2013.

2 ELEMENTS

2.1 End-users engagement

In order to ensure greater protection for individuals - not only data-subjects - the legislator requires that economic operators using IoT devices think about privacy as a general preventive measure, rather than a tool to be used after damage occurred. The goal is to ensure an “individual-centric” approach, aimed at preventing violations of individual fundamental rights (e.g. to self-determination in managing their data). In fact, although end-users believe that the IoT has the potential to benefit them, they will always be concerned about their data security and privacy and any potential data breach. The opportunities provided by interconnected IoT devices are usually accompanied by many security and privacy issues. It is found that trust can be perceived as a significant factor that influences behavioural intention to use an IoT technology and has a strong effect in comparison to other concerns such as privacy[9]. Therefore trust and, more in general, a “digital education” are necessary conditions to properly engage end-users and other data subjects. Only when trust and confidence are satisfied, end-users and other data subjects may feel open to accept such technology.

2.1.1. Who are end-users?

We can consider four different categories, that depending on four different levels of end-user participation, have to be taken into consideration when the individual who ultimately uses or whose data are collected and processed through IoT even if not in an interactive usage is approached.

IoT development is carried out in four different ways:

a) Development *for* users (following their needs);
b) Development *with* users (using their collaboration);
c) Development *by* users (following their instructions);
d) Development *through* individuals (not only collecting users’ personal data, but in general through all individuals involved in an IoT environment whose data are not necessarily collected).

These categories are the first level of elaborating the end-user’s engagement and usually there are different methods to increase end-user’s engagement depending on which approach is chosen.

[9] Yildirima, H.; Ali-Eldina, A.; “*A model for predicting user intention to use wearable IoT devices at the workplace*”. J. King Saud Univ. Comput. Inf. Sci. 2018, in press.

2.1.2 Why engage end-users?

The most important reasons why end-users and individuals should be engaged are to develop a democratic process in both governance and business areas. Engagement can be defined as the process of involving individuals in governmental and business-related practices, mainly for providing feedback to governments and companies about services and products and to influence policy-making decisions.

In this context a project can include users/individuals as actors or as factors.

It has to be noticed that most of IoT solutions are moving towards "factorization" of people, meaning that people may be seen as objects (not data subjects) which interact with other sensors, condition which could potentially contrast with general data protection's principles of the European Union law. In particular it could contrast with the principles of fairness and transparency of the processing, which requires that the data subject shall be informed of the existence of a processing operation and its purposes (Articles 5.1.a), 12, and 13 of the GDPR).

In order to comply with such principles and obligations, the data controller[10] has to provide the data subject with the necessary information in order to ensure a fair and transparent processing, taking into account the specific risks and circumstances. That information may be provided in combination with standardised icons in order to give a meaningful overview of the intended processing in an easily visible, intelligible and clearly legible manner. Where the icons are presented electronically, they should be machine-readable.[11]

[10] Art. 4.7 GDPR:
'controller' means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[11] Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Another reason to engage end-users is to educate and train them. Through training and education, users' awareness increases and their skills in using IoT can improve, building a self-sustaining mechanism which can lead to strengthen trustworthiness in the usage of smart devices.

Given the technological nature of IoT, the end-user's acceptance of the technologies is very important when it comes to adopt a service. Three models have been elaborated to explain end-user's intentions and behaviour in the usage of IoT: the unified theory of acceptance and use of technology (UTAUT), the technology acceptance model (TAM), and the task-technology fit model (TTF).

The findings of the studies[12] related to those models highlight how users are likely to adopt the service if they think that it is useful, if fun and pleasure are additional characteristics, and if low risks in the usage are perceived. Social influence is considered to play an important role in an early stage of technology diffusion since most users lack reliable information about the new product or service, that is why, alongside end-users, often the behaviour of lead end-users is studied. Lead end-users are the early adopters of the IoT technology, and they should be identified as they could help facilitate the diffusion of IoT services.

2.1.3 How to make IoT environments user friendly

In order to engage end-users in an IoT environment the main aspect that should be considered is their trust in this modern technology despite unpredictable circumstances. Only trust is what makes people use such devices, despite all of the possible risks and the need to overcome perceptions of uncertainty and risk. Moreover, trust helps users to distinguish trustworthy products and technologies from the

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

[12] Shin D. A User-based Model for the Quality of Experience of the Internet of Things in INFMAN , 3 February 2017.

malicious ones[13]. Trust is essential to encourage people to easily adopt modern technology despite unpredictable circumstances. In uncertain situations, trust assists the individual to understand the social surroundings of the technology and decreases vulnerability [14]. Thus, trust is considered to be a serious factor in studies concerning IoT environments. Research of human behaviour online has highlighted the significance of embracing trust in adoption models to understand success factors behind user acceptance and adoption of IoT products and services [15].

In order to make an IoT product or service friendly for a user, there are several factors that could influence the user decision to trust an IoT environment. According to different models and studies, the following factors could influence trust affecting user's adoption decision.

a) **Functionality and reliability**. This factor refers to whether a technology has the capacity or ability to perform a specific task by providing required features and functions, and whether it will consistently operate properly and predictably[16]. It must have the capacity to detect data corruption and try to fix it. This feature is essential for IoT products and services to keep running efficiently and securely[17]. Technology's functionality trust depends on its ability to perform correctly. It is noted that consumers' trust is based on perceiving that the product or service will perform its proposed and required functions[18]. Because end-users usually do not accept a great amount of errors, their trust towards IoT adoption is strongly affected by the absence or a minimum number of errors[19].

   Therefore we can conclude that the IoT technology *functionality and reliability* have positive effects on trust towards its adoption.

b) **Helpfulness.** This factor refers to the technology's support and ability to provide adequate, effective, and responsive advice that may be necessary to complete a task (including instructions, guidelines, and help pages)[20]. End-users may not fully utilize a technology, as they may fear that they will not find the appropriate support if things go wrong. This may limit the benefits of the technology and usually will affect the adoption of the technology itself. Providing such support to users can guide them by avoiding undesired surprises[21]. Moreover, users who trust the support that is offered to them might perceive themselves to be more capable of using the system successfully. For instance, if users trust the interactive guidance of a system, they

[13] Falcone, R.; Sapienza, A. On the Users' Acceptance of IoT Systems: A Theoretical Approach. *Information* 2018, *9*, 53.

[14] Mayer, R.; Davis, J.; Schoorman, F. An integrative model of organizational trust. *Acad. Manag. Rev.* **1995**, *20*, 709-734.

[15] Belanche, D.; Casaló, L.V.; Flavián, C. Integrating trust and personal values into the technology acceptance model: The case of e-government services adoption. *Cuad. Econ. Dir. Empres.* **2012**, *15*, 192–204.

[16] McKnight, D.; Carter, M.; Thatcher, J.; Clay, P. Trust in a specific technology: An investigation of its components and measures. *ACM Trans. Manag. Inf. Syst.* 2011, *2*, 12.

[17] Areej AlHogail. *"Improving IoT Technology Adoption through Improving Consumer Trust"*. Article. 7 July 2018.

[18] Lai, I.K.W.; Tong, V.W.L.; Lai, D.C.F. Trust factors influencing the adoption of internet-based interorganizational systems. *Electron. Commer. Res. Appl.* 2011, *10*, 85–93.

[19] Bart, Y.; Shankar, V.; Sultan, F.; Urban, G.L. Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study. *J. Mark.* **2005**, *69*, 133–152.

[20] Tam, S.; Thatcherb, J.B.; Craigc, K. How and why trust matters in post-adoptive usage: The mediating roles of internal and external self-efficacy. *J. Strateg. Inf. Syst.* **2017**, *27*, 170–190.

[21] *Ibid ut supra* note 17.

may believe that they are more likely to use it effectively, leading to their adoption of that system[22].

Hence, we can assume that, in order to gain better trust that leads to IoT adoption, good investment in providing support for end-users is crucial and also this second factor relating to IoT technology *helpfulness* has a positive effect on trust towards its adoption.

c) **Ease of use.** This third factor refers to the degree to which a user considers that using a specific technology would be effort free. According to some scholars[23], a technology's ease of use plays a noteworthy role in building up the trust of users towards this technology. Usually, the ease of use or usability is affected by how accessible the system is to the users and how the interaction is designed. For example, the user should be able to use it correctly with a minimal chance of making mistakes[24]. This in turn usually affects the trust towards IoT adoption. Studies have revealed that a high usability of IoT products or services increases the satisfaction level of end-users and affects the adoption intention[25]. Consumers tend to trust commonly used IoT products and services and distrust cases that are perceived to be outside their control[26]. This is often a matter of perception (that may be correct or wrong), because mass usage of a tool (e.g. iPhone) does not mean that users can trust 100% on it or that they need to be aware that they shall configure it properly and don't give up on advanced security for making it easier to use. Thus, it is expected that the perceived *ease of use* has a significant effect on trust toward IoT adoption.

2.2 End-users' engagement elements

2.2.1 Location and timing

To increase end-user's engagement, the end user must be found in his natural context to make him feel safer, in a comfortable zone. Feeling as part of a test, or in a laboratory, could convey problems which can easily affect the results of the test itself.

End-users can be engaged at any stage of the innovation process. The best approach is to engage them as soon as possible, because the sooner information is gathered about end-user's behaviour, the better the final solution will be for them.

