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 (IoT)

IoT: Ethical and legal requirements regarding data protection

Iñigo de Miguel Beriain (UPV/EHU)

Aliuska Duardo (UPV/EHU), Álvaro Anaya Rojas, Gerardo Pérez Laguna & María Carmen González Tovar (Everis Ciberseguridad)

Preliminary versions of this document were reviewed by Federica Lucivero (Senior Researcher in Ethics and Data at Ethox and the Wellcome Centre for Ethics and Humanities (Big Data Institute) and Irene Kamara (Assistant Professor Cybersecurity Governance at TILT)

Revised by Fruzsina Molnar-Gabor, Heidelberger Akademie der Wissenschaften (Germany) and member of the European Group on Ethics in Science and New Technologies of the EU Commission.

Finally validated by Iñaki Pariente, former director of the Basque Data Protection Agency.

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 it contains

Introduction

This section of our 'Guidelines on data protection ELI in ICT research and innovation' (hereafter 'The Guidelines') 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. They aim contribute to mitigate the ethical and legal issues in this field. Needless to say, this part of the Guidelines (as the whole of them) is not an authorized interpretation of the regulations, but some best practice recommendations.

This part of the Guidelines 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

Disclaimer

This part of The Guidelines was written at a time when the ePrivacy Regulation had not been approved. It may happen that at the time of using this tool, the Regulation is in force. If so, it will be necessary to take into account the possible changes that this may have produced in the regulatory framework. Until the ePrivacy Regulation enters into force, a fragmented situation will exist. Indeed, supervisory authorities face now a situation where the interplay between the ePrivacy Directive and the GDPR coexist and pose questions as regards the competences, tasks and powers of data protection authorities in those matters that trigger the application of both the GDPR and the national laws implementing the ePrivacy Directive.

Preface

Some years ago, the Article 29 Working Party stated that "the concept of the Internet of Things (IoT) refers to an infrastructure in which billions of sensors embedded in common, everyday devices – "things" as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities."[1]

As for today, ubiquitous, pervasive, internet of everything, are some of the qualifiers used to describe IoT. These adjectives are intended to illustrate that the interconnection between the physical and virtual world is happening and can happen at all levels. The

[1] A29 Working Party, Opinion 8/2014 on the on Recent Developments on the Internet of Things, 2014, at: https://www.dataprotection.ro/servlet/ViewDocument?id=1088

new and emerging IoT technologies comprises, among others: intelligent transportation systems, connected health devices, drones, 5G wireless communication, etc. Even the most trivial everyday aspects of our lives are beginning to be permeated by IoT. From "smart" coffee machines to mobile apps that allow us to perceive smells

IoT is a special technology with strong ties to traditional Data Science technologies, but also with many differences that must be taken into account when defining a development model. Speed in data generation is one of the biggest differences between IoT and traditional Data Mining technologies. Although these technologies can become complementary, dynamic data processing encompasses shared networks to perform an analysis and response in real time, such as IoT does against an analysis of large volumes of static data.

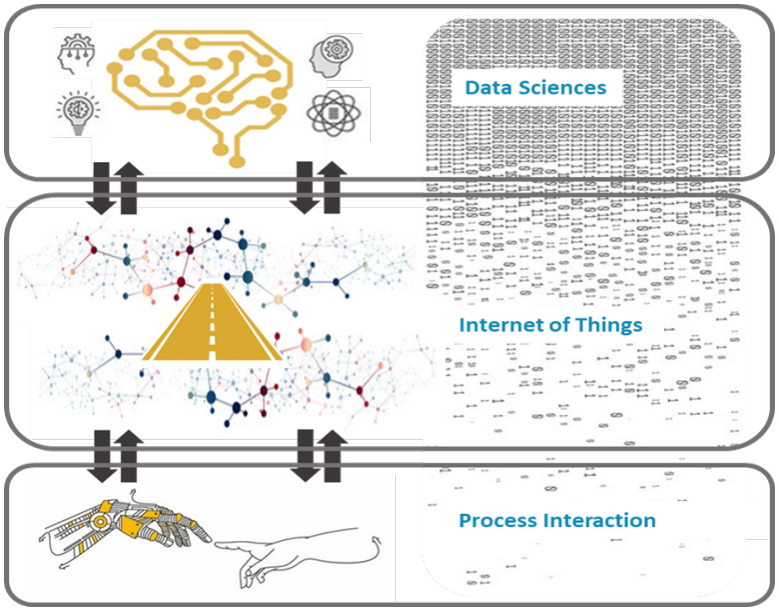

Figure 34 IoT and Data Sciences landscape

This success in the field of data handling also presents a complexity in the development of new technologies, which is why it is essential to define processes to facilitate the development and implementation of IoT applications. Having models that help ICT developers understand the data protection legal framework, and that make it possible to identify, classify, and define the necessary tasks to address processing from the beginning of the development of solutions, gives the opportunity to reach a more efficient and structured implementation.

Covering all the ethical and legal implications of any IoT system in a guideline would be impossible. The qualification of IoT applies to a lot of different things. First, the devices themselves (step-counters, sleep trackers, “connected” home devices like thermostats, smoke alarms, connected glasses or watches, etc.). Second, the users’ terminal devices (e.g. smartphones or tablets) on which software or apps were

previously installed to both monitor the user's environment through embedded sensors or network interfaces, and to then send the data collected by these devices to the various data controllers involved. Furthermore, software tools are necessarily used to make the systems work.

It would be hard to address all the issues related to this wide framework. Thus, our work proposes a simplified model that makes it possible to help IoT system developers fulfil the personal data protection requirements settled by the European Charter of Human Rights, the GDPR and the complementary regulatory tools. Nonetheless, stakeholders, including designers, manufactures, network owners and marketers, must take into account the applicable laws and ethical guidelines that for each specific development, -both mechanical and information and communication systems- related to its concrete IoT system.

To this purpose, this Chapter of the Guidelines attempts to offer ICT developers a systematic and simplified view of how to meet the legal requirements of EU data protection law. This is done without neglecting ethical guidelines, adding IoT products the value of "empowering individuals by keeping them informed, free and safe"[2]. In this sense, the present document, draws heavily on the considerations of the Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things[3]; the Commission Staff Working Document Advancing the Internet of Things in Europe[4]; and the Baseline Security Recommendation for IoT in the Context of Critical Information infrastructures[5]. **Notably, these documents are subject, in most member states, to a particular regulatory framework and represent different regulatory subject matter than the areas covered by the other guidelines. Furthermore, ICT developers should always keep in mind that the EU regulation on IoT will probably change in the next times. Consultation with their DPOs about possible changes and national particularities is always recommendable.**

2 According to the Article 29 Data Protection Working Party, this is "is the key to support trust and innovation, hence to success on these markets". Article 29 Data Protection Working Party Opinion 8/2014 Op. Cit.

3 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. Accessed Nov 2020). Although this opinion predates the entry into force of the current GDPR, we consider that the assessments made at the time by the working group are still valid. This opinion provides the ethical-legal keys to guarantee privacy, without hindering the development of the IoT.

4 Commission Staff Working Document Advancing the Internet of Things in Europe, accompanying the Document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitising European Industry Reaping the full benefits of a Digital Single Market. European Commission N5(APRIL 19, 2016) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016SC0110&qid=1610616372730 (Access Dec. 2020).

5 Baseline Security Recommendation for IoT in the Context of Critical Information infrastructures, ENISA 12 (2017), https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot. (Accessed Nov 2020)

1 Project Understanding

In this first part, we will give some general advice on how to approach the development of an IoT system in the early stages of its production cycle, i.e. when it is still not much more than an idea that has not yet been implemented. It is important to keep them in mind if you want to ensure the implementation of data protection by design policies (see "Data Protection by design and by default" section in the "Main Concepts", Part II of these Guidelines).

The essential tips are:

- Make sure that your project is compatible with the data protection framework
- Implement a training program in ethical and legal issues for IoT developers
- Define the roles played by all agents involved in the processing
- Promote end-users engagement

1.1 Make sure that your project is compatible with the data protection framework

Before starting the development of an IoT system, the developers should have its primary objectives and possible secondary goals and uses clear in mind. It might happen that such goal is not compatible with the ethical and legal standards of the EU (such as, for instance, the **Charter of Fundamental Rights** of **the European Union)**. If the system deprives or reduces data subjects' capacity to make free decisions about their lives, if it makes decisions about fundamental freedoms and freedoms without any form of human oversight or possibilities for redress, if the system is based on the need to create a kind of addiction, etc., the project should not be endorsed.

Alternatively, it might happen that the goal of the IoT system involves a disproportionate use of personal data which defies the minimization principle, rendering it hard to be in compliance with the applicable legal framework. Furthermore, developers also should keep in mind that the processing of data in the IoT may also concern individuals who will not be subscribers or users of their technology[6]. This scenario creates risks associated with the fact that some data subjects might not be aware that their data is being processed. Additionally, "if the controller envisages a 'model' where it takes solely automated decisions having a high impact on individuals based on profiles made about them and it cannot rely on the individual's consent, on a contract with the individual or on a law authorizing this, the controller should not proceed."[7] Finally, developers shall assess whether the project is acceptable according to ethical standards, despite it being compliant with legal obligations.

To sum up, developers shall analyze carefully the possible impact of the technology and appropriate measures to be designed to guarantee data protection, privacy

6 Art. 29 Op. cit. p. 13.

7 Ibid., p.30.

and other rights, as defined by the Charter of Fundamental Rights of the European Union and related legal framework As regards data protection and privacy, if the analysis shows that the processing will not be acceptable on the basis of the Charter of Fundamental Rights of the European Union, the GDPR and the ePrivacy framework, the project should not be endorsed.

Box 1: Smart Glasses

The Art. 29 WP draws attention to this issue with the following example: "wearable devices like smart glasses are likely to collect data about other data subjects than the owner of the device. It is important to stress that this factor does not preclude EU law from applying to such situations. The application of EU data protection rules is not conditioned by the ownership of a device or terminal but by the processing of the personal data itself."

