PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation.

INTERNET OF THINGS

Brief summary

Iñigo de Miguel Beriain (UPV/EHU)

This document is an abbreviated version of the part of the Panelfit Guidelines related to IoT. For better information, it is advisable to consult the full version of our Guidelines, written by Iñigo de Miguel Beriain (UPV/EHU), in cooperation with Aliuska Duardo (UPV/EHU), Álvaro Anaya Rojas, Gerardo Pérez Laguna & María Carmen González Tovar (Everis Ciberseguridad)

This document provides Internet of Things (IoT) developers and innovators with advice about the actions they should take to comply with the legal requirements related to the development of IoT tools in terms of data protection. It can only be understood in the context of the whole tool (the Guidelines). There are several concepts that are not explored in this document, because they are addressed in other sections; we have referred to these wherever needed (references are highlighted in yellow). All sections are available on an interactive website

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information.

DISCLAIMER

The information provided in this document does not constitute legal advice; instead, all information, content, and materials provided are for general informational purposes only. Furthermore, one must always keep in mind that the information provided in our Guidelines does not constitute legal advice; instead, all information, content, and materials provided are for general informational purposes only. The Guidelines provide general advice around EU data protection law under the GDPR. Accordingly, the reader should be aware that the situation relevant in their specific processing context, as well as in their specific jurisdiction, may deviate from the guidance provided. Indeed, information in our Guidelines may not constitute the most up-to-date legal or other information. The legal situation in relation to data processing in the EU changes regularly. New laws and new interpretations of existing laws relevant to the topics covered by the Guidelines appear frequently and changes may not be reflected in the Guidelines.

In this regard, we would highlight, without any intention of being comprehensive, at the time of writing, the significance of the following draft EU laws to the topics covered in these Guidelines: the ePrivacy Regulation, the AI Act, the Data Governance Act, the Digital Services Act, the Digital Markets Act and the Data Act.

Where relevant at the time of writing, authors may have attempted to highlight provisions of draft laws in relation to the topics covered in these Guidelines. The reader should be aware that drafts may change and that such references may not remain valid over time. Equally, authors' choices to consider certain provisions from certain draft laws should not be taken as indicative of effort to be comprehensive in addressing all relevant provisions from all draft laws.

Readers of the Guidelines should contact their DPOs and DPAs to obtain advice with respect to any particular legal matter. No reader, user, or browser of the Guidelines should act or refrain from acting on the basis of information provided without first seeking legal advice from counsel in the relevant jurisdiction. Only DPOs and DPAs can provide assurances that the information contained herein – and your interpretation of it – is applicable or appropriate to your particular situation. Use of, and access to, the Guidelines do not create any relationship between the reader, user, or browser and the authors, reviewers, validators, or commentors, of the Guidelines.

The views expressed in, or through, our Guidelines are those of the individual authors writing in their individual capacities only – not those of EU Commission, of course. All reference to reviews, validations, or provision of comments or suggestions, refer to the personal opinions of individuals acting in their personal capacities – and do not refer to the opinions of the organisations these individuals represent or to acts of these individuals in their official capacities.

The Guidelines contain links to other third-party websites. Such links are only for the convenience of the reader, user or browser; the authors and the reviewers/validators do not recommend or endorse the contents of the third-party sites.

All liability with respect to actions taken or not taken based on the contents of the PANELFIT Guidelines are hereby expressly disclaimed.

1 Project Understanding: the crucial issues to be considered

1.1 Make sure that your project is compatible with the fundamental values of the EU

Before considering the use of data gathered from social networks for the project, the developer should have her/his primary objective clear in mind. **A clear idea of the concrete use of data gathered through social networks will help controllers determine in the early stages of development some important legal issues regarding processing**, such as compliance with the Developer Policy of the social network, possible need of international transfers of data, existence of joint-controllers or processors -which need to be carefully selected-, or the security and organizational measures to minimize risks.

1.2 Implement a training programme in ethical and legal issues for ICT developers and other relevant stakeholders

Implementing **basic training programmes** for researchers/innovators. If they are gathering data from a concrete social network, this training should include a careful analysis of its particular Developer Policy. An early involvement of DPOs from the participating institutions is highly advised.

1.3 Define the roles played by all agents involved in the processing

The concepts of controller, joint controller and processor play a crucial role in the application of the GDPR. In the case of utilization of social networks for data processing, it is equally important to properly distinguish the data controller from the data processor, since the responsibilities of each are different. **To dispel any possible doubt,** we must first turn to the list of definitions in the GDPR, interpreted in accordance with the EDPB Guidelines 7/2020 on the concepts of controller and processor in the GDPR and the EDPB Guidelines 8/2020 on the targeting of social media users [1] and the relevant case law of the CJEU[2].

In the most common scenarios, ICT researchers and innovators will play the role of a third party regarding social networks and data subjects. The network will provide them with data that belong to the data subjects. Once these data are already under the control of the researchers/innovators, they become controllers of those data and take the corresponding responsibilities.

[1] EDPB Guidelines (Guidelines 8/2020 on the targeting of social media users Version 2.0 Adopted on 13 April 2021, at: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf, p. 11).