In order to build end-user's engagement in the experiments, a vast number of different methods and tools exist, ENoLL addressed the challenge to find relevant information and select appropriate means.[27]

[22] Daubert, J.; Wiesmaier, A.; Kikiras, P. A view on privacy & trust in IoT. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2665–2670.

[23] Lai, I.K.W.; Tong, V.W.L.; Lai, D.C.F. Trust factors influencing the adoption of internet-based interorganizational systems. *Electron. Commer. Res. Appl.* 2011, *10*, 85–93.

[24] Hochleitner, C.; Graf, C.; Unger, D.; Tscheligi, M. Making Devices Trustworthy: Security and Trust Feedback in the Internet of Things. In Proceedings of the Pervasive'12 Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK, 18–22 June 2012.

[25] *Ibid ut supra* note 17.

[26] Koien, G.M. Reflections on trust in devices: An informal survey of human trust in an Internet-of-Things context. *Wirel. Pers. Commun.* 2011, *61*, 495–510.

[27] https://www.u4iot.eu/userToolkit?fbclid=IwAR048Lk-b4QqU99MOr7vKva3fAKsfYVDjrAXxX-MJkypcMFfSjmUAz3MS_Q

A specific toolkit was created by ENoLL in the context of the European IoT LSP program to guide the researchers and practitioners through the innovation processes, with a specific focus on user-engagement. This toolkit, which can be followed according to the predefined instructions described by the tool itself, is available online[28], but from a pragmatic point of view, NGIoT project has to be designed with a tailored approach. Another approach, taken in consideration by the U4IoT[29] and Synchronicity Project[30], namely Living Lab approach, usually exploits a four steps approach based on contextualization, concretization, implementation and feedback gathering. The first phase aims to describe the framework and identify the group of users to be involved in the analysis. The concretization step is defined by the users' perception and their behaviour. During the implementation phase, the users are involved in the co-creation process. In the last step, users are required to provide their opinions on the experience in order to evaluate the change of attitudes and perceptions in relation to the products and services developed. Feedback has to be considered as a way to improve engagement and is one of the measures considered afterwards.

In the field of IoT personalization, a research carried out by professor Ardito presents a visual composition paradigm that allows non-programmers to synchronize the behaviour of smart objects with the aim of determining more engaging user experiences in cultural heritage sites by attributing the possibility to assign semantics to the objects[31].

2.2.2 Empowerment

Empowerment can be defined as the process of concretely enabling end-users to act as first actors in the IoT field by sharing their data with government and companies for the explicit purpose to improve services, thus collaborating in the whole co-creation lifecycle and producing a relevant impact on policy-making decisions.

Empowerment is a construct that measures perceived influence of consumer willingness to participate in the design of a product/services and consequent decision-making.

[28] Available at: www.european-iot-pilots.eu/u4iot/toolkit/

[29] U4IoT (User Engagement for Large Scale Pilots in the Internet of Things) brings together 9 partners from 5 European countries. The objectives are to develop toolkit for LSPs end-user engagement and adoption, including online resources, privacy-compliant crowdsourcing tools, guidelines and an innovative privacy game for personal data protection risk assessment and awareness, online training modules. More information is available at: https://u4iot.eu/.

[30] SynchroniCity: Delivering an IoT enabled Digital Single Market for Europe and Beyond) brings together 33 partners from 9 European countries and 1 from South Korea with the objectives to deliver a Single Digital City Market for Europe by piloting its foundations at scale in 11 reference zones – 8 European cities and 3 more worldwide cities. SynchroniCity is working to establish a reference architecture for the envisioned IoT-enabled city market place with identified interoperability points and interfaces and data models for different verticals. This includes tools for co-creation & integration of legacy platforms & IoT devices for urban services and enablers for data discovery, access and licensing lowering the barriers for participation on the market. SynchroniCity pilots these foundations in the reference zones together with a set of citizen-centred services in three high-impact areas, showing the value to cities, businesses and citizens involved, linked directly to the global market. More information is available at: https://synchronicity-iot.eu/.

[31] C. Ardito , P. Buono , G. Desolda , M. Matera (2017): *From Smart Objects to Smart Experiences: an End-User Development Approach* in International Journal of Human-Computer Studies.

While end-users feel empowered and, as a result, are enticed to add value to existing services through consuming and co-creating, governments and companies will have the opportunity to fully exploit the potential of innovative technologies to better optimise their delivery of services.

End-users, data subjects, and other individuals will need to acknowledge that IoT can also help empowering them. IoT features can increase their engagement levels towards a more proactive and mature role when interactive with public/private IoT service. IoT-enabled technologies can be utilized to further support the increase and participation of end-users as contributors and 'values added' of information to the IoT echo-system. End-users, government and business have the need to find new communication channels and processes to enable them to participate in the innovation process.

Within the IoT context, empowering end-users can contribute to concretely solve a potential lack of transparency and trust. Within this process, end-users have to be seen as real time data providers who are able to provide added value from data to be used for improving decision making processes and governmental and business-related digital services. An empowerment approach means that end-users are actors in generating economic and social impacts for the benefit of themselves and the society.

The studies around user's acceptance and adoption intention have provided several implications for businesses. Researchers confirmed that the determinants of users' adoption intention play a necessary role in investigating the implementation of smart cities, given that social influence that could be carried out by the end-user. Thus, empowerment has to be considered as an essential adoption factor.

2.2.3 Skills

Several internet end-user's skills are an important precedent for IoT acceptance and usage: mobile, information navigation, social, and creative Internet skills directly or indirectly contribute to the level of IoT skills. People's self-assessment of their IoT skills is important for IoT usage acceptance. Universities and schools have an important role in education, which can increase literacy in relevant skills and, by doing that, indirectly engage end-users.

Unlike earlier technologies, operating IoT devices does not involve continuous interactions between users and devices, therefore, people should be able to familiarize themselves with the enormous amount of data gathered without their active participation. Lacking the skills to correctly interpret, analyse, and communicate data could result in users collecting irrelevant data or failing to apply the data. These skills concern changing settings, interpreting data, sharing data. Internet skills develop through learning from doing, trial and error, problem sharing, and comparing to others through experiencing what to pay attention to when problems occur.

The acceptance of the IoT includes the perception of the end-users of their own skills, abilities, and resources to successfully perform IoT-related tasks and behaviours. Internet skills, and the ways in which they are generated, are transferable to IoT. Internet skills are dived in operational, mobile, social and creative skills. Operational skills consist in the ability to properly use the interfaces and regard the ability to search the Internet, including finding, selecting, and evaluating information sources. Mobile skills are related to the ability to perform download and install applications and monitoring the data costs involved in online mobile use. Social skills enable using online communication and interactions to understand and exchange information. Creative skills are the skills necessary to create content suitable for online display like text, music and video, photo or image.

The research carried out by De Boer, van Deursen and van Rompay, "Accepting the internet of things in our homes: The role of user skills"[32] shows that is expected that mobile skills will be needed for the initial setup and configurations of settings, but will play a less profound role in the continuous interaction between users and technology. In contrast, the researchers expect information navigation, and especially social and creative skills to become more important for interaction in the IoT system due to the emphasis on content visualization, interpretation, and sharing. Thus, internet skills are important for performing on IoT skills because mobile, information navigation, and creative skills, directly contribute to learn IoT skills. Anyway, social skills are also important in the IoT, this kind of skills contributes to the use of the IoT both directly and indirectly, because people's assessments of their own capabilities in using the IoT are important to actually start using the products.

2.2.4 Motivation and reward

Studies have concluded that direct interaction with IoT could increase the end-user's engagement even in their cultural interest, which in turn increase the end-user's engagement in a bilateral process[33]. The interaction with IoT favours emotions, improves understanding and increases the appropriation of cultural related contents. A gamification process is a growth factor in increasing end-user's engagement due to the level of interaction and the potential transfer of several information from the IoT environment to the end-user and vice versa.

This finding indicates that people are motivated to use the IoT because it is useful to them, even though they do not have an outspoken positive attitude towards using it.

In "An IoT-Based Gamified Approach for Reducing Occupants' Energy Wastage in Public Buildings" by T. Papaioannou et al[34] a reward-based model with a gamification approach was designed to demonstrate how users become engaged in the usage of IoT for the purpose of saving energy. A gamified application that motivates respective behavioural changes combining team competition, virtual rewards and life simulation brought to the engagement of end-users to reach a pre-established goal.

Balaji and Roy, in a 2016 research on the retail industry, found that the continuance intention of customers to use IoT technologies is also influenced by perceived value co-creation, which is determined by consumer experience attributes. Accordingly, with the aim of enhancing perceived value co- creation for customers, retail stores should ensure that the adopted IoT technologies are user-friendly, thus reducing customers' emotions of frustration and discomfort and are able to improve the effectiveness in the shopping process. Thus, the motivation to improve their shopping process led to increase end-user's engagement.