If developers are willing to create a device such as this, they should be aware of the fact that the GDPR requires the fair and lawful processing of all personal data gathered. This includes, among others, the condition of a valid legal basis for a processing operation, purpose limitation, data minimization, limitation of data retention, data quality and security, rights of the data subjects and independent supervision. GDPR also introduces the principle of accountability as an overarching obligation to strive for compliance not only with the letter of the law. It also provides concrete instruments and tools to achieve accountability, with a risk based approach implemented inter alia in data protection impact assessments (DPIA), data protection by design and by default, nomination of a data protection officer as well as compliance with existing codes of conduct and certification mechanisms.

The developers should consider all these essential issues at the first stages of their project development, so as to avoid unnecessary efforts, if compliance with the data protection legal framework cannot be guaranteed.

In addition, a clear idea of the project will help determine in early stages of the development other legal issues within data protection law, such as the possible need of international transfers of data, the existence of joint-controllers or processors, which need to be carefully selected, or the security and organizational measures to minimize risks.

This document will analyze the main data protection obligations in more detail.

1.2 Implement a training program in ethical and legal issues for IoT developers and other relevant stakeholders

One of the main problems with IoT systems is that they use personal data from data subjects other than the end-users of the devices interacting among themselves. Furthermore, they often provide the controllers with large datasets through the aggregation of data gathered from individual agents. These circumstances somehow blur the relationship between the controller and the data subjects. The controllers are

simply unaware of who are the data subjects providing some of the data collected by the devices. This could bring consequences in terms of adequate compliance with data protection standards. For instance, it is hard to inform data subjects about the processing if controllers are not aware of who the data subjects are. Indeed, the scenario is hard, since those data subjects could be identifiable, though, if a reasonable effort were made.

It is paramount that the key employees have the fullest possible awareness of the legal implications of their work, so as to avoid unwanted unlawful data processing or, in general, lack of compliance with the data protection regulation. In addition, employees and other stakeholders should gain awareness of the ethical and social consequences derived from the processing of personal data through technological means.[8]

IoT developers must be able to understand the implications of their action, both for individuals and society, and be aware of their responsibilities by learning to show continued attention and vigilance.[9] This will help the IoT developers to properly take into account ethical and legal matters. In that sense, **an optimal training for all agents** involved in the project (developers, programers, coders, data scientists, engineers, researchers, etc.) before it starts could be one of the most efficient tools to save time and resources in terms of compliance with data protection regulations.

Thus, implementing basic training programs that include at least the fundamentals of the Charter of Fundamental Rights (specially, as regards the role of privacy as catalyst for other rights such as non-discrimination, or ideological freedom), the principles exposed in Article 5 of the GDPR, the need for a legal basis for the processing (including contracts between the parties), the practical consequences of the data protection by design and by default principles, and others. Useful sources are for example available by the Fundamental Rights Agency[10], IEEE and its ethics guidelines[11], and the European Commission[12]. If training is not possible, implementing advice from an **external expert** from the very beginning of the project could be an acceptable alternative.

1.3 Define the data protection roles played by all agents involved in the processing: determination of controllers and processors

One of the biggest problems with IoT systems is that they often use different devices, with their own characteristics. This creates significant problems in terms of the distribution of roles among the different controllers involved. On the other hand, it is obvious that a controller will often entrust some of the technical tasks to a processor, who could even involve a sub-processor in the tasks. In practice, however, there will be

8 CNIL (2017) How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence. Commission Nationale de l'Informatique et des Libertés, Paris, p.55. Available at: www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf (accessed 15 May 2020).

9 Ibid., p.55.

10 https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition and

11 https://ethicsinaction.ieee.org/

12 https://ec.europa.eu/justice/smedataprotect/index_en.htm

times when it will be difficult to ensure that the processor is not actually acting as a controller or joint controller.

IoT developers should do their best to avoid such issues, since the data protection regulation requires a clear answer to the question of "who is responsible for this processing?" to guarantee an effective and complete protection of the data subjects' rights and freedoms. Thus, a key requirement of an adequate data protection by design policy is to **clarify from the very beginning who are the data controllers and processors, in order to ensure that the legal accountability is understood.**

In order to fulfil this goal**, written agreements between all agents involved in the development of the tool should be reached and documented.** 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. See the box below.

In addition, some parties may draft contracts positioning themselves in a different role than what really applies to them. For instance, a stakeholder may argue it is a processor in order to avoid certain controllership obligations, and even sign a contract. However, reality rules here and, regardless of what the parties say, their role will have to be defined according to their acts. In this sense, EU case law[13] tends to widen the concept of controller and joint-controller, reducing the space for pure processors. In this regard, it will often happen that all parties involved share some degree of responsibility and become joint-controllers for those parts of the processing activities involving those different parties. From there on, each party will have its own independent separate responsibility.

[13] See: Judgment of the Court (Grand Chamber) of 5 June 2018.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH.
Request for a preliminary ruling from the Bundesverwaltungsgericht. Case C210-16, at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62016CJ0210

Box 2: Dealing with complex data responsibilities scenarios

The EU-funded research project Synchronicity was aimed at creating a harmonized ecosystem for IoT-enabled smart city solutions, where IoT device manufacturers, system integrators and solution providers can innovate and openly compete. Thus, it used a lot of personal data provided by different sources. In this context, "it appeared quite clearly that the de facto data controllers were the cities themselves. They are the ones who control what data are collected and for what purpose. At the same time, the project had a collective responsibility to ensure that its research activities were complying with the regulation too. Data Protection Coordination – Mezzanine Model While several data controllers may be involved, coordination among them at the project level has to be ensured and guaranteed. This is what Synchronicity experienced by setting up a Data Protection Committee (DPC) gathering the Data Protection Officers (DPO) of each smart city chaired by a Project Data Protection Coordinator (PDPC) at the project level. By law, the cities remain the formal data controllers of the data processing under their control and they are directly accountable for it. However, the establishment of the DPC enables close coordination and sharing of experience to ensure that the project as a whole complies with the regulation, as well as to identify and mitigate potential risks that may impact the partners."

Following this criterion, the roles and responsibilities in the project were distributed as follow:

At City DPO Level

- x DPO functions and responsibilities, including data protection and GDPR compliance monitoring
- x Personal Data collection identification, including data controllers & processors identification
- x Data Protection Impact Assessment (DPIA)

At Project Level

- x Data Protection Policy Coordination
- x Public Information and Contact
- x Reporting and data protection Issues Management

(See: https://www.monica-project.eu/wp-content/uploads/2020/06/Personal-DataProtection-for-IoT-Deployments-final-MI.pdf, p. 11)

1.4 Promote end-users engagement

Since IoT involves the use of personal data from different types of data subjects, it is highly recommendable, where possible, 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, where they exist, ensures the implementation of a bottom-up framework that could be very helpful to this purpose.

Checklist: Project Understanding

- The IoT development does not promote scenarios that are not compatible with the EU fundamental values and legal framework.
- The IoT development does not involve a disproportionate use of personal data (processing is not against the minimization principle).
- The controller can ensure that appropriate lawful bases for data processing will apply to

all required data processing activities.

- The controller can ensure that the key team members processing personal data have been adequately trained on data protection issues and/or adequate assessment tools have been implemented.
- The roles played by all different agents involved in the IoT tool have been adequately identified and the controller can provide evidence on this (a statement or agreement has been signed, for instance).
- Whenever there are, the representatives of the key collectives involved in the data processing have been consulted on the IoT tool features.

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[14] 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.[15] However, it might happen that the criteria

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

15 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/

used by EU Member States DPAs are quite different. Thus, you should better ask your DPO about this issue.

A preliminary issue: do not forget that processing data of special categories is banned!

Before processing data, controllers should make sure that they are not data of special categories. If this is not the case, they shall remember that article 9.1 of the GDPR vetoes such processing, unless any of the circumstances described in article 9.2 applies. Furthermore, controllers should keep in mind that most of these circumstances (consent is an exception) require that such processing is performed on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject. These safeguards might be pseudonimization, professional secrecy, or even more complex mechanisms if transfer personal data to a third country or an international organization is foreseen (see article 46 of the GDPR).

2.1 Consent

Consent is the most traditional legal basis for data processing. Furthermore, the draft of the ePrivacy Regulation[16] 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. Consent, however, will only apply if some conditions are met. If consent is used as the legal basis for data processing, **developers should ensure that the device they are creating includes the need to require the users' prior consent for processing in a specific, informed and granular way and ensure the adequate documentation of such consent.**

According to the EDPB, granularity means that "a service may involve multiple processing operations for more than one purpose. In such cases, the data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes. In a given case, several consents may be warranted to start offering a service, pursuant to the GDPR."[17]

The granularity "should not only concern the categories of collected data, but also the time and frequency at which data are captured, as well as the different purposes those data will be processed for. Similarly to the "do not disturb" feature on smartphones, IoT devices should offer a "do not collect" option to schedule or quickly disable sensors."[18]

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

17 EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Adopted on 4 May 2020, at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

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.

It must be crystal clear that consent by the data subject cannot be obtained freely through mandatory acceptance of general terms and conditions, nor through opt-out possibilities.[19] Thus, devices should be designed in a way that ensure that consent is granular and users hold the possibility to renounce certain services or features of an IoT. Users should not be penalized or have degraded access to the capabilities of the system if they decide not to use it (when interacting with another system) or if they decide not to use a specific service incorporated in the system.

Devices and applications should always be designed to inform users and non-user data subjects about the processing of data, for instance via the device physical interface or by broadcasting a signal on a wireless channel. **Irrespective of the existence of any contractual relationship and even the legal basis for the processing, any data subject, no matter if they are a user or a non-user must be informed and in a capacity to exercise their rights, (the only exception is the right to object, which is not applicable if the legal basis for processing is consent).** [20] The possibility to withdraw consent shall be guaranteed from the moment when the data are collected and data subjects must be informed of such possibility.