[2] The judgments in Wirtschaftsakademie (C-210/16), Jehovah's Witnesses (C-25/17) and Fashion ID (C-40/17) are particularly relevant here.

1.4 Prepare the contracts with the social network and (in case) with the joint controllers, processors, etc. and document the

Gathering data from social networks often involves entering into some kind of agreement with their representatives. **Written agreements between all agents involved in the development of the tools should be reached and documented, whenever possible (see art. 28 of the GDPR).** These should include clear specifications about the responsibilities taken by all participants. Promoting a continuous interaction between all DPOs involved might be an excellent option. Ad-hoc supervisory bodies and tools can be adopted to ensure a smooth oversight of the participants' processing.

1.5 Promote end-users engagement

Since ICT involves the use of personal data from different types of data subjects, it is highly recommendable to hear the voices of the representatives of the collectives involved so as to ensure that the Data Protection by Design policies are in line with their interest, rights and freedoms. Organizing some **preliminary discussions** with those representatives ensures the implementation of a bottom-up framework that could be very helpful to this purpose.

Some essential tips regarding these preliminary stages include:

- Ensure that the use of data gathered by the IoT system does not promote scenarios that are incompatible with the EU fundamental values
- Conduct a proportionality assessment for the use of personal data gathered by the IoT system
- Ensure that the team members processing personal data have been\are adequately trained on the Developer Policy corresponding to the social network from which data will be extracted, and the key concepts on data protection issues
- Adequate assessment tools on data protection have been implemented from the very beginning of the project
- The roles played by your team members and their role in data processing have been adequately defined and you can provide evidence on this.
- The roles played by all different devices involved in the data processing by the IoT system are clear through the corresponding agreements and you can provide evidence on this.
- Ensure that you have gathered the relevant information on the terms of use of the social network from where you gather the data and abides by them
- Consult the representatives of the key collectives involved in the data processing on the impact of the use of the IoT system and implement their recommendations.

2 Lawfulness: Choosing a legal basis

According to the GDPR, lawful processing requires for a legal basis. If processing includes the type of activities that are included in the ePrivacy Directive (and in the

future ePrivacy Regulation), the provisions made by this new tool will apply as soon as it will be adopted. An IoT should be able to distinguish between different individuals using the same system so that they cannot learn about each other's activities without a legal basis that justifies such processing (most probably consent). Trust between actors must be based on the authentication of each IoT tool prior to communication and data access. Prevention of unauthorized objects and users from accessing a system can enhance confidentiality, and thus increase user trust. **Defining the legal basis that applies to such processing is, therefore, key, to ensure the lawfulness of the processing.** At the present moment, there are several legal bases for data processing that might apply well to IoT. These are: consent, performance of a contract legitimate interest and, of course, public interest, when we are talking about scientific research and innovation.

The draft of the ePrivacy Regulation[3] considers consent as the main basis for lawful data processing in the context of electronic communications, a circumstance that applies, for instance, in the case of IoT devices connected to the web. However, where a controller seeks to process personal data that are in fact necessary for the performance of a contract, then consent is not the most recommendable lawful basis and processing should be based on Article 6(1) (b).

Legitimate interest, on the other hand, is the most flexible legal basis for processing, but one cannot assume it will always be the most appropriate. The ICO considered that it is likely to be most appropriate where controllers use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.[4] However, it might happen that the criteria used by EU Member States DPAs are quite different. Thus, you should better ask your DPO about this issue.

3 Human agency (automated decision making and profiling)

One of the issues inherent to IoT is that this technology **can hardly avoid promoting profiling and automated data processing.** This creates important issues in terms of data protection. As the Article 29 Working Party stated, "unlike other types of content, IoT pushed data may not be adequately reviewable by the data subject prior to publication, which undeniably generates a risk of lack of control and excessive self-exposure for the user. In addition, communication between objects can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how objects interact or to be able to define virtual boundaries by defining active or non-active zones for specific things, it will become extraordinarily difficult to control the generated flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function

3 https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

4 ICO: Legitimate interests, at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

creep. This issue of lack of control, which also concerns other technical developments like cloud computing or big data, is even more challenging when one thinks that these different emerging technologies can be used in +combination."[5] Indeed, we must keep in mind that IoT often needs linking datasets from different devices to obtain detailed insight about users' private lives, and to make assumptions and predictions of their behavior. These practices are not contrary to data protection, provided that they strictly comply with the applicable regulations. However, it is often hard to ensure that fulfilment.

Some important tips regarding automated decision making and profiling include: Ensure that:

- The controller users about the type of data that are collected and further processed by the IoT sensors, other types of data that they receive from external sources and how it will be processed and combined.
- The IoT systems can distinguish between different individuals using the same device so that they cannot learn about each other's activities without an appropriate legal basis.
- You work with standardization bodies and data platforms to support a common protocol to express preferences with regard to data collection and processing by data controllers especially when unobtrusive devices collect such data.
- You have enabled local controlling and processing entities (the so-called personal privacy proxies) allowing users to have a clear picture of data collected by their devices and facilitating local storage and processing without having to transmit the data to the device manufacturer.
- The IoT systems provide:
    - a panoramic overview of what personal data have been disclosed to what data controller and under which policies;
    - online access to the personal data and how they have been processed;
    - counter profiling capabilities helping the user to anticipate how their data match relevant group profiles, which may affect future opportunities or risks (this is not required by the law, but recommendable).
- The IoT systems provide granular choices when granting access to applications. The granularity does not only concern the category of collected data, but also the time and frequency at which data are captured. Similarly to the "do not disturb" feature on smartphones, IOT devices should offer a "do not collect" option to schedule or quickly disable sensors.
- Profiling and automated decision making only happens when a legal basis applies and adequate safeguards have been implemented. Mechanisms able to inform about it to all involved data subjects have been implemented.