[32] De Boer, P.S., van Deursen, A.J.A., van Rompay, T.J.L. (2018): *Accepting the Internet-of-Things in our homes: The role of user skills, Telematics and Informatics* in https://doi.org/10.1016/j.tele. 2018.12.004

[33] Ardito C., Buono P., Desolda G., Matera M. (2017). *From Smart Objects to Smart Experiences: An End-User Development Approach* in International Journal of Human-Computer Studies, December 17, 2017;

[34] Papaioannou, Thanasis & Dimitriou, Nikos & Vasilakis, Kostas & Schoofs, Anthony & Nikiforakis, Manolis & Pursche, Fabian & Deliyski, Nikolay & Taha, Amr & Kotsopoulos, Dimosthenis & Bardaki, Cleopatra & Kotsilits, Sarantis & Garbi, Anastasia. (2018), *An IoT-Based Gamified Approach for Reducing Occupants' Energy Wastage* in *Public Buildings. Sensors*. 18. 537. 10.3390/s18020537.

2.2.5 Satisfaction

Satisfaction is the sum of system, content and service quality in IoT. Content quality is defined here as the relevance, reliability, and timeliness of knowledge provided by IoT services. System and service quality are defined as the user evaluations of system and service performance when delivering information and meeting user needs. User's satisfaction directly and indirectly influences users' behaviours, such as purchasing behaviour and intention to use.

Ubiquitous computing is becoming deeply embedded in people's lives, through IoT, people record and monitor themselves, they target behavioural problem, situation, symptom, or a disruption that symptoms may produce, as well as inner thoughts or feelings and objective information.

The proliferation of IoT makes collecting personal data easier, and thus has to be properly addressed how to help people engage with these systems and how consumers evaluate quality.

To be focused on the concept of the user's perceived quality means that the performance in terms of error, transmission delay and availability is a requirement that for most IoT-based services and does not directly imply the end-user's engagement. Most service providers are thus shifting their focus from an approach based on the evaluation of technological performance to one oriented on the user-engagement's measures.

The overall acceptability of an application or service as perceived subjectively by the end user is the main focus of several scientific publications in the IoT field. Addressing consumer expectations, feelings, perceptions, cognition, and satisfaction about a particular product, service, or application can act as a useful tool to enhance IoT products and thus increase end-user engagement. The concept of usability in the IoT field has been based on analyses of the media's technical properties; nonetheless it is important to estimate user satisfaction to assess if the users will be engaged in the usage of the products.

Several authors recognize how end-user satisfaction directly and indirectly influences user behaviours such as purchasing behaviour and intention to use. Although user satisfaction has become a topic of great interest to human-computer interaction and marketing researchers alike, its relation to psychological factors has been widely debated and new cognitive factors such as coolness and affordance emerged. Coolness can be defined as a sum of subcultural context, attractiveness and originality; affordance is "a relation between an object or an environment and an organism that, through a collection of stimuli, affords the opportunity for that organism to perform an action"[35].

Those two elements combined lead to satisfaction, which, in turns, can lead to end-user engagement. The affordance concept is particularly important in the IoT because the interface between it and users is nonlinear and unstructured, thus affordable interfaces and interactions facilitate certain user behaviours. Nonetheless, satisfaction cannot be measured by technological features because it is a subjective experience only captured by the end-users. Satisfaction leads to engagement because is a user-based dimension that encompass new factors and conceptualizes them as a quality of experience. Satisfaction can significantly influence attitudes and trigger behaviours of users. Furthermore, it exists in the users' domain, so an individual's quality of experience depends on how that user accepts, experiences, and interacts with an IoT product.

[35] Norman, D. A. (1990), *The design of everyday things. New York: Doubleday.*

Several studies on user satisfaction have often been criticized for their lack of context which leads to weak satisfaction models but, incorporating IoT, as a collection of objects with common property, specific factors and contextual considerations, into a satisfaction model, allows a better explanation of how the factors influence users' satisfaction and how that satisfaction, in turn, affects end-user engagement. Thus, how users feel about and perceive their technology usage seems to be more important than what technological functions offer to them.

Consistent with prior research in technology acceptance, the construct of satisfaction plays a major role in end-user's engagement toward products and services. The findings of the studies in this field provided useful insights for the development of strategies to meet end-user demands. IoT services conducted in accordance with user satisfaction could lead to end-user engagement and constitute a prerequisite of the measures to properly engage end-users while increasing their trust in the products.

Another factor that could influence users' satisfaction and engagement towards an IoT environment is the so called "social influence". It is demonstrated that a person's perception of a product or a service is highly influenced by the perceptions of others. The Unified Theory of Acceptance and Use of Technology (UTAUT) considered social influence as one of four factors that influence consumers' technology adoption. Gao and Bai[36] and Abu et al.[37] found a positive influence of social-related factors on the adoption of IoT technology. Social influence has gained extensive attention in the information systems field[38]. The social influence can be analysed through two precise factors: social network and community interest.

The individual social network refers to the notion that opinions and evaluations of a product will influence the individual decision on that product[39]. Therefore, the model should incorporate social influence as an influencing factor. It is demonstrated by a person's perception of whether other significant people in their community perceived that they should engage with this technology or service[40]. Social networks play a crucial role in influencing the user adoption of IoT technology since users generally seek information from peers, family, and even social media influencers' reviews to reduce IoT product or service uncertainty prior to purchase[41]. In this case satisfaction can be seen as result of the number of users involved in the adoption of a new technology. In fact users generally trust relevant users' reviews and feedbacks since these reviews can be taken as trusted evaluations of a product. As Gao and Bai[42] stated, numerous consumers have considered mobile IoT devices to be trustworthy since these devices have trended on their social networks. However, customers tend to doubt or resist the reviews and evaluations by developed companies. Thus, social networks play a significant

[36] Gao, L.; Bai, X. A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pac. J. Mark. Logist.* 2014, *26*, 211–231.

[37] Abu, F.; Jabar, J.; Yunus, A.R. Modified of UTAUT Theory in Adoption of Technology for Malaysia Small Medium Enterprises (SMEs) in Food Industry. *Aust. J. Basic Appl. Sci.* 2015, *9*, 104–109.

[38] Choi, B.; Lee, I. Trust in open versus closed social media: The relative influence of user- and marketer-generated content in social network services on customer trust. *Telemat. Inform*. 2017, 34, 550–559.

[39] *Ibid ut supra* note 17.

[40] *Ibid ut supra* note 36.

[41] *Ibid ut supra* note 38.

[42] *Ibid ut supra* note 36.

role in influencing consumer trust toward IoT adoption and must be taken into account when introducing IoT products or services into the market[43].

Therefore users' satisfaction on IoT products and services can be evaluated through the analysis of social network opinions and feedbacks on this technology, because bigger is the number of users positive involved in the use of IoT technology, stronger will be its market power and dissemination.

Another important factor is the community that empowers trust and satisfaction allowing interaction between objects of the same community[44]. Community interest and culture could highly affect how individuals make their decisions. Although globalization has enabled the world to grow closer, cultural differences still can distinguish nation from nation and a deeper analysis on the potential consequences relating to the adoption of a new technology on certain areas should be done before its adoption. For instance, a conservative Middle-Eastern culture could react differently to video-camera sensors than less conservative cultures[45]. Managing trust requires an in-depth investigation of the local market, as domestic culture might create barriers, in addition to national legislation. National differences might have a positive or a negative effect on trust in any new technology and on its adoption and consequent users' satisfaction[46]. It is also important to note that sometimes the lack of alternatives or necessity could influence that factor towards trust.

Consequently, it is evident that, for any new IoT technology or service entering a new market, the local community interest must be taken into the account and a deep investigation and appreciation of the local perceptions and opportunities related to trust and users' needs to be satisfied must be conducted.

[43] Lin, Z.; Dong, L. Clarifying Trust in Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* 2018, *30*, 234–248.

[44] Kowshalya, A.M.; Valarmathi, M.L. Trust management for reliable decision making among social objects in the Social Internet of Things. *IET Netw.* 2017, *6*, 75–80.

[45] *Ibid ut supra* note 17.

[46] Blomqvist, K.; Hurmelinna-Laukkanen, P.; Nummela, N.; Saarenketo, S. The role of trust and contracts in the internationalization of technology-intensive Born Globals. *J. Eng. Technol. Manag.* 2008, *25*, 123–135.

3 END-USER ENGAGEMENT MEASURES

Nowadays, the value for ICT providers lies on offering personalized services and contents, that are based on the combination of a huge amount of data collected from different sources. The figure of an interconnected industry acting as an “orwellian” eye capable of linking different personal data makes the user-data subject feels that he/she has no control over the use of his/her personal data.

Users may find themselves under monitoring, especially when the collection and processing of their data is not made in a transparent manner. The “non-centrality” of the user in IoT is also apparent in relation to the exercise of his/her rights: users are in most cases unable to access the personal data collected by IoT devices, which inevitably results in the impossibility of making choices about such data. Not forgetting also all the rights that has to be guaranteed to the data subject under the GDPR: the right to be informed (Articles 12 to 14); the right of access (Article 15); the right to rectification (Article 16); the right to erasure (Article 17), the right to restriction of processing (Article 18); the right to data portability (Article 20); the right to object (Article 21); and the right not to be subject to automated individual decision-making (Article 22).

In order to ensure greater protection for individuals, not only data subjects, the legislator has imposed on economic operators using IoT devices to think about privacy as an instrument that should intervene not just after the damage has been caused, but rather as a general-preventive measure. The goal is to ensure a “user-centric” approach aimed at preventing that constant dialogue devices, and continuous processing of personal data could result in a violation of the individual’s right to self-determination in managing his/her data.