Consent management needs prior compliance with the data protection by design and by default principles. As Wachter stated, it is highly recommendable that IoT developers set access permissions "**not only for users, but also for 'things' seeking to access or process a user's data on the user's or a third party's behalf.** These access permissions must respect user's privacy preferences. Identity management combined with role-based access control, for example, enables identity verification coupled with authorization of users' actions requests or devices according to their system-assigned role, ensuring that only actions authorized to a specific role (e.g. collecting, transmitting, or processing data) can be taken in a session. Administrators or users can define these permissions, offering different approaches to protect user's subjective privacy preferences."[21]

19 Article 29 Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices Adopted on 16 May 2011. 881/11/EN WP 185, P. 13, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf

20 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

21 Wachter, Sandra, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, Volume 34, Issue 3, 2018, pages 436-449.

Box 3: Sticky Policies and Privacy Proxies

A better control on data processing might be guaranteed by the use of an approach based on the so-called sticky policies can support compliance with the data protection framework by embedding information on conditions and limits to the use of data with the data itself. Thus, those policies could establish the context of use of the data, the purposes, policies on third party access and a list of trusted users

An alternative/complementary way to offer a data subject real control on how data must be processed when interacting with sensors by being able to express preferences, including getting and revoking consent and purpose limitation choices could be based on the use of **privacy proxies.** Supported by a device, data requests are confronted with predefined policies governing access to data under the control of the data subject. By defining sensor and policy pairs, third parties requests for collection or access to sensor data would be authorized, limited or simply rejected.

Source: 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

In order to prevent the risks of secret monitoring, the former Article 29 Working Party considers it essential that **the device warns that the data sharing feature is 'ON', for example through a permanently visible icon**.[22] Indeed, envisaging appropriate signposting that would be actually visible to the data subjects could be particularly important when we are dealing with wearables. All IoT devices should inform non-user data subjects whose data are collected of such processing, including all relevant information about it. Controllers should make their best to ensure that such information is provided, even though in practice this might be hard. **Adequate tools shall be implemented to ensure that the non-user data subjects' preference not to have their data collected by the device are respected.**

If the IoT device incorporates **tools provided by third parties**, and consent is the most appropriate lawful basis, the IoT developers should be aware of the fact that these tools should be installed on an opt-in basis (even when that is not a widely followed practice in some sectors). Therefore, the Article 29 Working Party stated that "as such access is subjected to the requirement of obtaining the user's prior consent, this consent needs to be clearly given, specific, and informed. Practice shows, however, that often authorization requests made by third-party application developers do not display

22 Article 29 Working Party (2011) Opinion 13/2011 on Geolocation services on smart mobile devices Adopted on 16 May 2011. 881/11/EN WP 185, P. 13, at: https://www.apda.ad/sites/default/files/2018-10/wp185_en.pdf. See the LaLiga case, at: https://asociaciondpd.com/wp-content/uploads/2019/07/PS-00326-2018_ORI.pdf. An English summary is available at: https://iapp.org/news/a/spanish-dpa-fines-la-liga-250k-euros-for-alleged-gdpr-violations/

sufficient information for the user's consent to be considered as specific and sufficiently informed, hence valid under EU law".[23]

Finally, yet importantly, the Article 29 Working Party recommended that providers of applications or services seek **to renew individual consent** (even where there is no change in the nature of processing) after an appropriate period of time. For instance, it may not be valid to continue to process personal data where an individual had not actively used the service within the previous 12 months. Even where a person has used the service they should be **reminded at least once a year** (ideally more often, especially where the nature of the processing warrants it) of the nature of the processing of their personal data. Thus, the developer could consider the possibility to incorporate in the device or system a tool able to send a request to the user and re-gain (or not) their consent to continue with the processing. **However, this is more a recommendation that a hard law requisite.** In any event, data subject must have at their disposal an easy way to withdraw consent, at any time, with no retroactive effects.

Broad consent might be acceptable, but only if some concrete circumstances apply, such as: it is difficult or improbable to foresee how this data will be processed in the future; broad consent used for processing of special categories of data is compatible with national regulations; where broad consent is used, the data subjects are given the opportunity to withdraw their consent and to choose whether or not to participate in certain research and parts of it. Furthermore, some **safeguards must be implemented (see box 4).**

Box 4: Broad consent and additional safeguards

The German DPA has listed some additional safeguards to be implemented in the case of broad consent in the context of research projects.[24] These, which can be appropriately adapted to other circumstances, are:

1. Safeguards to ensure transparency:

- Utilization of usage regulations or research plans that illustrate the planned working methods and questions that are to be the subject of the research project.
- Assessment and documentation of the question why in this particular research project a more detailed specification of the research purposes is not possible.
- Set up a website to inform study participants about ongoing and future studies.

2. Safeguards to build trust:

- Positive vote of an ethics committee before use of data for further research

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.

24 DSK, Beschluss der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zu Auslegung des Begriffs „bestimmte Bereiche wissenschaftlicher Forschung" im Erwägungsgrund 33 der DS-GVO 3. April 2019, at: www.datenschutzkonferenz-online.de/media/dskb/20190405_auslegung_bestimmte_bereiche_wiss_forschung.pdf (accessed 20 May 2020). The English translation comes from a nice summary of the measures that can be consulted here: www.technologylawdispatch.com/2019/04/privacy-data-protection/german-dpas-publish-resolution-on-concept-of-broad-consent-and-the-interpretation-of-certain-areas-of-scientific-research/

purposes.

- Assessment of whether it is possible to work with a dynamic consent or whether a data subject can deny consent or object before the data might be used for new research questions (depending on the lawful basis for such subsequent processing of data).

3. Security safeguards:

- No data transfers to third countries with a lower level of data protection.
- Additional measures regarding data minimization, encryption, anonymization, pseudonymization, or implementation of security measures.
- Implementation of specific policies to limit access to personal data.

Importantly enough, if the processing of the data is necessary for the processing, in such a way that the processing cannot take place without the data, or that a certain service cannot be offered without the processing, consent may not be the most effective lawful basis. This is true as data subjects may always have a right to withdraw consent at any time. In cases where the activity is dependent on the data, the withdrawal of consent may trigger the incapability to satisfy the service. Depending on all the other circumstances surrounding the processing activity, in these cases other lawful bases may be more appropriate, such as the necessity to execute a contract.

Furthermore, data subjects must have a possibility to withdraw any prior consent given to a specific data processing and to object to the processing of data relating to them. The exercise of such right must be possible without any technical or organizational constraints and the tools provided to register this withdrawal should be accessible, visible and efficient.

According to the Article 29 WP, "withdrawal schemes should be fine grained and should cover:

(1) Any data collected by a specific thing (e.g. requesting that the weather station stops collecting humidity, temperature and sounds);

(2) A specific type of data collected by anything (e.g. a user should be able to interrupt the collection of data by any devices recording sound, whether a sleep tracker or a weather station);

(3) A specific data processing (e.g. users could require that both their pedometer and their watch stop counting their steps). Furthermore, since wearable "connected things" are likely to replace existing items that provide usual functionalities, data controllers should offer an option to disable the "connected" feature of the thing and allow it to work as the original, unconnected item (i.e. disable the smart watch or glasses connected functionality).

The Working Party has already specified that data subjects should have the possibility to "continuously withdraw (their) consent, without having to exit the service provided"[25] .

25 Art 29 Data Protection Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things (SEP 16, 2014), p. 20, at: https://www.dataprotection.ro/servlet/ViewDocument?id=1088

Checklist: consent

 The controllers are able to demonstrate that, after balancing the circumstances of the processing, they have concluded that consent is the most appropriate legal basis for processing.

 The controllers request the consent of the data subjects in a free, specific, informed and unequivocal manner, according to Article 7 GDPR.

 The controllers have informed the data subjects about their right to withdraw consent at any time.

 Where broad consent is used for the processing of special categories of data is compatible with national regulations.

 Where broad consent is used, the controller is particularly the data subjects are given the opportunity to withdraw their consent and to choose whether to participate in certain projects and parts of it.

 The power imbalance between controllers and data subjects does not impede free consent. This is particularly important in context such as the labor framework.

 The controllers ask people to actively opt in.

 The controllers do not use pre-ticked boxes or any other type of default consent.

 The controllers use clear, plain language that is easy to understand.

 The controllers specify what types of data they want, why they want it, what they are going to do with it and for how long data will be processed.

 The controllers give separate distinct ('granular') options to consent separately to different purposes and types of processing.

 The controllers link which pieces of data or categories thereof will be processed for each purpose.

 The controllers have informed the data subjects about their right to withdraw consent at any time and how to do so.

 The controllers ensure that individuals can refuse to consent without detriment in their access to the service.

 The controllers avoid making consent a precondition of a contract to provide a service if the data is not necessary for the performance of such service.

2.2 Performance of a contract

Sometimes, data might be processed based on article 6.1(b) of the GDPR: Processing of personal data is lawful when it is necessary for the performance of a contract to which the data subject is party. The scope of this legal basis is limited by the criterion of "necessity", which requires a direct and objective link between the processing itself and the purposes of the contractual performance expected from the data

subject. Indeed, this legal basis only legitimates processing that is in fact necessary for such goal. On the contrary, if processing is not in fact necessary for the performance of a contract, such processing can take place only if it relies on another appropriate legal basis.[26]

Thus, **the idea of necessity is key in order to determine whether this legal basis is applicable to the processing or not.** The EDBP adopted in 2019 its Guidelines on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects that are particularly relevant to this issue.[27] According to these Guidelines, the use of data might be necessary for the performance of a contract with a data subject, or in order to take pre-contractual steps at the request of a data subject.

It is important to note that the concept of what is 'necessary for the performance of a contract' is not simply an assessment of what is permitted by or written into the terms of a contract. The concept of necessity involves several **requirements**.

- **First**, the processor shall identify the concrete purpose for the processing, since in the context of a contractual relationship, there may be a variety of purposes for processing and not all of them are necessary for the performance of a contract or in order to take pre-contractual steps. Thus, the concrete purposes to be legitimated via this legal basis shall be clearly specified and communicated to the data subject, in line with the controller's purpose limitation and transparency obligations. If, for instance, these purposes are necessary for the controller's other business purposes, but not for the specific performance of the contract with the subject, these might be lawful under the legitimate interest legal basis or consent, but not under the performance of a contract basis. Moreover, of course, sometimes processing would not be covered by any legal basis and, thus, should be avoided.
- **Second,** one must keep in mind that there are **three main conditions that need to be met to assess that this legal basis applies in a concrete contract**, namely: (a) a contract exists, (b) the contract is valid pursuant to applicable national contract laws, and (c) that the processing is objectively necessary for the performance of the contract. This last part is particularly important: **objectively necessary** means that this need relates to "a purpose that is integral to the delivery of that contractual service to the data subject. Included here is processing of payment details for charging for the service. **The controller should be able to demonstrate how the main object of the specific contract with the data subject cannot, in fact, be performed if the specific processing of the personal data in question does not occur**. The important issue here is the nexus between the personal data and processing operations concerned, and the performance or non-performance of the service provided under the contract."