5 Art 29 Data Protection Working Party (2014) Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

- You have performed a DPIA.
- You have consulted a DPO on the processing.
- You have ensured that all guarantees foreseen by Article 22 of the GDPR have been adequately implemented.
- You have ensured that all those intervening in profiling and automatic data processing have been adequately trained on data protection issues.
- You have documented all the information regarding this issue.

4 Fairness and Transparency

Fairness is an essential principle in the GDPR. Arguably, all of data protection and thus the GDPR is about fairness towards data subjects. The GDPR can be seen in spelling out what *fair* actually concretely means. In the case of ICT, it mainly relates to the need to avoid that no one is left out of the chance to benefit from the tools, that is, that all people are entitled to the same fundamental rights and opportunities to profit on the technological advances. Also, that there should be no discrimination on the basis of the fundamental aspects of our identity which are inalienable, such as gender, race, age, sexual orientation, national origin, religion, health and disability, etc. In other words, in terms of IoT, fairness is mainly related to the need to make the tools easy to use for those who are not especially skilled in digital technologies and to avoid that the system created discrimination by introducing unfair biases. To this purpose, organisational measures should be implemented to guarantee the accuracy and reliability of the gathered data, while still ultimately deferring to the right of users to withhold private information (e.g. confirming whether or not a record is accurate). Furthermore, performing an audit devoted to detecting biases in raw data or in the inferred or derived datasets is highly recommended.

The main focus of **transparency** is to inform **data subjects** up-front of the existence of the processing and its main characteristics.

Transparency, on the other hand, is key to help data subjects develop trust in IoT systems and devices. Indeed, the requirements of transparency are clearly related to the fairness principle, since the harder it is for the user to understand the IoT system, the greater the difference between different types of users becomes. Transparency shows the controller is acting with accountability. On the other hand, lack of overall transparency (and information rights specifically) is in breach of GDPR obligations and may amount to high fines for the controller. It is applicable to all elements relevant to an IoT system: the data, the system and the processes by which it is designed and operated, the interaction with other IoT systems, the use (or not) of AI tools, the performance of profiling or automatic decision making, etc. In addition, it amounts to the who: who is the controller, to whom the data are disclosed, who is the DPO (if there is one), etc.

In the case of IoT, controllers must keep in mind that transparency is hard to be ensured to data subjects, due to a number of factors that hinder such objective. First, one must consider that an IoT system usually interacts with some others, processing a lot of personal data. Indeed, "as the IoT relies on the principle of the extensive processing of data through these sensors that are designed to communicate unobtrusively and exchange data in a seamless way, it is closely linked to the notions of "pervasive" and "ubiquitous" computing."[6] Indeed, in the case of IoT, sensors are actually designed to be non-obtrusive, i.e. as invisible as possible. Consequently, in many cases, the data subject is not aware of data processing due to a lack of available information. In other cases, available information does not equal transparency and awareness for data subjects. In these cases, together with informative wording, transparency can mean using icons when data such as location is being collected, and switching off such icons when data is not being collected. Controllers must assess what transparency means in their specific development and device.

Furthermore, "once the data is remotely stored, it may be shared with other parties, sometimes without the individual concerned being aware of it. In these cases, the further transmission of their data is thus imposed on the user who cannot prevent it without disabling most of the functionalities of the device."[7] This can be enhanced by the ever-more-common data stored inside the device. In these, data do not leave the device, enhancing all transparency, data subjects control over their data, and, depending on the case, security.

Additionally, IoT systems often use AI tools. As extensively exposed in the corresponding section, these tools often suffer from diverse types of opacity, hindering an adequate fulfilment of transparency requirements

Some essential tips related to fairness are:

- Perform internal/external audits aimed at detecting biases in the datasets built and/or the conclusions of the analysis
- Perform audits aimed at detecting biases in the datasets built and/or the conclusions of the analysis

Some essential tips related to transparency are:

- Provides the data subjecs with complete information about the processing and their rights
- Ensure that the information is provided concisely, transparently, intelligibly, and in an easily accessible way. It is clear and redacted in plain language.

