DOI: 10.1561/9781680836837.ch9

Chapter 9

Data Protection Compliance Requirements for the Internet of Things

By Luca Bolognini, Sébastien Ziegler, Pasquale Annicchino, Francesco Capparelli and Alice Audino

9.1 Introduction

With the progressive implementation of new technologies, more and more interconnected, we are surrounded by an increasingly synchronized, delocalized, and correlated environment, animated by a continuous flow of data generated by our choices and behaviors.

The disruptive advent of IoT technologies has profoundly changed the relationship between human beings and "things." It is difficult to make a distinction between online and offline dimensions, because most of the devices used in everyday life are connected and interact with the surrounding reality in a continuous exchange of information between material and virtual environments.[1]

It can be observed, therefore, that a new challenge has opened up for the protection of the rights and freedoms of Data Subjects and stakeholders in the new technological environment that has changed since the broader adoption of IoT.[2]

1. L. Floridi, *The Ethics of information*, Oxford University Press, 2015.

2. EUROPEAN COMMISSION, The Internet of Things Opportunities and Challenges, 2015. Document available at the following link: https://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf. The document defines IoT as "a global, distributed network

Existing digital and electronic devices have implied the need to strongly focus on personal data protection safeguards. The more the technologies have evolved, the more it has been necessary to establish a legislative framework to protect a "personal" and "private" space. These needs have been at the heart of debates in the Parliament and in the Commission of the European Union, bringing to the adoption of a legal instrument to be valid in all the European Union Member States, the Regulation n. 679/2016, the General Data Protection Regulation (GDPR). This Regulation was introduced into an existing International and European normative framework protecting fundamental rights and freedoms, which includes, among others, the Universal Declaration of Human Rights and the Charter of Fundamental Rights of the European Union.

Even if the Regulation does not explicitly refer to IoT Devices or the IoT System, the principles emerging from the GDPR—first of all, the ones of purpose limitation, storage limitation, lawfulness, transparency, fairness, integrity and confidentiality, and data protection-by design/by default—are adaptable to any technological development and deployment, IoT technologies included.

The present document proposes some brief considerations, without claiming to be exhaustive, on the issues of Data Subject awareness and accountability in the IoT field, with a focus on technology developers in the light of the GDPR and cybersecurity international best practices.

9.2 IoT and General Data Protection Regulation: Awareness as a Key Safeguarding Factor

9.2.1 Awareness and Data Protection

Data subjects' awareness is a prerequisite in order to enhance their confidence in new technologies, as well as to ensure that the individuals can always choose, freely and autonomously, whether allowing or not the collection and further processing of their data in an IoT environment.

Data protection, privacy, and security are the main key factors to increase trust. The challenge is, then, to develop technologies that are, by design, inherently privacy-preserving and transparent, in order to empower end users (and more in general, the end target of individuals) to understand and to be informed of (and, where appropriate, to control over) the use of their personal data. The interaction

(or networks) of physical objects that are capable of sensing or acting on their environment, and able to communicate with each other, other machines or computers". See also ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 2017. The document refers to the concept introduced by *Kevin Ashton*: "a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context."

between individuals and IoT Devices or the IoT System has been studied in order to better understand practical and actual dynamics of relationship between individuals and objects; as a result, it emerged the need to ensure a human-centric IoT environment, as the EU project GHOST[3] demonstrates.

A new IoT project may involve users and Data Subjects as actors or as factors. Most of the IoT solutions are considering the possible *factorization* of people: people as an entity which interacts with other sensors. *Factorization* could bring to limit Data Subjects' rights and freedom, with the risk of *de facto* downgrading their role to the same level of "objects." A way to empower individuals, without *factorizing* them, is to educate and train them on the IoT ecosystem features, risks, and safeguards, so as to promote the creation and perception of an environment that they can consider "safe" and "manageable."