To make sure to engage end-users is a necessary condition to increase their trust. Only when trust and reliance are satisfied, end users can be considered opened to the adaptation of such technology.

Some measures aimed at achieving this goal are described below.

3.1 Feedback

One of the most important measures to increase end-user’s trust and assess their engagement is to give them constant feedback. In fact, giving credit to users on what is happening whit their data, with theirs input, increases their perception of security, making them feel subjects that are involved in the process, rather than objects from which information is harvested.

The relationship between the IoT technology and the users must not be unilateral: the information must not arrive only from the users to the device, for the latter to process it; the information must also be sent from the IoT device to the end-users so that they are constantly updated on the use made of their data.

This is a factual implementation of what has been suggested since 2010 by the WP29 (now European Data Protection Board) that identifies a set of “Obligations and rights” for ad network providers and publishers, stating that: “*Network providers/publishers should provide the information directly on the screen, interactively, if needed, through layered notices. In any event, it should be easily accessible and* *highly visible”*[47]. This clearly represents the aim of the feedback, which intends to simplify - and makes it solid - the relationship between IoT-technology and data subject: it will be an user-friendly and freely available tool for citizens/users/consumers, that enables them to understand, whenever they want (right of access), which kind of data are involved and the logic that rules the processing (right to receive the information/right of access), showing it continuously and promptly. The end-users also should be involved in the risk assessment process to address properly the risks that users can perceive and in co-creation of metrics and threats catalogues in order to perform Data Protection Impact Assessment according to Article 35 of the GDPR and risk assessment in order to be compliant with Article 32 of the GDPR.

Giving feedback to users also means taking into consideration their requests and their needs. Therefore, in addition to feedback, it is necessary to apply their suggestions.

At the same time, it is necessary to analyse feedback received from end-users, which should not be understood as the only input or just positive responses. Much more important in order to improve end user’s engagements are negative comments or the reasons why an end-user stops using IoT technology. Analysing this type of feedback and improving the abovementioned aspects enables the stakeholder to increase end-user engagement.

3.2 Crowd Privacy

One of the typical problems of the IoT scenario, especially in public contexts or in smart cities, is the difficult perception of the sensors by the individuals who are in those places. For this reason it is very difficult for individuals within an IoT environment to understand how to defend themselves in such environments. A solution that could be help to individuals is the so called “Crowd Privacy”. This measure enables end-users in order to organize self-defence measures from cyber threat and privacy-related issues to exchange information and spread awareness on-line. In IoT environments Crowd-Privacy can increase end-user engagement. An example in this field is the Synchronicity project the purpose of which is to open up a global IoT market where cities and businesses develop shared digital services to improve the lives of citizens and grow local economies.

Crowdsourcing mechanisms aim to identify, monitor and assess privacy-related risks, can increase trust and consequently engagement. End-users would feel more comfortable having a way to comment and alert other users on privacy-related risks.

Tools intend to simplify the relationship between IoT technology and data subjects have to be user-friendly and freely available; they have to enable them to understand, whenever they want (right of access), which kind of data are involved and the logic that regulates the processing (right to receive the information/right of access), showing it continuously and promptly, each time.

A tool, for example, can be matched with a smartphone app and by using the app an end-user can discover if there are new devices or sensors around him and decides to deactivate them.

[47] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, Adopted on 22 June 2010, in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

Hsu and Lin in 2016, developed a conceptual framework to understand the motivations of continued use of IoT services by investigating network externalities and information privacy factors[48]. Information privacy protection is of high concern for users. Data collected by the service providers may be beyond the users' control, be accessed and used without authorisation, or may be erroneous. Based on these concerns, four facets of concerns about information privacy are summarised as: collection, unauthorized secondary use, improper access, and errors. Results of the Hsu and Lin research show that the privacy concerns have less effect on users' continued intention to use compared with the perceived benefits[49]. This implies that users are more willing to adopt and use the IoT services when they are perceived to be compatible with the users' values and beliefs.

Privacy Flag[50], a H2020 research project on personal data protection, developed a set of tools to enable citizens to check whether their rights as data subjects are being respected, and tools and services to help companies to be compliant with personal data protection requirements. Privacy Flag IoT tool is available via the Privacy Flag app.

The findings of Privacy Flag on what a tool of Crowd Privacy has to contain are the following:

- Must be easy to rate/assess;
- Establishing sub-communities that would specialize on certain objective aspects, e.g., privacy and malicious contents;
- Suggestion to rate similar websites;
- Less text as possible, text broken down into meaningful segments;
- Icons should tell the story - colors;
- Outreach through the add-on/app;
- Drivers of Collaboration Crowdsourcing: Enjoyment, satisfy members, needs and interest, recognition, collectiveness, appreciativeness/attention, responsiveness, trustworthiness, fun, altruism, reciprocity, identification, personal need.

3.3 Human Law by default (adoption of a code)

The measure of human law by default embed the concept that subjecting end-users to rules, regulations, laws, decisions and codes that are automated and artificially created would not increase end-users' trust. If a public law is generated from an inhuman algorithm or an IoT are designed without an ON/OFF button, it is possible that end-users would leave feel not comfortable in the adoption of IoT solutions.

IoT should be controlled only by humans and not by other machines – meaning that for each device there should be at least one human super-admin and no artificial super-admin. On this regard the adoption of a code of conduct, pursuant to article 40 of the GDPR, could help trade associations or bodies representing IoT sector to apply the GDPR effectively and allow them to demonstrate their compliance. The tool of the code of conduct can collectively address the specific needs of micro, small

[48] Hsu, C. L., & Lin, J. C. C. (2016), *An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives* in *Computers in Human Behavior, 62*, 516–527.

[49] *Ibid ut Supra.*

[50] More information is available at https://privacyflag.eu/

and medium enterprises and help them to work together to apply GDPR requirements to the specific issues in the IoT sector. Codes are expected to provide added value for their sector, as they will tailor the GDPR requirements to the sector or area of data processing. The adoption of a code of conduct could be an effective mean to enable compliance with GDPR for IoT sector and its members.

In addition the adoption of a code of conduct can help – among the others – the data subjects to exercise their rights recognized in Article 22.1 of the GDPR, that is the right *“not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”*.

Therefore, profiling operations that consist *“of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements”* (Recital 71 of the GDPR) are related to a specific right under certain circumstances (if they “produces legal effects” or “significantly affects” the data subject). In fact, a code allows them to know why they have been targeted and which sources are behind the data combination. A code of conduct may also provide measures to facilitate the way to *“exercise of the rights of data subjects”* in case of profiling that *“produces legal effects”* or *“significantly affects”* them, but also in other circumstances.

In conclusion, codes of conduct could – particularly if targeted on specific sectors – improve the confidence of citizens/users/consumers towards IoT technologies and data markets, offering them a solid basis of empowerment so as to understand, be informed of and control over the effects implied by the data processing activity.

At the same time, data controllers and content providers would improve their tools, thanks to the commitments and the labelling and that, in terms of data protection, can represent an instrument for the safety of the consumer/citizen/user, capable of increasing the trust and improving the confidence in the IoT systems.

3.4 Metaphor of “food & drug” comparison

In the IoT supply chains (life cycle), personal data can go through a complex “itinerary” (both in the sense of path and journey) which involves a transfer between different subjects, objects, accountability and liability centres and therefore between several controllers and processors (some of these are human, other machine learning based software, objects, etc.). In outlining this context, we need to identify the measures that can govern this process.

In this case it would be advisable to adopt the “food & drug approach”: precisely because of this complexity of the personal data’s life cycle, it is practically impossible to trace the whole supply chain through a *probatio diabolica*. In fact, in many cases it is very difficult to explain all personal data’s life cycle *ex ante* in an information notice (pursuant to art. 13 and 14 GDPR - the latter is an *ex* post for what is provided, but the contents concern an *ex* ante representation in abstract). Therefore, in order to inform data subjects on the processing of their personal data we could use the metaphor of “food & drug additives labelling”. We should take into consideration the pre-packaged snack: on the label end-users are able to find crucial information, such as the name of the manufacturer, where the product was packaged and the best before date. More importantly still, end-users can see the ingredients, additives and preservatives included. Also, end-users can find the number of calories and even the provenance and traceability of the raw materials. As ordinary consumers it would make no sense to show the results of the bio-chemical analysis carried out on that food product (as prescribed by Article 13 of the GDPR).

Users receive their “food for thoughts” in a transparent way, knowing what they are taking, such as when a consumer reads food labels; moreover, users discover why they have been targeted, understanding the criteria and the sources which are behind the digital food, as if the producer gives them the recipe. The users increase their level of trust and awareness thanks to all the information received. When designing IoT technologies, a small label should be included in the top right or bottom left corner. This label - like the one used for snacks - would spell out which data has been used and by whom and shows the end-users how they can remove or amend their data. This also because the end-user will not read it and there would not be a useful moment to communicate all the information required by the GDPR (pursuant to articles 13 and 14 of the GDPR).