6 Art 29 Data Protection Working Party (2014) Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

7 Art 29 Data Protection Working Party (2014) Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

- If providing the information is rendered impossible, take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available.
- If a DPIA has been conducted, ensure that it has been published openly and is publicly available
- Since the personal data were not provided by the data subject, provide the data subjects with all the information listed in Article 14.1 GDPR;
- If the personal data is not provided by the data subjects, provide them with the information:
  - within a reasonable period after obtaining the personal data, but at the latest within one month;
  - if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject;
  - if a disclosure to someone else is envisaged, at the latest when the personal data are first disclosed
  - Document all the information regarding these issues

Last, but not least, do your best to avoid widening digital division. IoT is a complex technology that involves using many different IoT systems. Some processing is made automatically and lots of attention and skill is required to be aware of the implications of all the actions taken by the tools. Thus, it often happens that only a selective group will benefit from some concrete products based on IoT technologies, mostly people with higher education or incomes, strong social support, young people, etc. This may leave out of the technological adoption other groups such as older people, low income or low educational groups, disabled people, etc. These circumstances create an unfair scenario, which is particularly unacceptable if we talk about tools that may be used to provide citizens access to public services. In order to minimize this unfair digital discrimination, IoT developers should take some actions that might serve well to help everyone gain access to the tool, by implementing **additional functionalities or easy-to-use control interfaces that allow the management of technical and privacy settings.** For instance, designing clear terms of use and user-friendly IoT control systems should be an important objective. In general, **complexity should be avoided whenever possibl**e. If this is not possible, easy-to-understand instructions should be written or recorded and be accessible for the users in the most user-friendly thinkable way. "Utilizing IoT device affordances to create new interactions through delivery methods like videos, audio and feedback from gestures like hand-waving or blinking lights and sounds may redefine consent mechanisms and shift away from the dominance of form contract terms and conditions."[8]

5 Data governance: minimization, purpose limitation and

8 Urquhart, L., Sailaja, N. & McAuley, D. Realising the right to data portability for the domestic Internet of things. *Pers Ubiquit Comput* 22, 317–332 (2018).

storage limitation principles

The combination of these three principles creates a combined normative tool that must be strictly followed by IoT developers.

5.1 Minimization principle

The minimization principle states that personal data shall be **adequate**, **relevant and limited to what is necessary in relation to the purposes** for which they are processed. Unfortunately, this principle is sometimes in tension with the logic of the IoT technology. Sometimes, inferring data and profiling are necessary for the purposes of the system, but they multiply the amount of data involved in the processing. In addition, most IoT systems process many personal data between devices that are often under control of alternative processors and/or involve third parties. There are some ways through which pervasive scenarios might be avoided. If the purpose of the processing can be obtained with no need or identifiable information, data must be made anonymous as soon as possible. In principle, IoT systems **should promote the use of anonymized data, especially if those data are shared with other devices**. However, researchers/innovators should keep in mind that anonymization might be hard to reach. Thus, **controllers should not presume that their anonymization processes will serve well to preserve data subjects' privacy. Indeed, they should perform DPIAs and risk assessments to ensure such a belief.** An alternative to anonymization as such is the use of **aggregated data**. **When the purpose of the processing can be achieved using aggregated data, this is recommendable**

Last but not least, IoT developers "should enable local controlling and processing entities (the so-called personal privacy proxies) allowing users to have a clear picture of data collected by their devices and facilitating local storage and processing without having to transmit the data to the device manufacturer."[9]

5.2 Purpose limitation

Purpose limitation is a key concept in terms of data protection. The main problem is that IoT systems often collect vast amounts of data for **vague or broadly defined purposes.** As Watcher stated, "sensor fusion or the linkage of existing but previously unconnected datasets, can offer new opportunities for data analytics that were not envisioned when the data were collected. Invasive and unpredictable inferential profiling is enabled by identification services that link devices and the data they collect." [10] As a consequence, controllers might produce inferred data about the data subject that are not related to the purposes for which the data was originally collected and to which the data subject never consented. Furthermore, data subjects might not even be aware of such processing.

9 Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

10 Wachter, Sandra (2018). The GDPR and the Internet of Things: a three-step transparency model. Law, Innovation and Technology, 1–29. doi:10.1080/17579961.2018.1527479 .

Worse enough, it might happen that data are processed by third parties for other purposes to which the data subject never gave consent.

In order to avoid such scenario, **controllers should implement tools able to ensure that processing only takes place if a legal basis applies.** The utility of stored data for the intended purpose of a particular product or service will need to be periodically reassessed to avoid unlawful data processing.

5.3 Storage limitation

The principle of storage limitation obliges data controllers not to store personal data for 'longer than is necessary for the purposes for which the personal data are processed' and to introduce pseudonymization and anonymization measures that reduce/eliminate the identifiability of data subjects as soon as possible for such purposes.

In order to avoid unlawful storage, "necessity test must be carried out by each and every stakeholder in the provision of a specific service on the IoT, as the purposes of their respective processing can in fact be different. For instance, personal data communicated by users when they subscribe to a specific service on the IoT should be deleted as soon as the users put an end to their subscription. Similarly, information deleted by users in their account should not be retained. When a user does not use the service or application for a defined period, the user profile should be set as inactive. After another period of time the data should be deleted. The user should be notified before these steps are taken, with whatever means the relevant stakeholder has at its disposal".[11]

Some essential tips regarding these principles are:

- Assess what data is necessary and proportionate, and anonymised or pseudonymised any other data.
- Ensure that if special categories of data are used, a necessity analysis has been carried out.
- Use the data only for the purposes you collected them, unless a legal basis allows their lawful processing.
- Make sure that no one but the data subject should access the raw data, unless a legal basis legitimizes such processing (and provided that it is necessary for the purposes searched).
- Make sure that raw material leaving the device remains the minimal strictly needed.
- Do not store personal data for 'longer than is necessary for the purposes for which the personal data are processed and made data subjects aware of the lifespan.
- Check and documented the utility of the stored data for the intended purpose of the research.
- Make sure that all personal data communicated by users when they subscribe to a specific service on the IoT are deleted as soon as the users puts an end to their subscription.