A better education would also imply an increasing awareness of Data Subjects' skills and rights, related to the adoption of IoT tools, as well as a major attention by developers and producers to IT security and other technological features, in order to protect, by default, individuals from possible violations and to enable them to receive adequate information and to exercise their rights.

Moreover, the way in which personal information is collected and managed, in an IoT scenario, may affect not only end users' rights but also the rights of third subjects which are observed and recorded by the devices.

The processing of personal data carried out through IoT systems is certainly included in the material scope of application of the GDPR, which sets forth some conditions for the lawfulness of the processing as listed in Article 6:

"[…] *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;*

3. GHOST Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control: "D3.9: Trials use case specification and report" (1st release).

(*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.*"

There are six available legal bases for the processing. No single basis is necessarily more suitable than the others, due to the fact that the most appropriate basis will depend on the purpose of the data processing and on the possible relationship between Controllers and Data Subjects.

Among the various bases stated in the aforementioned Art. 6 of the GDPR, the one that necessarily implies a good degree of awareness and information of the Data Subjects is described in letter (a): consent.

In particular, according to Article 7 of the GDPR:

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.*"

Article 4 paragraph 1 n. 11 GDPR rules that "*consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject.*" However, as provided by the WP29 in the opinion adopted in 2014 on the "*Recent Developments on the Internet of Things*":[4] "*In many cases, the user may not be aware*

4. ARTICLE 29 DATA PROTECTION WORKING PARTY This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013. Website: http://ec.europa.eu/justice/data-protection/index_en.htm14/ENWP223 Opinion 8/2014 on the Recent Developments on the Internet of Things Adopted on 16 September 2014.

of the data processing carried out by specific objects. Such lack of information constitutes a significant barrier to demonstrating valid consent under EU law, as the Data Subject must be informed" pursuant to Article 13 and Article 14 of the GDPR.

In all cases of different legal bases of personal data processing, other than Data Subjects' consent (think about the data processing in the legitimate interest of the Controller or in the public interest), the challenge would be that of adequately informing Data Subjects and to make them as aware as possible of the activities carried out and of the related risks to their rights and freedoms.

9.2.2 Awareness of Data Subject as an Instrument for Opt-in and Free Choices

The processing of information by IoT technologies can involve natural persons. In this sense, Articles 13 and 14 of the GDPR provide the obligation to inform Data Subjects about the personal data lifecycle, while Recital 58 of the GDPR underlines that the principle of transparency requires that "*any information addressed to the public or to the Data Subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used*".

In addition, Recital 60 underlines that the obligation to inform comes from the application of the principles of fairness and transparency of processing. Precisely, the latter principle is also the logical basis for a conscious Data Subject's choice.

The "*Guidelines on transparency under Regulation 2016/679*"[5] issued by WP29 clarified that this principle applies in three main cases (par. 7):

(1) In the information provided to the Data Subjects;
(2) The way in which Data Controllers communicate with Data Subjects the information;
(3) The way in which Data Controllers allow the exercise of rights by the Data Subjects.

Therefore, the *ratio legis* of this principle is to allow Data Subjects to have control over their data and thus to make a choice about it.

In particular, paragraph 10 of the document states that: "*the Data Subject should be able to determine in advance what the scope and consequences of the processing entails*

5. ARTICLE 29 DATA PROTECTION WORKING PARTY This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013. Website: http://ec.europa.eu/newsroom/Article29/news.cfm?itemtype=1358&tpaid=6936 17/EN WP260 rev.01 Article 29 Working Party Guidelines on transparency under Regulation 2016/679 Adopted on 29 November 2017. As last Revised and Adopted on 11 April 2018.

and that they should not be taken by surprise at a later point about the ways in which their personal data has been used."