26 Article 29 Working Party Guidelines on consent under Regulation 2016/679 (WP259), endorsed by the EDPB, page 19.

27 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Adopted on 9 April 2019, at: https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

[28] That is, the fact that the processing of personal data is included as an obligation in a contract does not make it "necessary for the performance of a contract" in the terms of the data protection legislation. Thus, **if the controller introduces a condition in the contract that obliges the data subject to allow the processing, even though this processing is not strictly necessary to perform the contract, the legal basis is not applicable to this scenario.** If there are realistic, less intrusive alternatives, the processing is not 'necessary'." [29]

- Last but not least, controllers should always remember that **both purpose limitation and data minimization principles are particularly relevant when a controller uses "performance of a contract" as a legal basis for data processing**, since the contracts for online services (which are the typical services linked to IoT devices) are not usually negotiated on an individual basis.

28 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Adopted on 9 April 2019, at: https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

29 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects Adopted on 9 April 2019, at: https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-final_public_consultation_version_en.pdf

Box 5: Can profiling be considered as necessary for the performance of a contract?

The EDPB acknowledged that **personalization of content** may constitute an essential or expected element of certain services, and therefore **may be regarded as necessary for the performance of the contract** with the service user in some cases. Whether such processing can be regarded as an intrinsic aspect of a service, will depend on the nature of the service provided, the expectations of the average data subject in light not only of the terms of service but also the way the service is promoted to users, and whether the service can be provided without personalization. Where personalization of content is not objectively necessary for the purpose of the underlying contract, for example where personalized content delivery is intended to increase user engagement with a service but is not an integral part of using the service, data controllers should consider an alternative lawful basis where applicable.

Instead, **behavioral advertising** and associated tracking and profiling of data subjects **cannot be based on the performance of a contract legal basis**, not even where such advertising indirectly funds the provision of the service. Such processing is separate from the objective purpose of the contract between the user and the service provider, and therefore not necessary for the performance of the contract at issue. Therefore, the controllers should use other legal basis like consent or legitimate interest if they are willing to proceed in such way.

Source: EDPB Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects Adopted on 9 April 2019, at: https://edpb.europa.eu/sites/default/files/consultation/edpb_draft_guidelines-art_6-1-b-

Checklist: performance of a contract

 The controllers are able to demonstrate that, after assessing the circumstances at stake they have concluded that performance of a contract is the most appropriate legal basis for processing.

 The controllers can demonstrate that processing is **objectively necessary for the performance of the contract**. To this purpose, they have answered to these questions:

- What is the nature of the service being provided to the data subject? What are its distinguishing characteristics?
- What is the exact rationale of the contract (i.e. its substance and fundamental object)?
- What are the essential elements of the contract?
- What are the mutual perspectives and expectations of the parties to the contract? How is the service promoted or advertised to the data subject? Would an ordinary user of the service reasonably expect that, considering the nature of the service, the envisaged processing would take place in order to perform the contract to which they are a party?

 The controllers have informed the data subjects about the need to process their data on

this legal basis.

- If special categories of data need to be processed, controllers have identified an exception to the veto included in article 9.1 the GDPR in article 9.2.
- Where broad consent is used, the controller is particularly the data subjects are given the opportunity to withdraw their consent and to choose whether to participate in certain research and parts of it.
- The controllers do not extend this legal basis to the processing of data that are not strictly necessary to perform the contract.
- The controllers are aware that the inclusion of a condition to sign the contract that involves data processing does not justify that this processing is necessary for the performance of the contract.

2.3 Legitimate interest

Legitimate interest is one of six legal bases for the processing of personal data stated in Article 6(1) of the GDPR. This legal basis requires that the legitimate interests of the controller or any third parties to whom the data are disclosed prevails over the interests, fundamental rights and freedoms of the data subjects which require the protection of personal data (Article 6(1)(f)). To verify that this is indeed the case, controllers must conduct a ***balancing test***, following the Article 29 Working Party guidelines [30] (see the "Balancing test", within "Main Tools and Actions", in Part II of these Guidelines). Of course, the same as other lawful basis from the processing even though the legitimate interest prevails and the assessment concludes the processing can take place, data subject rights still not apply (see "Data subject' rights" within Part II of these Guidelines). Furthermore, adequate safeguards and mitigation measures aimed at minimizing risks and ensuring data subjects' privacy protection should be implemented whenever possible, especially when the assessment concludes there is a high risk for the rights of the data subjects.

Checklist: legitimate interest

- The controllers have checked that legitimate interest is the most appropriate basis.
- The controllers have checked that the processing is necessary and there is no less intrusive way to achieve the same result.
- The controllers have done a balancing test, and are confident that the individual's interests do not override those legitimate interests.

30 A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 05 January 2020

- The controllers only use individuals' data in ways they would.
- The controllers are not using people's data in ways they would find intrusive or which could cause them harm, unless we have a very good reason.
- If the controllers foresee the processing of children's data, they have taken extra care to make sure they protect their interests.
- The controllers have considered safeguards to reduce the impact where possible.
- The controllers have implemented adequate tools to ensure data subjects' rights.
- If they have identified a significant privacy impact, they have considered whether they also need to conduct a DPIA.
- The controllers include information about our legitimate interests in their privacy information.

2.4 Public interest and the scientific research framework

According to Article 6 (e) of the GDRP, processing is lawful if it is necessary for the performance of a task carried out in the public interest. Furthermore, scientific research could serve well to avoid the veto on special categories of data processing included in article 9.1 of the GDPR. However, in this case, according to Article 9.2(j), the processing shall be based in the law of the EU or a Member State and shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (see "Data processing for purposes of archiving in the public interest, scientific or historical research purposes or statistical purposes", "Main Concepts", Part II of these Guidelines). Nevertheless, IoT developers should always consider that it is not necessarily true that all scientific research involves a public interest. Indeed, "it is difficult at present, if not impossible, to view a 'substantial public interest' as a basis for processing sensitive data for scientific research purposes" if a Member State has not produced specific regulation to this purpose. Thus, IoT developers should analyze the legal framework in their concrete country.

On the other hand, one must remember that Article 5 (b) GDPR establishes the purpose limitation principle, under which data cannot be processed for purposes other than the specific initial ones (see "Data protection and scientific research", in "Main Concepts", Part II of these Guidelines).

If the development of an IoT system could be considered as scientific research, the Union or Member State law may provide for derogations from the rights referred to in Articles 15 (right of access), 16 (right to rectification), 18 (right to restriction of processing) and 21 GDPR (right to object), always subject to some conditions and safeguards (Article 89(2)).

Checklist: use of data for scientific research

- The controllers have checked that their project fits well with the concept of scientific research.
- The controllers have consulted their DPOs about the use of this exception to the ban on the processing of data of special categories.
- The controllers have consulted the national legal framework about this topic.
- The controllers have implemented the safeguards and organizational measures devoted to align with article 89 of the GDPR and corresponding national regulation.
- The controllers have documented all the information regarding 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 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."[31] 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.

Furthermore, this scenario enables the combination of multiple data that, on its own, may provide little information about the data subject. Some of the data may even be anonymized. However, **their combination often ends up creating a new scenario**, in

31 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

which personal data and particularly special categories of personal data. **These are usually called inferred data**, that is, "any personal data which have been created by the data controller as part of the data processing, e.g. by a personalization or recommendation process, by user categorization or profiling made on the basis of the personal data provided by the data subject (observed or raw data)[32]. They **are also personal data, which means that they are subject to the GDPR and the applicable data protection regulation**.

3.1 Automated processing of personal data, profiling, automated decision making: understanding the differences

A controller needs to distinguish between all these concepts, since they have different legal implications. They are clearly connected, but not at all equivalent, and the main legal outcome relates to whether certain processing falls within article 22 GDPR or not.

Indeed, casuistry can be very diverse: there can be automated data processing without profiling; however, profiling can also support for automated decision-making processes; moreover, profiling might serve as a basis for fully automated decision processes; but automated decision processes can be done with or without prior profiling. For instance, not every automated processing of personal data implies that profiling is taking place. Moreover, creating a user profile does not always involve profiling. A user profile may include information like username and observed characteristics without creating or inferring new data, or linking knowledge to a person derived from other data or analytics processes.

The next table shows the differences between these concepts[33]:

Concept	Definition	Example
Automated processing of personal data	The GDPR applies to "the processing of personal data wholly or partly by automatic means, as well as to the processing otherwise than by automatic means of personal data contained in or intended to be contained in a filing system" (article 2 GDPR).	Processing performed by photo cameras that impose fines related to exceeding the speed limit. Storing data in an Excel form allowing to automatically sort it by date, name, etc.
Profiling	It is defined by the GDPR as "consisting of the use of personal data to evaluate certain personal aspects	The photographs made by the photo cameras are included in a file corresponding to the driver

32 A29WP, Guidelines on the right to data portability, at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/right-data-portability_en

33 This table has been built on the basis of the distinctions made by Jorge García here: https://jorgegarciaherrero.com/decisiones-automatizadas-profiling-inteligencia-artificial-que-son/#De_que_hablamos_cuando_hablamos_de_profiling_en_que_se_diferencia_el_profiling_de_las_decisiones_automatizadas_del_art_22

	relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements " Profiling consists of three elements: -automated data processing; - personal data; and -its purpose must be to evaluate personal aspects about a natural person.	suffering the fine. These are used to toughen penalties for repeat offenses or bad driving habits.
Fully automated decision processes of Article 22 of the GDPR.	These are decisions taken and executed without decisive human intervention, with legal effects or which significantly affect in a similar way the data subjects.	The camera system is designed to trigger the automatic sending of a personalized sanction based on the history of sanctions, behavior of the offender prior to the sanctioned action, age of the vehicle, average speed of the other drivers at that time, etc.