To ensure end-user trust an IoT technology have to enable him/her to know if/which (his/her) data are tracked, their origin (from which third parties they came) and the logic of the processing that has led to a certain profiling result – if a profiling operation has been carried out starting from Big Data. For example at the time of the collection of data subject's personal data – that could be uploaded a month before from different sources and even if it would be possible that from every source the user has an information – also in the strange hypothesis in which controller succeed to inform the end user of this complex procedure, end-user would be provided with such complex information that an average person would not understand. What the end user is interested in are the summary information and the main sources of data collection. Such information will also help non-expert users to understand which kind of data are involved and the logic that rules the processing, by labelling the structure (data, sources, criteria) of the processing itself. As deduced by the lawfulness, fairness and transparency principle (Article 5.1.a) of the GDPR) the users/citizens/consumers should know what they are taking and why, understanding criteria and analysis which are behind a specific content proposal in the digital environment.

The metaphor of “food & drug additives labelling” fits again: users receive their “food for thoughts” in a transparent way, knowing what they are taking, such as happens when a consumer reads the food label; moreover, users discover why they have been targeted, understanding the criteria and the sources which are behind the digital food, as if the producer gives them the recipe. The users increase his/her level of trust and awareness thanks to all the information received. So, as happens with “food & drug”, the data subject/consumer put his/her trust in certain producers/controllers because he/she knows what they are administering to him/her and why he/she has to take (or should take) this kind of product.

3.5 Labelling Interface approach

As RFID technologies and video surveillance, the IoT technologies need to be reported. In fact, end-users must be adequately informed about the use of IoT systems, as well as the existence of optical readers who activate the label.

For this reason, according to Article 12.8 of the GDPR: *“The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardized icons”*.

It is important that the end-user is informed of the sensing capabilities of an environment and data processing. It is important for the end-user and data subject to be notified of the collection of personally identifiable data before entering a space with such sensing capabilities.

The information to be provided to end-users and data subjects may be added in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. The information to be provided to data subjects and to end-users can even have the form of a comic.

The importance of the information should be considered to warn and provide information to targeted-individuals who are not end-users in order to prevent negative effects caused by IoT deployments. IoT could be equipped with well-visible interfaces. For example, an image sensor and IoT object could be equipped with eyes, so as to increase awareness on the presence of the sensor and increase user confidence in using objects that gather data.

3.6 Choices & Consent (Control Panel)

In order to increase engagement and trust the end-users have to be in the condition to choose freely if they want to be involved in the data processing carried out by the IoT environment.

Nonetheless, the end-users should be able to choose freely what kind of personal data they share with the IoT environment before interacting with it in an ex-ante approach (opt-in).

End-users have to be able to control their data after the process in order to eventually exercise their rights in an ex-post approach (opt-out).

This would involve scrutinizing device settings, in addition to data visualization, interpretation, and sharing: a clear visualization facilitates interpretation. Data sharing is required to, for example, compare data from other users, make sense of their comments and opinions, and discuss data with one another online or offline.

Next to the amount of data, the complexity of them is increasing, and this can be attributed to the ability of IoT systems to make data-based decisions without interference from the user. This autonomous decision making, together with the connectivity between users and other devices, can result in problems in identifying who owns the data and defining system boundaries.

Due to the autonomous characteristics of the IoT, sharing content has become a matter of making choices regarding changing settings of what to share, when to share, and who to share with. Nonetheless, knowledge on the settings regarding data sharing is required since the collected data comprise personal information on habits and health, which could also be of interest to others. The need for consideration of potential negative consequences of data sharing behaviour, together with having to change sharing settings on the preferences, underlines the importance of awareness regarding autonomous content sharing and strategic decision making.

Developers of the IoT should provide guidance by clarifying what data are gathered, with whom the data are shared, and how to change settings related to data sharing. This is one of the measures that and IoT producer has to carry out in order to be compliant with GDPR provisions, such as the ones provided for by Article 6 if the GDPR, which states that:

"*processing shall be lawful only if and to the extent that at least one of the following applies:*

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing 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;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official

authority vested in the controller;

(f) processing 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."

And Article 7 which states that:

"*1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

The data controller must also deal with the obligations related to the provision of information as provided for by Articles 13 and 14.

The WP29, in the Guidelines on Consent under Regulation 2016/679[51], established that "[w]here consent is obtained through use of a service-specific user interface (for example, via a website, an app, a log-on account, the interface of an IoT device or by e-mail), there is no doubt a data subject must be able to withdraw consent via the same electronic interface, as switching to another interface for the sole reason of withdrawing consent would require undue effort. Furthermore, the data subject should be able to withdraw his/her consent without detriment. This means, inter alia, that a controller must make withdrawal of consent possible free of charge or without lowering service levels."

[51] Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, in https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

According to the above cited Guidelines, consent requires a statement from the data subject or a clear affirmative act which means that it must always be given through an active motion or declaration. It must be obvious that the data subject has consented to the particular processing.

Article 4(11) of the GDPR builds on this definition, by clarifying that valid consent requires an unambiguous indication by means of a statement or by a clear affirmative action.

The Guidelines clarify that physical motions can be qualified as a clear affirmative action in compliance with the GDPR. Here an example:

“Swiping a bar on a screen, waiving in front of a smart camera, turning a smartphone around clockwise, or in a figure eight motion may be options to indicate agreement, as long as clear information is provided, and it is clear that the motion in question signifies agreement to a specific request (e.g. if you swipe this bar to the left, you agree to the use of information X for purpose Y. Repeat the motion to confirm). The controller must be able to demonstrate that consent was obtained this way and data subjects must be able to withdraw consent as easily as it was given.” Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the GDPR.[52]

[52] Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

2. The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.

3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

4. If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

5. Information provided under Articles 13 and 14 and any communication and any actions taken under Articles 15 to 22 and 34 shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

- The IoT data controller must provide individuals with information including: its purposes for processing their personal data, its retention periods for that personal data, and who it will be shared with.
- The IoT data controller must provide privacy information to individuals at the time the IoT data controller collects their personal data from them.
- If the IoT data controller obtain personal data from other sources, the IoT data controller must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. There are a few circumstances when the IoT data controller does not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information the IoT data controller provides to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.
- The IoT data controller must regularly review, and where necessary, update its privacy information. The IoT data controller must bring any new uses of an individual's personal data to their attention before the IoT data controller starts the processing.

By complying with the obligation on information notice can help the IoT data controller to comply with other principles and obligations of the GDPR and build trust with end-users.

Hereinafter, a summary of the contents of Articles 15 to 22 of the GDPR which contain the rights of the data subject and therefore of the end-users (all terms in capital letters refer to the definitions given in the GDPR).

- Right of access: According to the right to access pursuant to Art. 15 GDPR, the Data Subject has the right to obtain the confirmation as to whether Personal Data concerning him or her is being Processed and, if it is the case, the Data Controller has to provide the Data Subject with access according to the modalities set forth in Art. 15 GDPR. The right of access implies, in any case, the right to receive a copy of the personal data being processed.

- Right to erasure: the so-called "right to be forgotten" is defined as a right to ask for the deletion of personal data in a strengthened form. It is mandatory for controllers to inform other requesting owners of processed personal data, including the cancellation request. According to the right to erasure under Art. 17 GDPR, the Data Subject has the right to request and obtain the erasure of

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6. Without prejudice to Article 11, where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

7. The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 92 for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

Personal Data or the anonymization of them provided that it takes place by means of techniques which avoid the re-identification of the Data Subject. Subject to the assessment of the conditions set forth in Art. 17.1 GDPR, the Data Controller, having considered the technologies at its disposal and the cost, has to promptly notify the erasure unless it involves a disproportionate effort, to all Recipients to whom Personal Data has been communicated, requesting them to erase the same Personal Data; in the event that Personal Data was disclosed or made public – (e.g., Personal Data published on the website of the Undertaking), any other Recipient who has collected these data, to erase any links to, or copies or replications of that Personal Data. The erasure of Personal Data has to be done from all corporate information systems. The Data Controller communicates to the Data Subject the erasure once completed. The Data Subject may require withdrawing his or her Consent at any time without providing any explanation. Following such request, the Data Subject's Personal Data has to be deleted or alternatively anonymized pursuant to Art. 17.1 GDPR, unless there is a further legal basis that legitimises the continuation of the Processing activity (e.g., compliance with a legal obligation). Depending on whether or not there is such further legal basis, the Data Controller will notify the Data Subject about the withdrawal of the Consent.

- The right to restrict processing requires that personal data be "marked" pending further determinations; therefore, it is advisable for the data controller to include in their information systems (electronic or otherwise) suitable measures for this purpose. The request for restriction of the Processing pursuant to Art. 18 GDPR, with the exception of storage, implies the prohibition of any type of Processing of the Data Subject's Personal Data unless the following circumstances apply: the Data Subject's Consent has been received; it is necessary for the establishment, exercise or defence of legal claims; it is necessary to protect any other natural or legal person's rights; there is a relevant public interest. Should none of these conditions be fulfilled, the Data Controller restricts the Processing and notifies such operation to the Data Subject. Afterwards, close to the expiration of the restriction period, the Data Controller notifies the Data Subject of the withdrawal of the restriction of the Processing. The Data Controller must promptly notify the request for restriction pursuant to Art. 18 to any other Recipient to whom Personal Data was communicated unless it involves a disproportionate effort.