The Data Controller would therefore be obliged to:

- Provide individuals with information including the purposes for the processing of their personal data, the retention periods for personal data processed, and with whom personal data will be shared;
- Provide privacy information to individuals at the time the IoT Data Controller collects their personal data;
- Obtain personal data from other sources; the IoT Data Controller shall provide individuals with privacy information within a reasonable period and no later than one month; there are 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 information to them;
- Provide information to people in a concise, transparent, intelligible, easily accessible manner, and it shall use clear and plain language;
- Regularly review, and where necessary, update its privacy information. The IoT Data Controller shall provide the individuals with any information related to the new uses of their personal data, before the IoT Data Controller starts the processing.

However, in this context, where information is exchanged between Data Subjects and "Things" and between "Things" and "Things," it is in many cases very difficult to make Data Subjects aware of the life cycle of their data. For this reason, it is not always that easy and effective to provide an *ex ante* information notice to Data Subjects, in an IoT scenario, while it could result more effective and efficient to provide relevant information, in a simplified way, after data collection or, anyway, in a non-traditional modality.

A way of considering the matter would be, then, the possibility of publishing a concise, schematic information, similar to labels on the packaging of medicines or food, to be affixed in proximity of the inter-connected arrangement. This signal or label […] like the one used for snacks […] would specify which data are being and/or have been processed and by whom and would show to the Data Subjects how they could exercise their data rights.

The solution here suggested could be particularly advantageous because the information on the label/signal will also help non-expert people to understand which categories of information are involved in the purposes and in the logic that rules the processing, by clarifying the structure (data, sources, criteria) of the processing itself, so as to better implement the principles of lawfulness, fairness, and transparency (pursuant to Article 5 paragraph 1, letter (a) of the GDPR). IoT

could be equipped with well-visible interfaces, displaying such labels. For example, an image sensor and an IoT object could be equipped with a screen, to increase awareness on the presence of the sensor and increase user confidence in using objects that gather data.

Another option, connected with the information just indicated above, could result in the obligation to alert individuals about the presence of IoT sensors in a given environment. Specifically, following the provision set forth by Article 12 paragraph 8 of the GPDR, where it is expected that "*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*," Solutions which provide for the use of icons or figurative representations of other kind, easily understandable by the interested parties, may be considered.

This "alert signals" solution could be even more helpful – in all cases in which Data Subjects are not "end users," but simply "non-users," since there are no interfaces and no features for interactivity between things and persons – in order to prevent negative effects caused by IoT deployments.

Finally, a third option consists in using a dedicated smart phone application to inform the data subjects about the presence of IoT in their vicinity. Such approach has been researched and implemented in the European Large Scale Pilot on IoT for smart cities, the H2020 Synchronicity European research project.[6] A dedicated application, titled Privacy App (www.privacyapp.info), has been developed.

The Privacy Application enables users to discover nearby IoT Devices or the IoT System on an interactive map. For each IoT device, the app provides the available information related to the purpose of the data processing, the controllers and processors involved, as well as information on retention period and cross-border transfer. The user can also add new IoT Devices or the IoT System on the map and request for more information. More importantly, the user can directly contact the Data Protection Officer of the data controller of the IoT device.

9.2.3 IoT Features Enabling Opting-out and Exercise of Data Subjects' Rights

Awareness is a prerequisite of Data Subjects' freedom of choice, as underlined above; a robust level of awareness may enable individuals to prevent their data collection (*ex ante*). However, awareness can empower individuals to control over their data after processing and to exercise their rights in an opt-out approach (*ex post*).

6. The Privacy App was developed by Mandat International in the context of Synchronicity, the H2020 European Large Scale Pilot on the Internet of Things for Smart Cities: https://synchronicity-iot.eu/

Hereinafter, we summarize the provisions of Articles 15 to 22 of the GDPR, which contain the rights of the Data Subject (all terms in capital letters refer to the definitions given in the GDPR):