3.2 Have a good knowledge of the legal framework regarding profiling

Profiling has been defined in Art. 4 GDPR as "any form of automated processing of personal data that involves the use of personal data to evaluate specific aspects of an individual, in particular to analyze or predict aspects relating to that individual's professional performance, financial situation, health, personal preferences, interests, reliability, behavior, location or movements".

In principle, **profiling can bring users important benefits**, since it could increase the efficiency of the system, save resources or help provide a better service. For instance, profiling by a smart TV could help us find out series that match well with our preferences without spending a lot of time looking for them on our own. However, it is also clear that it could serve for more obscure, discriminative purposes, which involve significant risks for individuals' rights and freedoms" and can "perpetuate existing stereotypes and social segregation" absent appropriate safeguards.

Caution regarding profiling should be specially adopted when controllers start mixing data. **The alignment of different types of personal data can reveal sensitive information about individuals.** Sometimes these processes even end up processing personal data of special categories in an unnoticed way. For instance, mixing non-

special categories of data such as data about preferences, location and social media connections may allow to infer with a high degree of success the sexual orientation of individuals or their religious believes. This may happen without the awareness of the individuals. Needless to say, these consequences should be carefully avoided.

In order to address these issues, AI developers should have a good knowledge of article 22 GDPR. This clause states that "data subjects shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them." On this basis, there are some important considerations to be made.

- First, the prohibition on "fully automated decision-making" only applies when the decision based on such technology "**has a legal effect on or similarly significantly affects someone**." The EDPB guidelines cite as examples of this: the rejection of a selection process, the denial of credit or insurance, or the application of different prices to the same group. It is not necessary that it affect a large number of people. In other situations, assessing whether the fully automated decision-making process creates significant effects may not always be clear to the controller. In these cases, we recommend getting advice from the DPO.
- Second, one must keep in mind that t**here is no "decision based solely on automated processing" if the decision is reviewed by a human being who "takes account of other factors in making the final decision"**. If a human being only ratifies what a tool states, this would not count as human intervention as such. The human element must have power enough to rectify the recommendation by the tool. Some factors to assess this could be the amount of times where the human deviates from the automated recommendation, whether the person has autonomy within the organization to make the decision, and which other factors are taken into account by the person that are not included in the automated model.

Box 6: Profiling negative effects and inferential analytics

Possible ways of monitoring and profiling that can lead to privacy and discrimination issues in IoT systems:

- profiling through data inference, whether on the basis of those primarly provided by data subjet or other sources of data (e.g. Internet browsing behavior);
- profiling through linking IoT datasets;
- profiling that occurs when data is shared with third parties that combine data with other datasets (e.g. product supliers, technical support).

- Furthermore, article 22(2) introduces some exceptions to this general ban of profiling or automated decision-making. Indeed, the Guidelines published by the A29WP declare that **the ban does not apply if the profiling or automated decision making is necessary for entering into, or performance of, a contract between the data subject and a data controller;** authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to protect the data subject's rights and freedoms and legitimate interests (technical and

organizational measures, safeguards, etc.); or is based on the data subject's explicit consent. That is, in these three circumstances, fully automated decision-making processes are allowed. For instance, a service consisting on offering personalized media content based on your declared preferences and consumption data, will necessarily require profiling. If the "necessity" can be proven, fully automated profiling will be permissible.

Therefore, profiling or automated decision-making can be acceptable if any of these circumstances apply, provided that processing does not contravene the data protection regulation in any other possible way. However, even in these cases, additional actions should be embedded. IoT developers should be especially careful if they are dealing with special categories of data inferred by the systems. Article 22(4) contains limitations as regards the use of special categories of data for fully automated decision making or profiling. In this case, art. 22 needs to be applied in accordance with art. 9 GDPR. Specifically, when dealing with special categories of data, fully automated decisions are only allowed with the explicit consent of the data subject (art. 9(1) (a)) or for reasons of substantial public interest, based on existing legislation (art. 9(1) (g)). For instance, a controller wishes to create citizens' profiles to infer the chances of getting a virus and prevent a pandemic. For that purpose, different sources of data are to be mixed, including health data. This could be considered necessary for the protection of a substantial public interest. In addition, there needs to be EU or national legislation allowing for this processing. If all these circumstances are met, art. 9(2) (g) is applicable, and therefore the controller may fall under the art. 22(4) exception allowing for this fully automated profiling.

In any case, all other obligations and guarantees need to be fulfilled. For instance, information obligations, assessment of a DPIA, etc. Furthermore, art. 22(3) contains additional guarantees that need to be observed when taking certain fully automated decisions, such as the right to obtain human intervention, to express the data subject's point of view and to contest the decision. The data subjects should be made aware of all this information and the corresponding rights and actions that they could embed.

Box 7: Inferring data. Example

"Company X has developed an application that, by analyzing raw data from electrocardiogram signals generated by commercial sensors commonly available for consumers, is able to detect drug addiction patterns. The application engine can extract specific features from ECG raw data that, according to previous investigative results, are linked to drugs consumption. The product, compatible with most of the sensors on the market, could be used as a standalone application or through a web interface requiring the upload of the data. Most likely, explicit consent will be the best suitable lawful basis for this processing."

Source: 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.

As mentioned before, the process of profiling is "often invisible to the data subject. It works by creating derived or inferred data about individuals. Individuals have differing levels of comprehension and may find it challenging to understand the complex techniques involved in profiling and automated decision-making processes."[34]

3.3 Introducing safeguards and minimizing risks

Fully automated decision-making and profiling are sensitive processing activities that need to be taken with caution. Controllers must be aware of this and act accordingly in order to identify risks, reduce them, and implement safeguards and guarantees.

We have just mentioned the existence of data subjects' rights linked to these processed and recognized in article 22(3), namely, the right to obtain human intervention, to express the data subject's point of view and to contest the decision.

In addition, controllers must inform in a simple but transparent and complete way of the existence on automated processes and profiling activities when they fall under the definition of article 22 GDPR. Information must also extend to an explanation of the logic involved in the process and the existence of the above-mentioned rights.

The information about the logic of a system and explanations of decisions should give individuals the necessary context to decide whether, and on what grounds, they would like to request human intervention. In some cases, insufficient explanations may prompt individuals to resort to other rights unnecessarily. Requests for intervention, expression

34 Article 29 Working Party (2017) Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679. Adopted on 3 October 2017 as last Revised and Adopted on 6 February 2018. European Commission, Brussels, p.9. Available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

of views, or contests are more likely to happen if individuals do not feel they have a sufficient understanding of how the decision was reached.[35]

Furthermore, Article 35(3) (a) GDPR states the obligation for the controller to carry out a DPIA in the case of a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person. Controllers should be aware that, now, each country has submitted their lists of when a DPIA is required to the EDPB. If the controller is within the EEA, this list should also be locally verified.[36] (see "DPIA" in "Main Tools and Actions", Part II of these Guidelines and see section "Data protection Impact Assessment" within this part on IoT).According to Article 37(1) (b) and (5) GDPR, controllers shall designate a data protection officer where "the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale".

Controllers are also required to keep a record of all decisions made by an AI tool as part of their accountability and documentation obligations. This should also include whether an individual requested human intervention, expressed any views, contested the decision, and whether a decision has been altered as a result[37] (see the "Accountability" section in the "Principles" within Part II of these Guidelines). Some additional actions that might be extremely useful to avoid automated decision-making are as follows:[38]

- Consider the system requirements necessary to support a meaningful human review **from the design phase.** Particularly, the interpretability requirements and effective user-interface design to support human reviews and interventions. This can indeed be considered a binding obligation to controllers in compliance with the data protection by design principle.

- Design and deliver appropriate training and support for human reviewers. This should include an understanding of which variables the decision-making or profiling model is built on, and specially, which variables are not taken into account in the model. These can be key to spot specificities in a data subject that make them an outlier on the model or whose circumstances account for a different decision.

- Give staff the appropriate authority, incentives and support to address or escalate individuals' concerns and, if necessary, override the AI tool's decision. For instance, where human reviewers face organizational pressures or negative professional

35 ICO (2020) Guidance on the AI auditing framework - draft guidance for consultation. Information Commissioner's Office, Wilmslow, p.94. Available at: https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf.

36 EDPB (2019) Data Protection Impact Assessment. European Data Protection Board, Brussels. Available at: https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_es .

37 ICO (2020) Guidance on the AI auditing framework - draft guidance for consultation. Information Commissioner's Office, Wilmslow, p.94-95. Available at: https://ico.org.uk/media/about-the-ico/consultations/2617219/guidance-on-the-ai-auditing-framework-draft-for-consultation.pdf .

38 Ibid, p.95.

consequences if they deviate from the automated decision, such authority and independence will be put at risk.

Checklist: Automated decision-making and profiling

- The controller informs 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.
- The controllers 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.
- The controllers 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.
- The controllers have performed a DPIA.
- The controllers have consulted a DPO on the processing.
- The controllers have ensured that all guarantees foreseen by Article 22 of the GDPR have been adequately implemented.
- The controllers have ensured that all those intervening in profiling and automatic data processing have been adequately trained on data protection issues.
- The controllers 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 (see subsection "Fairness" within "Lawfulness, fairness and Transparency" in "Main Concepts", Part II of these Guidelines).

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.

Transparency is spelled out in the GDPR as detailed requirements of information that has to be provided by the controller to both, data subjects and supervisory authorities. The focus of transparency is to inform data subjects up-front of the existence of the processing and its main characteristics, according to arts. 12-14. Other information (such as the data about the data subject) is available on request (upon exercise of a right to access or right to data portability, for instance). Data subjects also have to be informed of certain events, most notably data breaches (in the case where the data subject is exposed to high risk). Evidently, transparency is a pre-requisite for detecting and intervening in case of non-compliance (see "Transparency" in the "Lawfulness, fairness and Transparency" within "Main Concepts", Part II of these Guidelines).

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."[39] 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

39 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

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."[40] 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 (see "Transparency", within Part IV (AI) of these Guidelines).

Finally yet importantly, IoT developers shall guarantee transparency by using a number of **complementary tools.** Naming a DPO, who then serves as a single point of contact for queries from data subjects, is an excellent option. Preparing adequate records of processing for the supervisory authorities, or performing DPIAs, are also highly recommended measures to promote transparency. Undertaking analysis that evaluate the effectiveness and accessibility of the information provided to the data subjects helps to ensure the efficient implementation of this principle. Or providing for interoperability among different systems so data subjects are able to exercise portability or providing for easy ways to download one's data and self-exercise a right to access.