- The right to rectification: The interested party has the right to obtain from the data controller the rectification of inaccurate personal data concerning him without unjustified delay. The Data Subject has the right to obtain rectification/correction of his/her inaccurate Personal Data under Art. 16 GDPR. The Data Controller, if it is possible and unless it involves a disproportionate effort, has to notify the rectification/integration to each Recipient to which it has communicated the Personal Data; Once the Data Processor rectifies or integrates Personal Data autonomously, it is necessary to notify the Data Subject promptly.

- Right to portability: The data subject has the right to receive in a structured format, commonly used and readable by automatic device, the personal data concerning him provided to a data controller, and also has the right to transmit such data to another controller without impediments. In case of automated Processing, the request for data portability pursuant to Art. 20 GDPR implies that the Data Controller has to provide the Data Subject with Personal Data in a structured, commonly used and machine-readable format. Data to be provided shall also include data generated as a result of the use of a service or a device. In case of expressed request from the Data Subject, and if technically feasible, the above data has to be transmitted directly to another Data Controller designated by the Data Subject.

- Right to object: The data subject to the right to the object, to the time of the processing of personal data and to what is based on the point (e) or (f) of Article 6 (1 GDPR), including profiling based on those provisions. The Data Subject may request to object to Process his/her Personal Data, including Profiling, in the following cases: the Processing is necessary to comply with a relevant public interest or in the exercise of official authority vested in the Data Controller; the Processing 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. In such cases, the request for objection must be motivated and may be refused by the Data Controller in the following cases: the Data Controller demonstrates compelling legitimate reasons for Processing that override Data Subject's interests, rights and freedoms; Processing is necessary for the establishment, exercise or defence of legal claims. Save the above cases, the Data Controller refrains from further Processing Personal Data.

- The request for objection determines the termination of the Processing definitively and permanently. Personal Data is deleted and anonymized pursuant to Art. 17.1 GDPR, unless one of the exceptions above applies.

- Automated individual decision-making, including profiling: the data subject is the subject of a decision based solely on automated processing, including profiling, which has legal effects on him or her. If the Data Subject is subject to decisions based solely on automated Processing, including Profiling, which produces legal effects concerning him or her or similarly significantly affects him or her, the Data Subject has the right to require the Data Controller to communicate meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject. Furthermore, the Data Controller has to guarantee to the Data Subject a human intervention and/or to express his or her point of view and as well as to contest the decision.

3.6.1 The Italian job

Another measure that could increase end-users engagement and trust in an IoT environment is that one regulated by the Italian labour law. The employee who will operate in an IoT context will be captured, observed, stored continuously by the machines in front of him/her (robot, or algorithm). The best measure that could be adopted in this context is borrowed from the Article 4 of the Italian workers' Statute which is a perfect example of engagement and trust. In 2015 the Italian legislator ruled and updated an engagement and trust mechanisms: the individual consent of each worker is not necessary to carry out the processing of personal data, but involving trade unions representatives and third parties, an element of trustability and engagement is created by regulating the use of new equipment in the workplace. This solution could be adopted also for the introduction of new technologies such as IoT services or devices.

In Italy before the reform of 2015, there was an absolute ban on the use of audio-visual equipment and other devices for the purpose of remote monitoring of employees' work. This prohibition was not applied only in cases in which the employer, for organizational, productive or job security reasons, intended to install new equipment from which remote control of the employees' working activity could derive. In this case, it was necessary the prior agreement with the trade union representatives or, failing that, the authorization of the local branches of the Ministry of Labour territorially competent.

Now, there is no longer an explicit prohibition of remote control of work performance. The employer (audio-visual systems and remote-control instruments) continue, as in the past, to be used by the entrepreneur exclusively for organizational and production needs, work safety and protection of company assets. In order to consider their installation and use legitimate, it is necessary a trade union agreement regarding the methods of use of such equipment (an agreement, depending on the size of the company, with the trade unions comparatively more representative at national level). If such an agreement is missing, the employer must obtain the prior authorization of the Territorial Labour Office or the Ministry of Labour (he/she will address one or the other according to the size of the company).

Therefore, before installing and using these systems within the company, the employer must have reached an agreement with the trade union representatives or, at least have received the ministerial authorization: in fact, both bodies carry out a verification task of the lawfulness and correctness of the use of these tools to protect all employees working in the company. This procedure prescribed by the Italian labour law could be used as a measure to develop end-users engagement and to increase their trust in the IoT environments.

On the other hand, the Italian labour law, legitimizes the exercise of a remote control (so called “direct control”) carried out on the instruments used by the employee to perform his/her duties and on the instruments for detecting accesses and attendances (so called “badge readers”). In this case, in fact, there is no obligation for the employer to reach a trade union agreement or obtain ministerial authorization: the control is free and can be carried out even without an organizational or production requirement. In the absence of any “filter” function attributed to the trade union representatives or to the supervision of the Ministry of Labour by the Territorial Labour Office, it is the single employee who shall verify if the control is exercised legitimately by the employer and possibly go to a trade union or a lawyer to protect his/her rights. This second approach without a trade union agreement or a ministerial authorization, could be riskier and would grant less end-users’ engagement and trust in the IoT environments.

What is essential to know is that, according to the Italian labour law, the employer can use the information collected through the exercise of the power of control for all purposes related to the employment relationship. This can only happen if the following two conditions are met:

1. employees shall be adequately informed about the ways in which the tools supplied must be used and the methods through which control will be exercised;
2. data protection law shall always be respected.

Failure to comply with even one of the two conditions indicated makes the use of information illegitimate for the purpose, for example, of a disciplinary procedure and, therefore, even of a dismissal. Compliance with these two conditions shall be granted also in the development of IoT environment within the workplace.

3.6.2 Privacy by Design

The most important measure in the IoT field is to properly address the data protection by design and by default principle according to Article 25 of the GDPR:

"*1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

3. An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article."

Before the GDPR, Directive 95/46/EC already made reference to the protection of Personal Data by design (i.e. the principle of "data protection by design") in its Art. 17, regarding «technical and organizational measures to protect personal data». Directive 2000/58/EC makes a similar reference in its Art. 14(3): *«Where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data [...]»*. Despite these provisions' usefulness in promoting the principle of data protection by design, they were never applied effectively in a sufficient manner to ensure the actual integration of data protection "by design".

Art. 25 GDPR, on the other hand, explicitly mentions the principles of "data protection by design and by default". This provision, read in conjunction with Recital 78 GDPR, determines that producers of products, services and applications based on the processing of Personal Data or which process Personal Data to fulfil their task, should be encouraged to take this principle into account when developing, designing, selecting and using these products, services and applications, so as to comply with the GDPR.

Recital 78 GDPR combines the development and design of products and services with the principle of accountability of the Data Controller or Data Processor who use those technologies. Thus, compliance with the principle of data protection by design should be considered a criterion for assessment of the Data Controller or Data Processor's liability.

The value in having introduced the principle of data protection by design set forth in Art. 25 (together with the principle of "data protection by default") lies in the fact that Supervisory Authorities will take this principle into account when deciding on whether to apply administrative fines (and on the amount of those fines). A failure to comply with these principles in punishable, under Art. 83(4)(a) GDPR, with fines of up to 10.000.000 EUR or, in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, if higher.

In this legislative scenario the development and use of IoT devices in smart cities shall be done according to the privacy by design principle. The use of IoT devices is not new, but it makes more complex the data subject's control over his/her own personal data and becomes more difficult to identify the legal basis for the processing of personal data. *The presence of multiple devices, data sources and entities processing personal data has also an effect on the acquisition of the data subject's consent which in the context of smart cities, under EU law, may constitute a legal basis for personal data processing of IoT* *deployments. There is therefore a direct relationship between IoT architectures in smart cities and privacy protection and this is the reason why an approach of privacy by design should be encouraged*[53].

Considering that compliance with the principle of data protection by design is made mandatory by the GDPR, the following guidelines illustrate the application of this principle to the Processing activities, in the IoT field. As such, the major areas which must include the protection of Personal Data by design are, essentially, the following two: obligations related to security; obligations related to Data Subjects' rights and other legal principles.

From a technical perspective, it is necessary to integrate security measures directly into applications, services and products from the moment of their development and design. On this regard, "*as data controllers, cities will be required to implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR, and review and update those measures when necessary. In each case cities will be called to evaluate which measures will be appropriate. This will depend on the nature, scope, context and purpose of the processing and also the risks for rights and freedoms of individuals*[54].

In fact pursuant to Article 32 of the GDPR, products, services and applications should include, *ex ante*, technical and organisational measures which ensure a level of security adequate to the risk of the processing which will be carried out with those products, services and applications – this may include measures such as Pseudonymization and Encryption of Personal Data. These measures should also ensure the confidentiality, integrity, availability and resilience of Processing systems and services, through technical procedures capable "to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident" (Article 32 GDPR).

The measures adopted to comply with the said principle may be changed over time. Under Art. 32(d) GDPR, an internal process for "regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing" must be established. To this end, the Undertaking organizes regular IT, documental and organisational audits, in addition to periodically performing stress tests (e.g., penetration tests within the IT framework of the Undertaking) on the security measures implemented regarding the various IT Processing systems.