- Right of access: according to the right of access pursuant to Article 15 of the GDPR, the Data Subject has the right to obtain the confirmation as to whether Personal Data concerning him or her is being Processed. The right of access can imply, if requested by the Data Subject, the right to receive a copy of the personal data being processed.
- Right to erasure is defined as a right to ask for the deletion of personal data. According to the right to erasure under Article 17 of the GDPR, the Data Subject has the right to request for and obtain the erasure of Personal Data or the anonymization of such data, 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 Article 17 paragraph 1 of the GDPR, the Data Controller, having considered the technologies at its disposal and the costs, has to promptly notify the erasure, unless it involves a disproportionate effort, to all Recipients to whom Personal Data have been transferred. The Data Controller communicates to the Data Subject the erasure once completed.
- The right to restrict processing requires that personal data are "marked," without being processed for purposes other than mere storage, pending further determinations; therefore, it is advisable for the Data Controllers to include in their information systems (electronic or otherwise) suitable measures for this purpose. The request for restriction of the Processing pursuant to Article 18 of the 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 given; the Processing is necessary for the establishment, exercise, or defense of legal claims; the Processing is necessary to protect any other natural or legal person's rights; a substantial public interest applies. The Data Controller must promptly notify the request for restriction pursuant to Article 18 of the GDPR to any other Recipient to whom Personal Data were 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/her without unjustified delay. The Data Subject has the right to obtain rectification/correction of his/her inaccurate Personal Data under Article 16 of the 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, it is necessary to notify the Data Subject promptly.

- Right to portability: the Data Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

  (a) the processing is based on consent or on a contract; and
  (b) the processing is carried out by automated means.

- Right to object: the Data Subject shall have the right to object, at the time of the processing of personal data, to what is based on the point (e) or (f) of Article 6 paragraph 1 of the GDPR, including Profiling based on those provisions. The Data Subject may request to object to Process his/her Personal Data, including Profiling (except for) 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 defense 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. Personal Data are deleted and anonymized pursuant to Article 17 paragraph 1 of the GDPR, unless one of the exceptions above applies.
- Automated individual decision-making, including Profiling: each individual has the right not to be subject to decisions based solely on automated Processing, including Profiling, which produce legal effects concerning him or her or similarly significantly affect him or her. 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. In case an Automated individual decision-making is carried out, the Controller has the obligation to provide the Data Subject with meaningful information about the logic involved, as well as the relevance and the envisaged consequences of such Processing for him/her.

9.3 The Principles of Accountability, Data Protection by Design and by Default as Indirect Requirements for IoT Technology Producers and Controllers

9.3.1 Controllers vs Producers in IoT: Direct and Indirect GDPR Requirements

Articles 5 and 24 of the GDPR set one of the fundamental and innovative principles of the Regulation, the essence of the legislator's change of approach with the GDPR, establishing the principle of accountability of the Data Controller. It is the Controller's task + the action to "*implement appropriate technical and organisational measures to ensure, and be able to show, that the processing is carried out in accordance with the Regulation.*" Furthermore, Article 24 paragraph 2 of the GDPR provides that "*these measures shall be reviewed and updated as necessary,*" which is intended to reaffirm the central role of the Controller and its responsibility in adopting technical and organizational measures.

The principle of accountability is key, in order to better understand the nature of the activities that the Data Controller must carry out from the earliest stages of design of new processes, products or services.

Whoever undertakes to process, must ensure that the data must be "*accountable.*" This means, on the one hand, that Controllers will be responsible for the identification and choice of the legal bases, the procedures, the modalities of implementation, the security measures and the operations, which involve the processing of the data, but also, on the other hand, that Controllers must be able to demonstrate that their actions comply with the provisions of the GDPR, especially with regard to the "*effectiveness of the measures,*" keeping records and documentation of such assessments and choices.

Measures to be put in place by Controllers and Processors shall be "*adequate*," but Article 24 of the GDPR does not specify what measures can be adequate: it is up to Controllers the assessment of possible fitting technical and security measures, on a case-by-case basis.

The "*one-size-fits-all checklist*" approach is therefore replaced by a by-design approach, permeated with contextualization and risk-specific analysis.