11 Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

- Ensure that information deleted by users in their account is not retained by the IoT system.
- Make sure that if a user data subject does not use the IoT system for a defined period of time, their profile is set as inactive and after another period of time the data is deleted.
- Guarantee that the user of the IoT system is notified before these steps are taken.
- Store data in a way that hinders personal data processing as much as possible and document the reasons that made you select such policy.
- Document all the information regarding these issues.

6 Data subjects rights

Since we have already analysed the right to information and the right not to be Subject to Automated Decision-Making has been extensively addressed in the "Human Agency" section of this document, we will focus now on the remaining rights.

In general, most of these rights are hard to implement in the case of IoT, due to the pure nature of the technology, which is based in the high-speed of data provided by different systems and devices. Continued aggregation and profiling techniques, together with the continued creation of inferred data contribute to hinder rights such as access, portability o erasure. Furthermore, in the IoT framework it is quite common to find different controllers and processors processing aggregated datasets that are stored through cloud computing led by a supervisor, who takes the role of joint controllers or processors.

The contracts that rule such interactions are complex and multi-layered. Consequently, the distribution of roles and responsibilities becomes difficult in practice. Even though in theory contracts should clarify all these issues, "in reality, the processors are the ones who draft standard contractual terms and processing instructions because they process data on behalf of many controllers and do not have separate processing instructions for each controller. This makes it difficult for the controllers to comply with the contractual requirements and the accountability principle under GDPR, as they are not fully aware of all of the processors and subprocessors involved. Furthermore, the complex multi-layered contractual relationships between IoT stakeholders make it more difficult to claim the responsibility for a damage caused to data subjects by IoT devices or analytical algorithms."[12]In addition, some parties may draft contracts positioning themselves in a different role than what really applies to them
Different tools have been proposed to face these issues and the 'personal information management system' ('PIMS') approach has been promoted by the European Data Protection Supervisor.[13] The use of blockchain techniques to design GDPR-based smart contracts that are privacy aware to improve the accountability of IoT devices, which are data controllers or processors of user data might be an adequate alternative, since they

12 El-Gazzar, R., & Stendal, K. (2020). Examining How GDPR Challenges Emerging Technologies. *Journal of Information Policy, 10*, 237-275. doi:10.5325/jinfopoli.10.2020.0237.

13 European Data Protection Supervisor (2016) Opinion on personal information management systems towards more user empowerment in managing and processing personal data. Brussels. At: https://edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_en.pdf

do not need general supervisor or ―data controller. However, blockchain might provoke disadvantages in terms of data subjects' rights and freedoms, since their being node owners would make them "controllers" and consequently they would have obligations and liabilities according to the GDPR.[14]

Even though there are no definitive technical solutions to these complex issues, IoT developers should do their best to ensure that the systems are able to respect data subjects' rights and freedoms. Domains of IT design like privacy-enhancing technologies (PETS), privacy engineering, usable privacy and human data interaction all have methodologies and frameworks to offer.[15]

Some general tips regarding data subject rights include:

- Introduce the necessary procedures to ensure that the data subject rights are adequately satisfied, no matter if they are the end-users or third parties.
- Introduce the necessary procedures to ensure that the data subject rights are satisfied in time (maximum one month after request, extendable by two additional months with regard to the complexity of the task and the number of requests). If you need this additional time, inform the data subject about.
- Introduce efficient tools to ensure that data subjects are able to exercise their rights in a practical manner, for instance by introducing data interoperability standards.
- Provide the data subjects with remote access to their personal data.
- Ensure that data subjects have easy access to the procedures to exercise their data rights and the contact details of the DPO or person responsible to handle data requests
- Document all the information regarding these issues.

6.1 Right of access

Article 15 provides that data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and where that is the case, access to the personal data together with some additional information which is usually provided in the privacy policy. In the case of IoT, this might be done through a web portal or an app, since these systems usually send data to the device manufacturer, who often keeps them in specific systems. On the one hand, it allows IoT to provide online services that leverage the device capabilities, but, on the other hand, it may also prevent users from freely choosing the service that interacts with their device.

14 Nicola Fabiano, Internet of Things and the Legal Issues related to the Data Protection Law, Athens Journal of Law - Volume 3, Issue 3, 2018, Pages 201-214 https://doi.org/10.30958/ajl.3-3-2 doi=10.30958/ajl.3-3-2 according to the new European General Data Protection Regulation By

15 Urquhart, L., Sailaja, N. & McAuley, D. Realising the right to data portability for the domestic Internet of things. *Pers Ubiquit Comput* 22, 317–332 (2018).

Furthermore, and as the Article 29 Working Party stated, "end-users are rarely in a position to have access to the raw data that are registered by IoT devices. Clearly, they hold an immediate interest in the interpreted data than in the raw data that may not make sense to them. Yet, access to such data can prove useful for the end-users to understand what the device manufacturer can infer from it about them". [16]

It is considered that the right to access cover both raw data and observed data about the user. However, under current developments, it does not seem to cover inferred data. This can cause detriment to users, as there is little options for them to gather insights of the most sensible data the system is processing about them.