3.6.2.1 Cybersecurity measures

ETSI's standard on cybersecurity in IoT for consumers lists some key concepts of security in IoT[55]. From the abovementioned source is possible to extract several objectives and security measures to increase security in IoT and thus, trust and end-user engagement. In the table below the cybersecurity measures.

The IoT Devices requires at least one administrative user, that is a user having the ability to operate with elevated privileges inside the IoT Devices (e.g. definition of other users, reset of their passwords).
The IoT Devices requires the passing of an authentication procedure (e.g. login) before being able to allow the processing of any personal data. This authentication procedure verifies the username and a password of at least

[53] Robert Lewis-Lettington (UN-HABITAT), Pasquale Annicchino (Archimede Solutions), Nathalie Feingold (NPBA), Antonio Kung (TRIALOG SA) and Xiaomi An (RUC) under the chairmanship of Gyu Myoung Lee (Korea, Rep.of); *"Framework for security, privacy, risk and governance in data processing and management"* (Technical Report D4.1); 19 July 2019.

[54] *Ibid ut Supra*.

[55] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

of 8 characters in length and containing alphanumeric, special and uppercase characters.
The IoT Devices requires strong authentication (multi-factor authentication, e.g. possession or biometrics). For IoT Devices that have stateless systems in general, the IoT Devices generates a token to associate to the session. The token associated with the session of the web IoT Devices or stateless systems is sufficiently long (64 or more alphanumeric characters) and impossible to guess. The token associated with the session of the IoT Devices or stateless systems has an expiration time.
The IoT Devices stores the password within its database in encrypted form.
The IoT Devices uses a hashing algorithm suitable for password encryption.
The IoT Devices implements automated password selection restrictions (e.g. a minimum number of characters is set, ignores common or user-referenced passwords). When the user ID is associated to an email address, the IoT Devices requires such email address to be verified. Email addresses associated with a user ID are periodically verified to ensure that the email is still valid and in use.
The IoT Devices limits or throttles the availability of logins in the event of an abnormal number of unsuccessful access attempts occurring within a short time frame.
The IoT Devices allows each of its administrative users to assign different permission levels to different users.
The IoT Devices prevents any non-administrative user from changing the permission levels assigned to other users.
The IoT Devices protects the data it allows to be processed through pseudonymisation techniques.
The IoT Devices protects the data that it allows to be processed through transparent encryption techniques. Data processed through the IoT Devices are appropriately classified (e.g. common, particular, judicial, subdivisions in personalized under systems).
The IoT Devices transmits network traffic in a protected from via state-of-the-art security protocols (e.g. TLS1.2, valid certificates, HSTS). Data processed with the help of the IoT Devices is backed up at least daily. Data processed with the help of the IoT Devices can be restored quickly.
The IoT Devices is currently supported (e.g. through the release of security updates and patches).
The IoT Devices is constantly kept up to date. The IoT Devices is periodically subjected to sessions of vulnerability assessment and penetration testing to assert its robustness to cyber-attacks.
The IoT Devices generates access logs.
The IoT Devices generates logs of critical actions (e.g. creation or removal of content or users).
The IoT Devices generates logs of the performed processes.
The logs are complete, unalterable, are stored for at least six months and the integrity of the logs can be verified. If the IoT Devices is connected with smartphones and requires permissions on the device, it provides policies that describe the purposes of the processing enabled by each permission. If the IoT Devices is connected with smartphones, it never uses the Device ID as a key to identify a record. If the IoT Devices is for smartphones, it uses certified pinning techniques to avoid MITM attacks.
The IoT Devices code does not contain confidential credential components (e.g. passwords, tokens, keys…). The IoT code is developed in accordance with the guidelines for secure code (e.g. CERT, OWASP...).

Table 1: cybersecurity measures for an IoT product

3.6.2.2 Privacy Measures

In the table below several privacy measures, in accordance with the GDPR principles, have been addressed to adequately design the IoT product, to fulfil the obligation under art. 25 GDPR

The IoT Devices is accompanied by a specification of the type of data of which it allows the processing (common, particular, judicial).
The IoT Devices is accompanied by a specification of the data flows from/to the outside.
The IoT Devices allows to define and modify the retention times for the various types of data that it stores.

The IoT Devices makes it possible to record the source of the data it stores (e.g. data supplied directly by the person concerned, data extracted from databases…)
The IoT Devices stores only the data necessary for its operation (e.g. it does not store unnecessary data).
The IoT Devices performs periodic automated checks to verify the accuracy of the data entered by the user (e.g. by comparison with golden records or other authoritative sources).
If the process of verifying the accuracy of the data entered by the user identifies incorrect or suspicious data, the IoT Devices sends a direct communication to the competent function or reports it to an administrator (to allow the competent function to be informed).
The IoT Devices retains the date of the last update of each record.
The IoT Devices allows an administrator to “mark” data as restricted (for example, providing flags in the database that identify the associated field as restricted).
The IoT Devices prevents the processing of a restricted data field (the restricted data field must not be read, modified, deleted, transmitted, displayed, etc. until it is unlocked by the platform administrator. No other user or IoT Devices should be able to do this).
If the conditions for the restriction are no longer met and the data of a data subject are therefore unlocked, the IoT Devices will directly notify the data subject.
The IoT Devices allows the aggregation in a comprehensible way of all the data that it retains in relation to an interested party, allowing the party the ability to modify and visualize it.
The IoT Devices allows to record aggregated data in one or more common format files (.jpg, .png, .pdf, .docx, .doc, .xlsx, .xls, etc.).
The IoT Devices allows the import of aggregated data relating to a data subject in an interoperable format (e.g. XML, CSV e JSON).
The IoT Devices allows to export the aggregated data related to a data subject in an interoperable format (e.g. XML, CSV e JSON), flanking them with useful metadata in order to identify them correctly.
If the IoT Devices collects data on minors, it requires the consent of the parental guardians to be entered.
If the IoT Devices collects data on minors, the consent of the parental guardians is pre-set as denied.
The IoT Devices allows to modify the consent lent by underage users once they have reached the age of majority.
If the IoT Devices generates scores relating to a data subject (e.g. third party data resulting from automatic processing) and the data subject has not given his or her consent to automated processing, the IoT Devices makes it possible to demonstrate that the decision having legal effects on the data subject comes from an operator and not from an automated process.
The IoT Devices works in accordance with the consent given by the data subjects (e.g. it informs the operators about the consent given and does not make certain types of data available for certain processing operations if their consent has not been given).
The IoT Devices keeps a record of the consent lent or denied, each with its own timestamp.
The IoT Devices shall keep a record of the requests by the data subjects to exercise their rights.
The IoT Devices does not feed databases and/or does not transfer personal data to servers not allocated within the European Union in the absence of assessment of adequacy of the country in which the data are transferred and explicit consent requested and provided by the data subject/IoT Devices user.
If the IoT Devices is public, it provides views dedicated to the disclosures and privacy policies to allow the data subject to review them at any time.

Table 2: privacy measures for an IoT product

Table describing how KPIs concerning all the above-mentioned measures are measured:

Measure	KPI	Measurement	Range
Feedback	**Suggestions sent**	Quantity of IoT product improvement interactions	1-100
Feedback	**Implementations inserted on users' recommendation**	Number of features inserted	1-10
Feedback	**Functionality and reliability**	Ability to perform a specific task	1-100
Feedback	**Helpfulness**	Ability to provide adequate, effective, and responsive advice necessary to complete a task	1-100
Feedback	**Ease of use**	How accessible the system is to the users	1-100
Labeling interface approach	**Perceived usefulness**	Degree that a user believes that the system usage would enrich their performance and lifestyle	1-100
Labeling interface approach	**RFID and label usage**	Amount of interactions	1 - 100
Crowd Privacy	**End-users comments**	Amount of comments received	1-100
Human law by default	**Request of rights' exercises**	Number of requests	1 - 100
Metaphor of food and drug comparison	**Privacy policy read**	Number of users who have read the privacy policy	1-100
Metaphor of food and drug comparison	**Consents given**	Number of users who have given consent	1-100
Choices and Consent	**Control panel usage**	Amount of interactions with the panel	1 - 100

Table 3: KPIs

4 CONCLUSIONS

In conclusion, what emerges from the research carried out, which, as can be seen from point 1.3 “Methodology”, was based mainly on the major European projects related to NGIoT as well as on literature, is that the measures necessary to increase the confidence of end users in the usage of IoT devices are intrinsic elements of the concept of privacy by design. The analysis and breakdown of the measures listed under point 3 “End-User Engagement Measures” clearly reveals a minimum common denominator, namely the principles set out in Article 5 of the GDPR[56], and in particular the principles of lawfulness, correctness and transparency, limitation of purpose, data minimization, accuracy, storage limitation, integrity, confidentiality and accountability. Therefore, in order to increase the end-user's confidence in the usage of IoT devices, it is essential that the protection of personal data becomes an intrinsic component of the structure-architecture of the device itself; only through this approach, technically implemented with the measures referred to in point 3.6.2.2 “Privacy Measures”, it will be possible to develop technologies that are inherently privacy-preserving and can offer the basis for empowering the end-user (and more in general, the end-target) to understand and be informed of (and, where appropriate, control over) the use of their data.