The European legislator's new approach is typical of international standards on the management of information systems. The determinations deriving from the knowledge of the internal dynamics of an organization, and its processes/activities, are potentially more effective than the choices made for the mere purpose of complying with a norm.[7]

7. The approach of the International Standard Organization already in 2013, with the ISO/IEC 27001 Standard, focuses on risk assessment as a source from which to derive the implementation of technical and organizational security measures.

The application of the principle of accountability, therefore, should bring IoT designers, producers, and deployers to weigh and objectively justify their choices, in matter of personal data processing, while at the same time, allowing them to devote the necessary resources and effort to achieve the highest level of security and safety for individuals, considering their dynamics and processes, and not to only refer to a list of abstract requirements.

With regard to effectiveness, WP29 in op. 3/10[8] highlights that "*there are various methods available to Data Controllers to assess the effectiveness (or ineffectiveness) of the measures. For the processing of larger, more complex and higher risk data, internal and external audits are common verification methods. The way audits are conducted can also vary, from full audits to negative audits (which can take different forms)*," so to evaluate the effectiveness of the measures. Depending on the type of data processing activities carried out, it will be needed to use both internal and external means of evaluation. Article 24 paragraph 1 of the GDPR, additionally, expressly provides that the measures adopted shall be periodically "*reviewed and updated where necessary.*" This is particularly relevant for IoT, in light of the great variety of possible deployment scenarios of IoT solutions and of the risks to rights and freedoms of individual that may derive from them.

This approach is, furthermore, compatible with the ISO/IEC 27001 standard, which obliges those who provide certification of conformity to the standard to carry out repeated risk assessments over time, planned in such a way as to discover and adequately mitigate previously ignored risks and to further mitigate the risks already treated.

The principle of accountability is directly linked to the principles set out in Article 25 of the GDPR, the "data protection by default principle" and the "data protection by design principle."

The latter opens to a pragmatic view: 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 organizational measures, such as pseudonymization, which are designed to implement data-protection principles, or data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects.

8. ARTICLE 29 DATA PROTECTION WORKING PARTY 17/EN WP260 Guidelines on transparency under Regulation 2016/679.

The "data protection by default principle" finds substance in all those measures, technical and organizational, functional to ensure that only personal data necessary for the purposes pursued 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.

In the light of the above considerations, in conclusion, it should be noted that the GDPR, in its Articles 5-24-25 as analyzed above, does not provide for a merely formal fulfillment of data protection obligations; quite the opposite, the Regulation calls for a real assessment, concrete and substantial, by those who are responsible for the processing of personal data. In this regard, the recent EDPB guidelines on the topic have specified that (par. 8): "The term *measures* can be understood in a broad sense as any method or means that a Controller may employ in the processing. These measures must be appropriate, meaning that they must be suited to achieve the intended purpose, i.e. they must be fit to implement the data protection principles effectively by reducing the risks of infringing the rights and freedoms of Data Subjects. The requirement to *appropriateness* is thus closely related to the requirement of *effectiveness*".[9]

The GDPR introduces, of course, a cultural change that will inevitably impact also IoT developers and manufacturers, even if it has to be taken into account that the "accountability principle," the "data protection by default principle" and the "data protection by design principle" refer to actual Data Controllers, while, according to Recital 78 of the GDPR, "*producers of the products, services and applications* ***should be encouraged*** [but not obliged, authors' note] *to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that Controllers and processors are able to fulfil their data protection obligations.*"

Notwithstanding this, the GDPR combines the mild "encouragement" of producers with the principle of accountability to be respected by Data Controllers, thus elevating data protection by design from an option to a strict parameter of compliance to be assessed by Controllers in the selection of products and/or services providers. And the mentioned Recital 78 of the GDPR provides that "*the principles of data protection by design and by default should also be taken into consideration in the context of public tenders.*"

9. EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. In particular, the concept of effectiveness is extremely connected with the accountability principle of Article 5 paragraph 2 of the GDPR. Indeed, the Data Controllers must be able to demonstrate that they have implemented dedicated measures to protect these principles, and that they have integrated specific safeguards that are necessary to secure the rights and freedoms of Data Subjects.