4.1 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.[41] 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**

40 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

41 Van Deursen, A. J. A. M., & Mossberger, K. (2018). Any thing for anyone? A new digital divide in internet-of-things skills. *Policy and Internet*, *10*(2), 122–140.

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."[42]

IoT system should be designed in a way that facilitates that preferences and needs of the users are translated to the tool in a distributed, cooperative manner so that appropriate decisions about the resources being controlled are made. Providing active support that allows IoT users benefit from the system is highly recommendable**. Better usability will reduce demand for technical skills, whereas improved comprehensibility will reduce higher-order skills requirements.** This, of course, includes the decision of sharing some data or allowing processing and automated decision-making. Furthermore, if the IoT tool needs to incorporate tools designed by third parties (apps, for instance), the developers should opt for those who work better in order to avoid digital discrimination.

4.2 Avoid biases

Biases create prejudice and discrimination against certain groups or people. Harm can also result from the intentional exploitation of (consumer) biases, or by engaging in unfair competition, such as the homogenization of prices by means of collusion or a non-transparent market. IoT systems could contribute to exacerbate such terrible situation in **two main different ways:** through the incorporation of AI tools in the IoT system that are biased; or by building biased datasets through an inadequate collection the data produced by the data subjects. If the use of these data fuels profiling or automated decision-making, this could bring unacceptable social consequences.

Thus, there are some actions that IoT developers should embed in order to avoid unfair biases provoked by the use of AI. On the one hand, they should only incorporate to their tool devices or AI tools that can demonstrate a lack of biases. Tools such as ethical algorithmic auditing should be implemented to flag up discrimination. Internal auditing schemes should be considered to guard against discrimination of protected groups, but also to protect victims of unanticipated discrimination.[43] On the other hand, the IoT system should be designed in a way that automated decision-making based on the data gathered is able to avoid biases. This could be done by using the tools that are generally used in AI to this purpose (see the section "Fairness" in Part IV on AI of these Guidelines).

42 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).

43 Wachter, Sandra, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, Volume 34, Issue 3, 2018, pages 436-449.

It is important to mention that IoT might also cause serious biases due to **inaccuracies** provoked by the way in which these systems work. For instance, data subjects might provide incorrect data or might not fully understand the consequences if their behavior is constantly monitored. This may cause a breach of the accuracy principle when the situation could have been prevented or solved by the controller had it been taken into account. Similarly, data processing can also lead to unexpected biases because potential relationships between data categories, revealed only through aggregation and linkage of disparate datasets, may not be known at the time of data collection. It might happen that if the systems uses such data for profiling, inaccuracies might bring to biased recommendations, for instance. In order to avoid such scenario, critical assessment of the provenance of data is required. To this purpose, organizational 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 a record is accurate).

4.3 Provide adequate information so as to ensure transparency

IoT systems are usually complex tools that process many personal data in connection with other IoT systems or by tools incorporated to the device. This creates a complex scenario, since, as the Article 29 WP stated, "interaction between objects, between objects and individuals' devices, between individuals and other objects, and between objects and back-end systems will result in the generation of data flows that can hardly be managed with the classical tools used to ensure the adequate protection of the data subjects' interests and rights."

Controllers must be aware that, even though it might be hard to reach, data subjects must be able to understand how, and for what purpose, the IoT system uses their personal data to function and come to its decisions. In general, this means that **IoT developers should incorporate in the system features able to provide such knowledge in the easiest possible way**. Explainability –that is, the ability to explain the technical processes of an IoT system and the logics of the decision it makes- is key in the case of IoT, especially if it incorporates an AI tool (see the section "Transparency" in the "AI Requirement for Innovators and Developers", Part IV of these Guidelines").

In this regard, the Article 29 Working Party stated that "The methods for giving information, offering a right to refuse or requesting consent **should be made as user-friendly as possible.** In particular, information policies must focus on information that is understandable by the user and should not be confined to a general privacy policy on the controllers' website.[44] In this regard, controllers must take into account the specificities of the IoT device, in light of issues like small screens that may turn read privacy policies almost impossible, or even the total lack of screens. Dual-layer schemes could be particularly useful when dealing with the scenarios in which the amount of information and its complexity is hard to handle. A first layer providing the user with the essential information and a second layer with more in-deep information and explanations seems reasonable.

44 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

In general, IoT systems should be able to provide a panoramic overview of "what personal data have been disclosed to what data controller under which policies; provide online access to the personal data and how they have been processed; and provide counter profiling capabilities helping the user to anticipate how their data match relevant group profiles, which may affect future opportunities or risks".[45] If the controller "plans" to carry out a processing for purposes other than those for which the data were collected, they must inform users or data subjects beforehand of such further processing, providing information and comply with all other requirements, such as having a legal basis for this new purpose or carrying out a compatibility assessment. Based on the above obligations, and applying them specifically to IoT, a first layer of information must be provided to users before they start using the device. Additionally, information requirements state that full information must be provided before the processing starts, so users must have a way to access it before register or access the IoT device.

According to the GDPR, the information that an IoT system must provide to the data subjects varies depending on whether this information has been obtained from them or inferred by the system.

- If the data is obtained directly from the data subject (Art. 13 GDPR)

The IoT system controller must inform the user, prior to the processing, about the identity of the controller, the DPO´s contact information, the specific processing purposes; the legal basis for the processing and, if applicable, which are the legitimate interests on which the processing is based on[46], which legal basis apply to each purpose; the recipients or categories of recipients of the data; the existence of international transfers; where applicable, the time limits for storing the data or the criteria used to determine those time limits; how to exercise data subjects' rights and the right to lodge a complaint to the Supervisory Authority; and in the case of automated decisions, including profiling, the controller must provide relevant information about the logic involved and the expected consequences of such processing for the data subject.

- If the personal data is not obtained from the user (Art. 14 GDPR)

In this case, if the personal data are obtained from a third party, the controller of IoT system must inform the user of the provisions of Art. 13 of the GDPR, and communicate the information regarding the origin or source of the data, specifically if they come from publicly accessible sources. In this regard, controllers must bear in mind the concept of "public accessible sources" is not an extensive list but a rather close one, and it does not include social media or the Internet. The information shall be provided within a month 'at the latest' to the IoT user.

45 Weber, Rolf H., 'Internet of Things: Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618, 625; similarly, Tene and Polonetsky (n 18).

46 Bear in mind that, according to recent case law from the Spanish Data Protection Authority, APED, the interests that serve as the ground for the legal basis of art. 6.1.f GDPR would not be the same as the purposes of the processing.

Checklist: fairness and transparency[47]

Fairness

- The controllers have implemented functionalities or easy-to-use control interfaces that allow the management of technical and privacy settings
- The IoT systems have been designed in a way that facilitates that preferences and needs of the users are translated to the tool in a distributed, cooperative manner so that appropriate decisions about the resources being controlled are made
- The controllers have implemented adequate measures to avoid biases provoked by the use of AI tools.
- The controllers have implemented measures to avoid collecting biased datasets

Transparency

- The IoT systems provide:
  - a panoramic overview of what personal data have been disclosed to what data controller 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.
- If the personal data were directly provided by the data subject, the controllers provided all the information enlisted in Article 13 GDPR.
- If the personal data were not provided by the data subject, the controllers provided all the information enlisted in Article 14 GDPR.
- If the personal data is directly provided by the data subject, the information is provided before the processing and, at the latest, at the time it is collected from the data subject.
- If the personal data is not provided by the data subject, the information is provided:
  - 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.
- The information is provided concisely, transparently, intelligibly, and in an easily accessible way. It is clear and redacted in plain language.
- The controllers have documented all the information regarding these issues.

[47] Not all these requirements are legal requirements *strictu sensu*, but they can all be considered as ethical requirements.

5 Data governance: minimization, purpose limitation and storage limitation principles

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. On the other hand, according to Article 5(1) (e) of the GDPR, personal data should be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". Finally, purpose limitation means that personal data cannot be processed for purposes other than the ones stipulated in the privacy policy when the data were collected, unless these purposes correspond to archiving activities of public interest, purposes of scientific and historical research or statistical purposes.

The combination of these three principles creates a combined normative tool that must be strictly followed by IoT developers. In general, data controllers[48] must make the purposes of the processing explicit: "disclosed, explained or expressed in an intelligible form". In line with the principle of data minimization, they should also identify the minimum amount of personal data needed to achieve their objectives. In addition, in respect of the accountability principle, data controllers should be able to demonstrate that they only collect and hold the personal data needed and that it is used solely for the specific purposes that have been informed under an adequate legal basis.

Summarizing, setting clear objectives of an IoT development will help ensure that the personal data to process be:

- adequate: sufficient to fulfil the stated purpose;
- relevant: as they should have a rational link to the purpose;
- limited to what is necessary: they should not hold more data than those needed for the stated purpose.

Controllers shall not forget that, if the devices will process data for purposes other than those for which they were collected, a legal basis that legitimizes such processing will be needed, unless the new use of data is compatible with the purpose for which the personal data were initially collected, according to article 6.4 GDPR. The possibility to make use of the exception to this rule linked to processing for research purposes should be carefully analyzed before any processing. Consultation with the DPO is highly recommended.

48 it is important to identify who the "data controller" is; developers are rarely the "data controller", since they are no responsible to take care of the business objective, this is a task for the management of the company.

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 (see "Data minimization", in the "Principles" section in Part II of these Guidelines). In simple terms, it would mean reducing as much as possible the amount, categories and granularity of personal data that processed. This means that it will not be possible to collect personal data that are not going to be processed simply so that the controller can have them and use them in the future, either for the declared purposes or new ones. 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**. "Since the possibility to build extensive personal profiles can be hardly avoided, data anonymization is important in the context of data sharing."[49] In principle, this seems feasible, but in practice, it might be hard to reach. As the AEPD stated, "Linking IoT devices to unique identifiers, lined to the close links between certain devices and its users, make it virtually impossible to use such data anonymously, and the risk of re-identification skyrockets. For example, many devices require user registration or include advertisement unique identifiers, such as smart televisions. Linking unique identifiers in mobile devices is a proven fact, and such devices are widely used to interact with and operate IoT devices."[50] Thus, **controllers should not presume that their anonymization processes would serve well to preserve data subjects' privacy. Indeed, they should perform DPIAs and risk assessments to ensure such belief (see accountability in this part of the Guidelines)**.