6.2 Right to rectification

As laid down in Article 16 GDPR, data subjects hold the right to have their personal data rectified. This is particularly relevant in the case of IoT, since any inaccuracy in the collected data might have dramatic consequences in terms of profiling. Indeed, "IoT developers face a significant challenge to curate and update their datasets to meet this requirement. Verification of user identity is critical to ensure accuracy, particularly when multiple people can potentially use the same device."[17] The main problem here is that data are often stored in different servers and the IoT developers are not always aware of the existence of some concrete backup copies. This should be carefully examined in the contracts between controllers and joint-controllers or processors.

Controllers are obliged to communicate the rectified data to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort. Controllers could hardly argue that the sharing information and storage system is too complex to ensure rectification to avoid this requirement.

6.3 Right to erasure

Data subjects have a right to ask controllers the deletion of their personal data under article 17 GDPR. However, the use of cloud computing, the existence of diverse servers and repositories, the possibility that the data are processed by different processors and controllers makes it hard to ensure that all backup copies and the personal data –and not only their encryption keys- are deleted. To avoid such results, IoT developers should monitor procedures carefully.

Finally, controllers shall keep in mind that this right does not cover processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' or when it will 'adversely affect the rights and freedoms of others'. If deleting some data might cause severe

16 Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

17 Wachter, Sandra, (2018) The GDPR and the Internet of Things: a three-step transparency model, Law, Innovation and Technology, 10:2, 266-294, DOI: 10.1080/17579961.2018.1527479.

damage to the rights and freedoms of others, erasure should not be allowed. This involves the need to balance different interests involved.

6.4 Right to restrict the processing

According to article 18 of the GDPR, The data subject shall have the right to obtain from the controller restriction of processing where one of the circumstances described in this article applies". Since different joint controllers, processors or subprocessors might be involved in processing in the case of IoT, it might be good to keep in mind that this right shall be exercised through any of them, who should inform the rest about the requirement and proceed accordingly.

6.5 Right to object

In the case this right is exercised, the controller must assess whether there exists a "compelling" reason to continue the processing. This must be interpreted in a strict and narrow way, and it cannot be the same interests and reasons that justified the processing in the first place. This is because, this time, the controller must re-assess the processing in light of the personal reasons argued by the data subject. If such compelling ground cannot be found and strongly argued, the processing activity must stop. In these cases, a false assessment of such compelling reasons to continue the processing could be seen, for instance, by the number of times the controller does not concede the exercise of the right and keeps with the processing. When the processing consists on direct marketing, the data subject can exercise a right to object in a direct way, and the controller must stop the processing with no option to argue a compelling reason.

6.6 Right to data portability

According to Article 20 GDPR, data subjects have a right to portability. Data subjects "should be provided with tools enabling them to easily export their data in a structured and commonly-used format. Therefore, data interoperability is a key technical component to fully deploy this right and device manufacturers should provide a user-friendly interface for users who want to obtain data that they still store."[18]

Some practical tips to ensure that these rights are adequately exercised include: Make sure that

- You have introduced the necessary procedures to ensure that the data subject rights are adequately satisfied, no matter if they are the end-users or third parties.

18 Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088

- You have introduced the necessary procedures to ensure that the data subject rights are satisfied in time (maximum one month after request).
- You have introduced efficient tools to ensure that data subjects are able to exercise their rights in a practical manner, for instance by introducing data interoperability standards.
- Data subjects are in a position to have access to all their personal data, including the raw data that are registered by IoT devices.
- You have implemented tools to locally read, edit and modify the data before they are transferred to any data controller. Furthermore, personal data processed by a device is stored in a format allowing data portability.
- You have introduced tools able to communicate rectified data to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort.
- You have introduced tools able to ensure that all data are efficiently deleted at the data subjects' request if there are no lawful reasons to oppose to that request.
- You have introduced user-friendly interface for users who want to obtain the raw and observed personal data that they still store. These tools enable data subjects to easily export their data in a structured and commonly-used format.

7 Accountability and oversight[19]

Accountability is an essential requirement given the risks inherent in IoT, such as the "opaque nature of distributed data flows; inadequate consent mechanisms, and lack of interfaces enabling end-user control over the behaviors of Internet-enabled devices"[20].

Another particularly complex issue is the fact that the IoT enables many tools and technologies that have their own data protection risks. Particularly, AI, machine learning, big data, cloud computing, "with personal data collected by IoT devices typically being distributed to the cloud for processing and analytics"[21].

There are standards being developed by CEN and CENELEC

See the list here:
https://standards.cen.eu/dyn/www/f?p=204:32:0::::FSP_ORG_ID,FSP_LANG_ID:2307

[19] This part of these Short Guidelines was originally written by Bud Brugger, see:
https://guidelines.panelfit.eu/the-gdpr/main-principles/accountability/
20 Urquhartet L. *et* al, Demonstrably doing accountability in the Internet of Things, International Journal of Law and Information Technology, 2019, 27, 1–27
21 Ibid.