In conclusion, the compliance with the GDPR principles can be considered as an "indirect requirement" for IoT technology producers, even if they do not directly process personal data on behalf of Controllers.

To this end, new certification mechanisms, guidelines and standards will be welcome, in order to direct the application of such principles in the field of IoT, both from the side of producers and of Data Controllers and Processors.

9.3.2 Cybersecurity Measures for IoT: Recommendations

IoT Devices or the IoT System can simplify our lives and their adoption is constantly increasing; unfortunately, such devices and applications are not always safe from the cybersecurity point of view.

The growing number of devices which are connected to the network also raises the amount of possible vulnerabilities and access points for potential IT attacks. The fact of being networked objects makes IoT Devices or the IoT System vulnerable to cyber threats.

In this sense, in 2019 the European Telecommunications Standards Institutes (hereinafter referred to as "ETSI") issued a document "to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products."[10] In particular, the document proposed solutions consistent with the GDPR approach.

From the abovementioned source, it is possible to extract several recommendations of security measures to enhance security in IoT systems and, thus, Data Subjects' engagement and trust. In the Table 9.1 below, we can list the cybersecurity measures envisaged by the ETSI Document.

Table 9.1. Cybersecurity measures for an IoT device and an IoT system (Source: ETSI).

The IoT Devices or the IoT System requires at least one administrative user, that is, a user having the ability to operate with elevated privileges inside the IoT Devices or the IoT System (e.g., definition of other users, reset of their passwords).
The IoT Devices or the IoT System 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 of 8 characters in length and containing alphanumeric, special, and uppercase characters.

(*Continued*)

10. ETSI, Cyber Security for Consumer Internet of Things, 2019. Document available at the following link: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Table 9.1. Cybersecurity measures for an IoT device and an IoT system (Source: ETSI) (continued).

The IoT Devices or the IoT System requires strong authentication e.g., (multi-factor authentication, possession or biometrics). For IoT Devices or the IoT System that have stateless systems in general, the IoT Devices or the IoT System generates a token to associate to the session. The token associated with the session of the web IoT Devices or the IoT System 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 the IoT System or stateless systems has an expiration time.
The IoT Devices or the IoT System stores the password within its database in encrypted form.
The IoT Devices or the IoT System uses a hashing algorithm suitable for password encryption.
The IoT Devices or the IoT System implements automated password selection restrictions (e.g., a minimum number of characters is set, and it ignores common or user-referenced passwords). When the user ID is associated to an email address, the IoT Devices or the IoT System 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 or the IoT System 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 or the IoT System allows each of its administrative users to assign different permission levels to different users.
The IoT Devices or the IoT System prevents any non-administrative user from changing the permission levels assigned to other users.
The IoT Devices or the IoT System protects the data it allows to be processed through pseudonymization techniques.
The IoT Devices or the IoT System protects the data that it allows to be processed through transparent encryption techniques. Data processed through the IoT Devices or the IoT System are appropriately classified (e.g., common, particular, judicial, subdivisions in personalized under systems).
The IoT Devices or the IoT System 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 or the IoT System are backed up at least daily. Data processed with the help of the IoT Devices or the IoT System can be restored quickly.
The IoT Devices or the IoT System is currently supported (e.g., through the release of security updates and patches).

(*Continued*)

Table 9.1. Cybersecurity measures for an IoT device and an IoT system (Source: ETSI) (continued).