In this regard, controllers must be aware that capturing personal data that is then made anonymous accounts for processing of personal data, until such data has finished the anonymization process, no matter how little that time lapse is. Moreover, anonymization is processing, which means that it can only be lawful if a legal basis applies. Legitimate interest or consent are the most promising candidates. Once the data has been made anonymous, the processing must no longer comply with the personal data protection requirements. It may still fall under e-Privacy rules, but still in a more diluted way.

An alternative to anonymization as such is the use of **aggregated data (sometimes aggregation is considered an anonymization tool)**. This should be reachable in most IoT systems, since most of the data values we deal with are a form of aggregation, even if this may not be evident since it may be done "invisibly" by some sensor or data

49 Rolf H Weber, 'Internet of Things: Privacy Issues Revisited' (2015) 31 Computer Law & Security Review 618.

50 AEPD, "**IoT (I): What is IoT and which risks does it entail", at: https://www.aepd.es/en/prensa-y-comunicacion/blog/iot-%20and-which-risks-does-it-entail**

collection method. Aggregation is a way of **substituting several data elements by a single one**. Prime examples come from statistics and include the average, median, minimum, and maximum. In the context of data protection, two kinds of aggregation have to be distinguished (see "Data minimization" within "Principles", Part II of these Guidelines):

- Aggregation of data elements pertaining to a **single person**: Taking for example a person's average monthly income over a year reduces the information content pertaining to that person.
- Aggregation of data elements pertaining to a **multitude of persons**: Taking for example the average yearly income over group of people also reduce the overall information content (data minimization). In addition, it also weakens the degree of association between a data element and a given person. This kind of aggregation is therefore also pertinent to storage limitation.

When the purpose can be achieved using aggregated data, this should be implemented. Under such circumstances, no one but the data subject should access the raw data, unless a relevant reason applies. The transformation of raw data into aggregated data should be possible in the IoT tool, so as raw material leaving the device remains the minimal strictly needed. These aggregated data should be in a standardized format."[51] In any ways, controllers must be aware of the fact that collecting data and deleting it after a small amount of time, even milliseconds, still constitutes processing of personal data and full compliance with data protection rules is required.

If the purpose of the processing can only be obtained by processing personal data, such data can still be made pseudonymous. This will still fall under data protection and privacy rules, but accounts as a good security measure and enhances accountability.

An important topic to highlight if the fact that a controller must not create, collect and store data "just in case". That is, data stored for the case that a future new idea comes which requires such data to develop a different project. In this case, the storage of data for longer than necessary and the repurposing of data in unlawful ways can trigger the highest fines.

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."[52]

5.2 Purpose limitation

The purpose limitation principle (see the "Purpose limitation" section within "Principles", Part II of these Guidelines) requires that personal data collected and processed in the context of IoT are processed only for the purpose for which the data were collected.

51 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.

52 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.

The data controller can only use the data for those purposes or objectives that have been clearly and explicitly notified to the users in the privacy policy. Non informed purposes of data will not be legitimate, and even poorly informed ones. For instance, when the information provided is not transparent or complete, it can be argued purposes were not made explicit.

In addition to that, purposes need to be specified. That is, a wide and open wording that does not allow an average person to understand all and every purpose of the data, will fall out of the law.

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." [53] 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. 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 obligates 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 when identification is no longer than necessary for such purposes. The problem here is that controllers might be interested in storing data more data than necessary, for longer periods than necessary to ultimately use the stored data for different purposes. Furthermore, as mentioned, sometimes they are collected and stored "just in case" they might serve for unforeseen uses.

Therefore, storage periods should be proportionate to the aims of the processing: "In order to define storage periods (timelines), criteria such as the length and the purpose of the research should be taken into account. It has to be noted that national provisions may stipulate rules concerning the storage period as well."[54]

53 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 .

54 EDPS (2020) Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak Adopted on 21 April 2020. European Data Protection Supervisor, Brussels, p.10. Available at https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (accessed 23 April 2020).

Controllers should be aware that even though the GDPR allows storage for longer periods, although **there should be a good and real reason to opt for such an extended period,** for instance, when the sole purpose is subsequent scientific research (or the other circumstances mentioned in the close list contained in art. 5.1(c) GDPR like or archiving in the public interest, historical research or statistical purposes) (see the "Data protection and scientific research" section in the "Main Concepts" and the "Temporal aspect" subsection in the "Storage limitation" section of the "Principles", Part II of these Guidelines).

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".[55]

To sum up, if controllers do not need the data, and there are no compulsory legal reasons that oblige them to conserve the data, they must fully anonymize or delete them. Researchers should consult their DPOs if they are willing to storage data for a long-lasting period and be aware of the applicable national regulation. This could also be an excellent moment to **envisage time limits for erasure of the different categories of data and document these decisions or apply them in an automated manner** (see the "Accountability" section within "Principles", Part II of these Guidelines).

Checklist: data governance

Minimization

- The IoT systems use of anonymized data, especially if those data are shared with other devices, whenever possible.

- If anonymizations is not possible, the IoT systems opt for the aggregation of data in a standardized format.

- The controllers have ensured 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).

- The controllers have ensured that raw material leaving the device remains the minimal strictly needed.

Purpose limitation

55 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

- The controllers only use the data for the purposes they were collected, unless a legal basis allows their processing unlawful processing by third parties.

- The controller transparently informs about such purposes and which legal basis will support each of them.

Storage limitation

- Controllers do not store personal data for 'longer than is necessary for the purposes for which the personal data are processed', according to the Necessity Toolkit by the EDPS[56].

- Controllers check the utility of the stored data for the intended purpose of a particular product or service will need to be periodically reassessed.

- 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.

- Information deleted by users in their account is not retained by the IoT system.

- 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.

- The user is notified before these steps are taken.

- The controllers have documented all the information regarding these issues.

6 Data subjects rights

Chapter III of the GDPR provides for a set of rights that the data subjects can exercise to safeguard their personal data. Although each right has specific details and issues that could affect and be affected by ICT research and development (see the section "Processing for scientific research" in "Main Tools and Actions", Part II of these Guidelines) they all share some general features concerning their transparent information, communication and modalities of exercise (Article 12 GDPR). In this section, we analyze each specific right in the light of an IoT system development. We have already analyzed the right to information (see the Transparency section of this part of the Guidelines) and the right not to be subject to automated decision-making has been extensively addressed in the "Human Agency" section of this part of the Guidelines.

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

[56] https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en

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."[57]In addition, some parties may draft contracts positioning themselves in a different role than what really applies to them (see "Define the data protection roles played by all agents involved in the processing: determination of controllers and processors" section in this part on IoT)

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.[58] 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 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.[59]

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.[60]

57 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.

58 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

59 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

60 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).

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 (see section "right of access" in the "Data subject rights" in Part II of these Guidelines). Additionally, upon the data subjects' request, the data controller must provide them with a copy of the personal data being processed, without charge (reasonable fees to cover administrative costs could be charged for any further copies requested by the data subject). 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.

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". [61]

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.

Furthermore, the right to access is currently closely related to the right to data portability (see the "right to data portability" below, within this part on IoT).

6.2 Right to rectification

As laid down in Article 16 GDPR, data subjects hold the right to have their personal data rectified (see the section "Right to Rectification" in the "Rights" part of these Guidelines). This is particularly relevant in the case of IoT, since any inaccuracy in the collected data might have dramatic consequences in terms of profiling (see the "human agency" section in this part of the Guidelines). 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."[62] 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.

61 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

62 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.

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 (see the section "Right to Erasure" in the "Data subject rights", Part II of these Guidelines). 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 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 (namely: the accuracy of their data is contested; the processing is unlawful and the data subject opposed erasure of their personal data; the controller no longer needs the personal data, but is required to store it; or the data subject otherwise objects to the processing.

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

Data subjects shall have the right to object, on grounds relating to their particular situation, at any time to processing of personal data. This right only applies when the lawful basis for the processing is either legitimate interest or public interest. When the legal basis for processing is consent, the data subjects shall simply withdraw their consent.

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.

In this regard, it is to be noted that those personal data can still be processed for other purposes, as long as there is a lawful basis for them.

6.6 Right to data portability

According to Article 20 GDPR, data subjects have a right to portability. This means a right to obtain their data from a data controller in a structured, commonly used, and machine-readable format, but also a right to move data between data controllers without hindrance, or where technically feasible. However, it only applies to data 'concerning' the data subject and data they 'provided to' the data controller. As a consequence, neither anonymized, inferred or otherwise "created" data are included in the right to portability (anonymized data is not covered since they do not concern the data subject anymore; and inferred data since they have not been provided by the data subject but are the result of a technical process developed by the controller). Thus, it seems data subject to not hold a right to have their full profiled information transferred to another provider. The rationale behind this is the protection of the know-how of the controller.

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."[63]

Checklist: data subjects' rights

- The controllers 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.
- The controllers have introduced the necessary procedures to ensure that the data subject rights are satisfied in time (maximum one month after request).
- The controllers have introduced efficient tools to ensure that data subjects are able to exercise their rights in a practical manner, for instance by introducing data

63 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

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.

- The IoT developers 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.

- The controllers 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.

- The controllers 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.

- IoT developers 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

The accountability principle in the GDPR is risk-based: the higher the risk of data processing to the fundamental rights and freedoms of data subjects, the greater the measures needed to mitigate those risks.[64] (See the section "Accountability Principle" within "Principles" in Part II of these Guidelines). The accountability principle is based on all compliance duties for data controllers, including: transparency duties (Articles 12-14); guaranteeing the exercise of data protection rights (Articles 15-22); keeping records of the data-processing operations (Article 30); notifying eventual data breaches to a national supervisory authority (Articles 33) and to the data subjects (Article 34); and, in cases of higher risk, hiring a DPO and carrying out a DPIA (Article 35).