986,25&cs=1F4A71C19873519CC81C4B2C031CF3CF5

Accountability consists of two requirements for controllers:

- **Compliance** with the principles of the GDPR;
- **Demonstration of compliance.**

Compliance is achieved by implementing ***technical and organizational measures*** that are adequate compared to the risks to the rights and freedoms of data subjects, correspond to the state of the art of technology, and are cost-effective.
Demonstration of compliance is predominantly achieved by **documentation**. Every implemented measure, including data-protection-relevant considerations and decisions, should be documented. The GDPR requires two formal documents as part of demonstrating compliance towards supervisory authorities: the **register of processing** and, where the risks are likely to be high, a **data protection impact assessment.** Certification can support the demonstration of compliance.

7.1 Data Protection Officer

In most cases, IoT systems involve operations that, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale. Therefore, the appointment of a DPO is compulsory according to the conditions settled by Article 37(1) apply. Even if this is not the case, **it is always recommendable to proceed to do so, at least in terms of transparency.**

7.2 Data protection Impact Assessment

A DPIA is not always compulsory in the case of IoT development (see "In what cases must I carry out a DPIA" subsection within "Data Protection Impact Assessment", "Main Tools and Actions", Part II of these Guidelines). It depends on whether the risks associated with the processing are high or not, according to Article 35(3) of the GDPR. However, it is highly recommended as it supports accountability. For instance, DPIA is compulsory if processing involves a systematic monitoring of a publicly accessible area on a large scale, or it is intended at evaluating or scoring vulnerable populations. In order to see if a DPIA is necessary:

- Determine the jurisdictions where data-processing activities will take place.
- Check if those jurisdictions have enacted lists indicating the processing that requires a mandatory DPIA and checked if the intended data processing is covered by those provisions.
- If you are unsure of the necessity of carrying out a DPIA, you must consult with the DPO or, in lieu of, the legal department of the controller.
- If necessary, file a prior consultation with the appropriate supervisory authority.

There is no standard way to perform a DPIA. However, Article 35.7 GDPR calls for specific elements that shall always be present. These are:

- a systematic description of the envisage processing operations;
- the purposes of the processing operations;
- an assessment of the necessity of the processing operations in relation to the purposes;
- an assessment of the proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects;
- the technical and organizational measures envisaged to address the risks.

7.3 Design your Privacy Policy and prepare the documentation of processing

The Privacy Policy is the public document that explains how a research project processes personal data and how it applies data protection principles, according to articles 12-14 of the GDPR. All data subjects must have access to this Privacy Policy. It should be documented. A non-official, but recommendable template can be found here: https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf

Controllers must always keep in mind that, in the case of data gathered from social networks, they might end up mixing different datasets or create inferred or derived data. The traceability of the processing, the information about possible re-use of data, and the use of data pertaining to different datasets in either the same or different stages of the life cycle must be ensured by the records. Whoever processes personal data (including both controllers and processors) needs to document their activities primarily for the use of qualified/relevant Supervisory Authorities. This must be done through records that are maintained centrally by the organization across all its processing activities, and additional documentation that pertains to an individual data processing activity.

The main decisions made by the data controller "have to be documented in order to comply with the requirement of data protection by design" (of Article 25 of the GDPR). Indeed, an organization who is processing personal data (including both, controllers and processors) needs to documents its activities primarily for consumption by the competent Data Protection Supervisory Authorities (DPA). This includes the ***records of processing*** that is maintained centrally by the organization across all its processing activities and **additional documentation** that pertains to an individual data processing activity.

Records of processing can be kept in written or electronic form[1]. So expect to either fill in an organization-specific form or enter your information into some (data protection) management system.

To provide an initial idea, the minimal content of the records of processing for controllers includes the following items[2]:

- The **name** and **contact** details **of the controller**, the controller's **representative** and the **data protection officer**;
- the **purposes** of the processing;
- a description of the **categories of data subjects** and of the **categories of personal data**;
- the **categories of recipients** to whom the personal data have been or will be disclosed;
- where applicable, **transfers of personal data to a third country** together with the documentation of suitable safeguards;
- where possible, the envisaged **time limits for erasure of the different categories of data**
- where possible, a general description of the **technical and organizational *security* measures**

Keep in mind that:

- Your organization may use a different set of items since on one hand, it already is in possession of some of this information (such as the first bullet), and on the other hand, it may require additional information (such as the contact of the person responsible for the single processing activity at hand).
- It is possible that the legally required record keeping is combined with the management needs of the organization, such as an internal inventory of computing and computing resources.
- Your organization may also use multiple systems, e.g. depending on whether it is acting as a controller or as a processor; or distinguishing between permanent data processing activities (such as communication systems and accounting) and temporary ones (such as those linked to temporary projects or assignments). The creation and maintenance of records across multiple systems is not prohibited under the GDPR.

Some essential tips are:

- Data protection (like security) is a process, not a final state. Continuously document that process rather than only the final characteristics of the processing activity.
- When applying data protection by design[4], the processing activity can be seen as the results of a series of many considerations and decisions. It is these considerations and decisions that should be documented.
- Deciding on a structure and format to systematically collect this information at the point of time when you conceive your processing activity.
- Where the documentation itself contains personal information (see below), make sure to protect is sufficiently and limit its further use to the purpose of demonstrating compliance with the GDPR.