The IoT Devices or the IoT System is constantly kept up to date. The IoT Devices or the IoT System is periodically subjected to sessions of vulnerability assessment and penetration testing to assert its robustness to cyberattacks.
The IoT Devices or the IoT System generates access logs.
The IoT Devices or the IoT System generates logs of critical actions (e.g., creation or removal of content or users).
The IoT Devices or the IoT System generates logs of the performed processes.
The logs are complete, unalterable, and stored for at least six months; the integrity of the logs can be verified. If the IoT Devices or the IoT System 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 or the IoT System is connected with smartphones, it never uses the Device ID as a key to identify a record. If the IoT Devices or the IoT System is for smartphones, it uses certified pinning techniques to avoid MITM attacks.
The IoT Devices or the IoT System 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 …).

9.3.3 Data Protection by Design Measures for IoT: Recommendations

In accordance with the GDPR principles, in the Table 9.2 below, several privacy measures have been identified, in order to adequately design IoT product and systems, fulfilling the obligation under Art. 25 GDPR.

Table 9.2. Privacy measures for an IoT device and an IoT system.

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

(*Continued*)

Table 9.2. Privacy measures for an IoT device and an IoT system (continued).

The IoT Devices or the IoT System stores only the data necessary for its operation (e.g., it does not store unnecessary data).
If the process of verifying the accuracy of the data entered by the user identifies incorrect or suspicious data, the IoT Devices or the IoT System sends an alert to the competent function or reports it to an administrator (to allow the competent function to be informed).
The IoT Devices or the IoT System retains the date of the last update of each record.
The IoT Devices or the IoT System allows an administrator to "mark" data as restricted (e.g., providing flags in the database that identify the associated field as restricted).
Where applicable, the IoT Devices or the IoT System prevents the processing of restricted data fields (the restricted data field must not be read, modified, deleted, transmitted, displayed, etc. until it is unlocked by the platform administrator. Neither another user nor IoT Devices or the IoT System should be able to do this).
The IoT Devices or the IoT System shall enable the Data Controllers to aggregate in a comprehensible way 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 or the IoT System shall enable the Data Controller to record aggregated data in one or more common format files (.csv, .xlsx, .xls, .txt, etc.).
The IoT Devices or the IoT System shall enable the Data Controller to transfer aggregated data relating to a Data Subject in an interoperable format (e.g., XML, CSV, JSON).
The IoT Devices or the IoT System allows to export the aggregated data related to a Data Subject in an interoperable format (e.g., XML, CSV, JSON), flanking them with useful metadata in order to identify them correctly.
If the IoT Devices or the IoT System collects data on minors, it requires the consent of the parental guardians to be entered and given to the Data Controller.
Where applicable, if the IoT Devices or the IoT System collects data on minors, the consent of the parental guardians shall require an express opt in consent.
If the IoT Devices or the IoT System generates scores relating to a Data Subject (e.g., third-party data resulting from automatic processing) and the Data Subject did not give his or her consent to automated processing, the IoT Devices or the IoT System makes it possible that the decision having legal effects on the Data Subject comes from an operator and not from an automated process.

(*Continued*)

Table 9.2. Privacy measures for an IoT device and an IoT system (continued).

Where applicable, the IoT Devices or the IoT System 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 was not been given).
Where applicable, the IoT Devices or the IoT System keeps a record of the consent lent or denied, each with its own timestamp.
Where applicable, the IoT Devices or the IoT System shall keep a record of the requests by the Data Subjects to exercise their rights.
The IoT Devices or the IoT System 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 or the IoT System user.
If the IoT Devices or the IoT System is public, the Data Controller shall communicate and ease access to privacy policies in order to allow the Data Subject to review them at any time.

Conclusion and Acknowledgments

Considering the pervasive nature of the Internet of Things, the risk for the rights and freedoms of data subjects will be higher and higher. Adopting data protection by design approach will be key for the adoption and compliance of IoT-related services and applications.

The adoption of the GDPR has raised the level of awareness on data protection regulations. However, ensuring compliance will require to bring together experts in technology and in law in order to build a bridge between these two worlds.

The present chapter has been redacted in the context of the European Research Project NGIoT in the context of the Horizon 2020 European Research Program.