[56] *Article 5: Principles relating to processing of personal data*

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

5 REFERENCES

Ardito C., Buono P., Desolda G., Matera M. (2017). From Smart Objects to Smart Experiences: An End-User Development Approach in International Journal of Human-Computer Studies, December 17, 2017;

De Boer, P.S., van Deursen, A.J.A., van Rompay, T.J.L. (2018), Accepting the Internet-of-Things in our homes: The role of user skills, Telematics and Informatics in https://doi.org/10.1016/j.tele;

El-Haddadeha R., Osmania M., Thakkerc D., Weerakkodyb V., Kaur Kapoord K. Examining citizens' perceived value of internet of things technologies in facilitating public sector services engagement in Government Information Quarterly (2018);

Fadda E., Perboli G., Tadei R. Customized multi-period stochastic assignment problem for social engagement and opportunistic IoT in Computers and Operations Research 93 (2018);

Habibipour, A., Padyab, A., Bergvall-Kåreborn, B. and Ståhlbröst, A. (2017). Exploring Factors Influencing Participant Drop-out Behavior in a Living Lab Environment. 8th Scandinavian Conference on Information Systems, SCIS 2017, Halden, Norway, August 6-9, 2017, Cham, 2017;

Habibipour, A., Georges, A., Ståhlbröst, A., Schuurman, D. and Bergvall-Kåreborn, B. (2018). A Taxonomy of Factors Influencing Drop-out Behaviour in Living Lab Field Tests. Technology Innovation Management Review, Vol. 8, No., pp.5-21;

Hsu, C. L., & Lin, J. C. C. (2016), An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives in Computers in Human Behavior, 62, 516–527;

Law, E. L.-C., van Schaik, P. and Roto, V. (2014). Attitudes Towards User Experience (Ux) Measurement. International Journal of Human-Computer Studies, Vol. 72, No. 6, pp.526-541;

Norman, D. A. (1990), The design of everyday things. New York: Doubleday.

Papaioannou, Thanasis & Dimitriou, Nikos & Vasilakis, Kostas & Schoofs, Anthony & Nikiforakis, Manolis & Pursche, Fabian & Deliyski, Nikolay & Taha, Amr & Kotsopoulos, Dimosthenis & Bardaki, Cleopatra & Kotsilits, Sarantis & Garbi, Anastasia. (2018), An IoT-Based Gamified Approach for Reducing Occupants' Energy Wastage in Public Buildings. Sensors;

Shin D. A User-based Model for the Quality of Experience of the Internet of Things in INFMAN, 3 February 2017.

Santucci, G. (2011), *"The Internet of Things: A Window to Our Future"*, la http://www.theinternetofthings.eu /content/g%C3%A9rald-santucci-internet-things-window-our-future.

Ashish Ghosh, Debasrita Chakraborty, Anwesha Law; *"Artificial Intelligence in Internet of Things"*; IET Research Journals.

Luca Bolognini; *"Se gli algoritmi vanno al governo"*; Left page 58, 11 October 2019.

N. Gershenfeld, *"When Things Start to Think: Integrating Digital Technology into the Fabric of our lives"*. Henry Holt and Company, 2014.

Daniela Popescul, Mircea Georgescu**;** **"***Internet of Things – Some Ethical Issues*"; Article December 2013.

Yildirima, H.; Ali-Eldina, A.; *"A model for predicting user intention to use wearable IoT devices at the workplace"*. J. King Saud Univ. Comput. Inf. Sci. 2018, in press.

Falcone, R.; Sapienza, A.; *"On the Users' Acceptance of IoT Systems: A Theoretical Approach"*. Information 2018, *9*, 53.

Mayer, R.; Davis, J.; Schoorman, F.; *"An integrative model of organizational trust"*. Acad. Manag. Rev. 1995, *20*, 709-734.

Belanche, D.; Casaló, L.V.; Flavián, C.; *"Integrating trust and personal values into the technology acceptance model: The case of e-government services adoption"*. Cuad. Econ. Dir. Empres. 2012, *15*, 192–204.

McKnight, D.; Carter, M.; Thatcher, J.; Clay, P.; *"Trust in a specific technology: An investigation of its components and measures"*. ACM Trans. Manag. Inf. Syst. 2011, *2*, 12.

Areej AlHogail. *"Improving IoT Technology Adoption through Improving Consumer Trust"*. Article. 7 July 2018.

Lai, I.K.W.; Tong, V.W.L.; Lai, D.C.F.; *"Trust factors influencing the adoption of internet-based interorganizational systems"*. Electron. Commer. Res. Appl. 2011, *10*, 85–93.

Bart, Y.; Shankar, V.; Sultan, F.; Urban, G.L.; *"Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study"*. J. Mark. 2005, *69*, 133–152.

Tam, S.; Thatcherb, J.B.; Craigc, K.; *"How and why trust matters in post-adoptive usage: The mediating roles of internal and external self-efficacy"*. J. Strateg. Inf. Syst. 2017, *27*, 170–190.

Daubert, J.; Wiesmaier, A.; Kikiras, P.; *"A view on privacy & trust in IoT"*. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2665–2670.

Lai, I.K.W.; Tong, V.W.L.; Lai, D.C.F.; *"Trust factors influencing the adoption of internet-based interorganizational systems"*. Electron. Commer. Res. Appl. 2011, *10*, 85–93.

Hochleitner, C.; Graf, C.; Unger, D.; Tscheligi, M.; *"Making Devices Trustworthy: Security and Trust Feedback in the Internet of Things"*. In Proceedings of the Pervasive'12 Fourth International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), Newcastle, UK, 18–22 June 2012.

Koien, G.M.; *"Reflections on trust in devices: An informal survey of human trust in an Internet-of-Things context"*. *Wirel. Pers. Commun.* 2011, *61*, 495–510.

C. Ardito , P. Buono , G. Desolda , M. Matera (2017): *From Smart Objects to Smart Experiences: an End-User Development Approach* in International Journal of Human-Computer Studies.

De Boer, P.S., van Deursen, A.J.A., van Rompay, T.J.L. (2018): *Accepting the Internet-of-Things in our homes: The role of user skills, Telematics and Informatics* in https://doi.org/10.1016/j.tele. 2018.12.004

Ardito C., Buono P., Desolda G., Matera M. (2017). *From Smart Objects to Smart Experiences: An End-User Development Approach* in International Journal of Human-Computer Studies, December 17, 2017;

Papaioannou, Thanasis & Dimitriou, Nikos & Vasilakis, Kostas & Schoofs, Anthony & Nikiforakis, Manolis & Pursche, Fabian & Deliyski, Nikolay & Taha, Amr & Kotsopoulos, Dimosthenis & Bardaki, Cleopatra & Kotsilits, Sarantis & Garbi, Anastasia. (2018), *An IoT-Based Gamified Approach for Reducing Occupants' Energy Wastage* in *Public Buildings. Sensors*. 18. 537. 10.3390/s18020537.

Norman, D. A. (1990), *"The design of everyday things"*. New York: Doubleday.

Gao, L.; Bai, X.; *"A unified perspective on the factors influencing consumer acceptance of internet of things technology"*. Asia Pac. J. Mark. Logist. 2014, *26*, 211–231.

Abu, F.; Jabar, J.; Yunus, A.R.; *"Modified of UTAUT Theory in Adoption of Technology for Malaysia Small Medium Enterprises (SMEs) in Food Industry"*. Aust. J. Basic Appl. Sci. 2015, *9*, 104–109.

Choi, B.; Lee, I.; *"Trust in open versus closed social media: The relative influence of user- and marketer-generated content in social network services on customer trust"*. *Telemat. Inform.* 2017, *34*, 550–559. Lin, Z.; Dong, L. Clarifying Trust in Social Internet of Things. *IEEE Trans. Knowl. Data Eng.* 2018, *30*, 234–248.

Lin, Z.; Dong, L.; *"Clarifying Trust in Social Internet of Things"*. IEEE Trans. Knowl. Data Eng. 2018, *30*, 234–248.

Kowshalya, A.M.; Valarmathi, M.L. *"Trust management for reliable decision making among social objects in the Social Internet of Things"*. *IET Netw.* 2017, *6*, 75–80.

Blomqvist, K.; Hurmelinna-Laukkanen, P.; Nummela, N.; Saarenketo, S.; *"The role of trust and contracts in the internationalization of technology-intensive Born Globals"*. *J. Eng. Technol. Manag.* **2008**, *25*, 123–135.

Hsu, C. L., & Lin, J. C. C. (2016), *An empirical examination of consumer adoption of internet of things services: Network externalities and concern for information privacy perspectives* in *Computers in Human Behavior*, *62*, 516–527.

Robert Lewis-Lettington (UN-HABITAT), Pasquale Annicchino (Archimede Solutions), Nathalie Feingold (NPBA), Antonio Kung (TRIALOG SA) and Xiaomi An (RUC) under the chairmanship of Gyu Myoung Lee (Korea, Rep.of); *"Framework for security, privacy, risk and governance in data processing and management"* (Technical Report D4.1); 19 July 2019.

Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in: eurlex.europa.eu

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), in: http://eur-lex.europa.eu/legalcontent/IT/TXT/?uri=CELEX%3A32016R0679.

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, Adopted on 22 June 2010, in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

Article 29 Data Protection Working Party, Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017, in https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030