The first stages of the project development are the perfect moment to set up a systematic way of collecting the necessary documentation, since it will be the time when the organization conceives and plans the processing activity[22].

Last but not least, controllers must keep in mind that ethics committees will probably play a key role in personal data processing. However, this might change considerably between sectors and countries. Controllers shall ask their DPO about this topic.

Finally, controllers shall not forget that there might be ethical implications beyond legal compliance. Consultation with an expert in the ethics of social networks is always recommended.

8 Integrity and confidentiality

This principle involves three main issues: integrity, confidentiality and availability. Availability and integrity are somehow linked in the case of IoT, since only data that are adequately preserved can be made available to the data subject. Confidentiality, instead, is a more complex issue that deserves complex measures due to the pure nature of the processes involved and the risks inherent to such processes.

8.1 Availability and integrity

IoT usually involves gathering an impressive amount of data. The processing or analysis of these data usually takes place in very remote locations in the cloud and, to be able to reach them, it is necessary to use shared networks, public networks, etc. Some of these data are raw data and some of them are aggregated data, which are created through the interaction by different IoT systems.

Under such circumstances, it is usually hard to make all data available for the data subjects. Indeed, this would not be a good idea in the case of raw data. Most of IoT complex systems, incorporating several tools, only need aggregated data and have no need of the raw data collected by IoT devices. Therefore, controllers usually delete raw data as soon as they have extracted the data required for their data processing. However, devices should always include a functionality allowing data subjects control this process and control the process of deletion of all their personal data. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).[23] These data, thus, would not be available for the data subjects or an intruder. This is not particularly important, since they could hardly benefit from getting access to them. Instead, storing all data would be against the minimization, purpose limitation and storage limitation principles, not to mention that it would probably increase the costs of the services.

---

[22] Article 25(1) of the GDPR calls this "the time of the determination of the means for processing".

23 Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014) https://www.dataprotection.ro/servlet/ViewDocument?id=1088.

On the other hand, it is worth noting that the integrity of the data might be compromised by the way in which IoT data are shared and stored. It might happen that one of the processors or joint-controllers delete or damage the data at some point. In order to prevent such scenarios, backup copies are a compulsory security measure. Their creation should be foreseen from the first stages of the functioning of the IoT system.

8.2 Perform a security risk analysis

According to the confidentiality principle, controllers should minimize the risks to data subjects' rights, interests, and freedoms. To this purpose, they should work on a risk-based approach. To manage the risks to individuals that arise from the processing of personal data in IoT systems, it is important that controllers develop a mature understanding and articulation of fundamental rights, risks, and how to balance these and other interests. Ultimately, it is necessary for controllers to assess the risks to individuals' rights that the use of IoT poses, and determine how they need to address these and establish the impact this has on their use of IoT.[24] To this purpose, two key factors must be considered:[25]

- Risks arising from the processing itself, such as the emergence of biases associated with profiling or automated decision-making systems.
- Risks arising from the processing in relation to the social context and the side effects indirectly related to the object of processing that may occur.

In order to minimize such risks, controllers must ensure that appropriate technical and organizational measures are implemented to eliminate, or at least mitigate the security risk, reducing the probability that the identified threats will materialize, or reducing their impact. It is necessary to take into account the security standards that already exist in the market, as well as the compliance standards in relation to data protection that will apply to the IoT solution.

8.3 Be aware of the risks that are intrinsically linked to most IoT systems

It is necessary to take account key aspects of the IoT application when defining its functionality and the potential impact on data protection, such as:

- Generally, there is a part for data collection or to provide information for the IoT application or services, so the security of the data collected must be managed.
- The processing or analysis of these data usually takes place in very remote locations in the cloud and, to be able to reach them, it is necessary to use shared

24 ICO (2020) IoT auditing framework - draft guidance for consultation. Information Commissioner's Office, Wilmslow, p.13-14. Available at: https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf (accessed 15 May 2020).

25 AEPD (2020) Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. Agencia Espanola Proteccion Datos, Madrid, p.30. Available at: www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf (accessed 15 May 2020).

networks, public networks, etc. This aspect has an impact on the protection of the data stored and in motion managed in person by the development team or by a third party.

- It is becoming increasingly common for IoT applications to be hyper connected with other ones, from either the same manufacturer or developers or a different one, creating large networks of IoT devices. It is thus necessary to consider the security of data shared or accessible by third parties.
- The integration with third parties ensures compatibility with other products and grants the application greater versatility and functionality, but on the other hand it makes necessary to define a procedure to assess the security of components provided by external suppliers.
- The interaction between the human “user” and the “product machine” is present and special attention must be paid to ensure a satisfactory user experience while not compromising security.
- The security assessment of the IoT application should include technical tests such as code review and penetration testing. Penetration testing helps to check the security level of the system, early detection and, in case of failures, to fix possible errors that may affect data security during implementation in order to mitigate or minimize risks before moving to production. Penetration testing is a very efficient test during the evaluation phase because it subjects solutions to the same threats, they might face during the normal operation of an IoT application. As part of so-called ethical hacking, these tests aim to uncover weaknesses in the system that could be exploited in the future by a hacker.