Since the processing of personal data in IoT systems might often be considered as high risk,[65] the developers of AI will often need to have a DPO and perform a DPIA. Also, controllers should create a Data Protection Policy that allows **the traceability of information.** Finally, if approved codes of conduct exist, these could also be

64 See Articles 24, 25 and 32 of the GDPR, which require controllers to take into account the "risks of varying likelihood and severity for the rights and freedoms of natural persons" when adopting specific data protection measures.

65 See, in particular, Article 35(3)(a), according to which data processing is considered as high risk in cases of, inter alia, "a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person".

implemented (see the "Economy of scale for compliance and its demonstration" subsection in the "Accountability" section of the "Principles" in Part II of these Guidelines).

Box 8: The difficulty of accountability in IoT development

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"[66].

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"[67].

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:2307986,25&cs=1F4A71C19873519CC81C4B2C031CF3CF5

7.1 Data Protection Officer

The appointment of a DPO is one of the best steps that can be taken by the controller to properly implement measures that ensure compliance with the rights of the data subjects. Appointing a DPO is not always a necessary consequence of operating with IoT deployment. It is undeniable, however, that appointing a DPO is compulsory, at least, if conditions settled by Article 37(1) apply. Indeed, in the case of IoT, it will often happen that the core activities of the controller or the processor consist of processing 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. Nevertheless, even if this is not the case, **it is always recommendable to proceed to do so, at least in terms of transparency** (see the "Transparency" section in the "Principles", Part II of these Guidelines)**.**

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.

66 Urquhartet L. *et* al, Demonstrably doing accountability in the Internet of Things, International Journal of Law and Information Technology, 2019, 27, 1–27
67 Ibid.

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 any case, the WP29 included some fundamental criteria in its Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679[68].

In case of doubt, consultation of the competent supervisory authority prior to processing is highly recommended (see the "Data Protection Impact Assessment" section of the "Main Tools and Actions", Part II of these Guidelines).

The CNIL created an excellent tool aimed at providing advice on how to perform a Privacy Impact Assessment[69], which includes a well-designed and practical advice. Consulting it is highly recommended: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

Checklist

- Verify whether you need to conduct a DPIA for your processing activity.
- Document this verification (no matter whether it was affirmative or not).

If a DPIA is necessary:

- Start as early as ever possible (following the principle of Data Protection by Design).
- Get an overview of what a DPIA is.
- Use the guidance and templates provided by the competent Data Protection Supervisory Authority (DPA) where possible.
- If not (your DPA does not provide such material or you have to cater to many areas of competence of different DPAs), follow the guidance provided by the Article 29 Working party in wp248rev.01.
- Assemble the team necessary to conduct the DPIA.
- Consider ways of facilitating your work.

[68] A29WP, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, Adopted on 4 April 2017 As last Revised and Adopted on 4 October 2017, at: https://ec.europa.eu/newsroom/article29/items/611236/en .

[69] CNIL, Privacy Impact Assessment. Application to IoT devices. February 2019. At: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-piaf-connectedobjects-en.pdf

7.3 Prepare the documentation of processing

Controllers must always keep in mind that the development of IoT solutions often involves the use of different datasets. The traceability of the processing, the information about possible re-use of data, and the use of data pertaining to different datasets in different or in the same stages of the life cycle must be ensured by the records, since the controller shall be responsible for, and be able to demonstrate compliance with article 5 of the GDPR (See "Accountability principle" in the "Principles" section of Part II of these Guidelines). Whoever processes personal data (including both, controllers and processors) needs to document their activities primarily for the use of qualified/relevant Supervisory Authorities (see the "Documentation of processing" in the "Main Tools and Actions", Part II of these Guidelines), but also, when appropriate, by data subjects and other stakeholders.

This must be done, among other things, through records of processing activities that are maintained centrally by the organization across all its processing activities, and additional documentation that pertains to an individual data processing activity (see the "Documentation of processing" section in the "Main Tools and Actions", Part II of these Guidelines).

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[70].

Checklist. Documentation

- Contact the office/person who is keeping the records of processing for your organization.
  - If necessary, your Data Protection Officer can help establish the contact.
- Inform them early on that you intend to process personal data.
  - Your processing activity needs to be entered in the records before processing starts.
- Follow their instructions of
  - what information you need to provide for the records of processing,
  - when you need to send updates of this information.

Additional documentation pertaining to a single processing activity).

The following items must be documented:

- Assessment whether the processing activity likely results in a high risk to the

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

rights and freedoms of natural persons.

- A Data Protection Impact Assessment where the above assessment yields an affirmative result.
- Potential consultation of the competent supervisory authority prior to processing.
- Requirements and acceptance tests for the purchase and/or development of the employed software, hardware, and infrastructure.
- Implemented technical and organizational measures.
- Regular testing, assessing and evaluating the effectiveness of technical and organizational measures.
- Requirements and acceptance tests for the selection of processors.
- Contracts stipulated with processors.
- Possible inspections and audits of the processor.
- Method to collect consent.
- Demonstrations of individual expressions of consent.
- Information provided to data subjects.
- Implementation of data subject rights.
- Actual handling of data subject rights.
- Possible breach notifications to the competent supervisory authority.
- Possible communication of data breaches to concerned data subject.
- Any other communication with the competent supervisory authority.

7.4 Design your Privacy Policy

The Privacy Policy is the public document that explains how your 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

Checklist. Privacy Policy

- Contact the office/person who is keeping the records of processing for your organization.
  - If necessary, your Data Protection Officer can help establish the contact.

- Inform them early on that you intend to process personal data.
  - Your processing activity needs to be entered in the records before processing starts.
- Follow their instructions of
  - what information you need to provide for the records of processing,
  - when you need to send updates of this information.

Additional documentation pertaining to a single processing activity.

The following items must be documented:

- Assessment whether the processing activity likely results in a high risk to the rights and freedoms of natural persons.
- A Data Protection Impact Assessment where the above assessment yields an affirmative result.
- Potential consultation of the competent supervisory authority prior to processing.
- Requirements and acceptance tests for the purchase and/or development of the employed software, hardware, and infrastructure.
- Implemented technical and organizational measures.
- Regular testing, assessing and evaluating the effectiveness of technical and organizational measures.
- Requirements and acceptance tests for the selection of processors.
- Contracts stipulated with processors.
- Possible inspections and audits of the processor.
- Method to collect consent.
- Demonstrations of individual expressions of consent.
- Information provided to data subjects.
- Implementation of data subject rights.
- Actual handling of data subject rights.
- Possible breach notifications to the competent supervisory authority.
- Possible communication of data breaches to concerned data subject.
- Any other communication with the competent supervisory authority.

8 Integrity and confidentiality

According to the GDPR, personal data shall be processed in a manner that **ensures appropriate security** of the personal data, including protection against **unauthorized** or **unlawful processing** and against **accidental loss, destruction** or **damage**, using appropriate technical or organizational measures ('*integrity and confidentiality*' principle). (See the "Integrity and confidentiality" section in the "Principles", Part II of these Guidelines).

In practice, this principle involves three main issues: integrity, confidentiality and availability

- Integrity refers to the protection of personal data "against accidental damage", for example due to a transmission error, accidental or unauthorized modification. It thus aims at preventing any kind of event that could "corrupt" the data in any way that renders them unfit for the purposes of processing.

- Confidentiality refers to the protection of personal data "against unauthorized or unlawful processing".

- Availability refers to the protection of personal data "against accidental loss or destruction", for example due to the failure of a storage component.

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).[71] 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.

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.

71 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.

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 (see the "Integrity and confidentiality" section in the "Principles", Part II of these Guidelines). The risk-based approach of data protection law requires controllers to comply with their obligations and implement appropriate measures in the context of their particular circumstances – the nature, scope, context and purposes of the processing they intend to do, and the risks this poses to individuals' rights and freedoms. Their compliance considerations therefore involve assessing the risks to the rights and freedoms of individuals and taking judgements as to what is appropriate in those circumstances. In all cases, controllers need to ensure that they comply with data protection requirements and are able to show how they comply e.g. through documentation (see "Accountability" within "Principles, Part II of these Guidelines).

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.[72] To this purpose, two key factors must be considered:[73]

- 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.

Box 9:

For example, if an IoT application does not guarantee the security of information by means of security measures such as data encryption in the different states that the information goes through, we will be putting security at risk. Additionally, the encryption techniques must use internationally recognized algorithms considered secure and with a sufficiently long key.

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

72 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).

73 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).

in the market, as well as the compliance standards in relation to data protection that will apply to the IoT solution, such as the GDPR for data protection or PCI-DSS for transactions using payment cards. Furthermore, IoT developers should always remember that Article 32(4) GDPR clarifies that an important element of security is to ensure that employees accessing the data act only on instruction and as instructed by the controller (see the "Integrity and confidentiality" section of the "Principles" in Part II of these Guidelines).

Box 10:

For example, if the application includes a module to manage banking or payment data using credit/debit cards, it is necessary to take into account the standard PCI DSS. Additionally, if it is going to handle and process personal data it must be adapted to the regulatory framework operating in the territory, such as the GDPR in the European Union.

Some risk assessment mythologies already available:

- CNIL: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf
- ISO: ISO/IEC 29134

The general description of the technical and organizational security measures must become a part of the records of processing, where possible (Article 30(1) (g) for controllers, and 30(2) (d) for processors) and all implemented measures are part of the DPIA, as supporting remediation measures to limit risk. Finally, once the selected measures are implemented, the remaining residual risks should be assessed and kept under control. Both the risk analysis and the DPIA are the tools that apply.

As stated in the requirements and acceptance tests for the purchase and/or development of the employed software, hardware, and infrastructure, the risk evaluation and the decisions taken "have to be documented in order to comply with the requirement of data protection by design" (of Article 25 of the GDPR) (see "Data Protection by Design and by Default" section in the "Main Concepts" section, Part II of these Guidelines).

Finally, the controllers should always be aware that, according to Article 32(1) (d) of the GDPR, data protection is a process. Therefore, **they should test, assess, and evaluate the effectiveness of technical and organizational measures regularly**. Procedures that serve controllers to identify changes that would trigger the revisit of the DPIA should be created at this moment. Whenever possible, controllers should try to impose a dynamic model of monitoring the measures at stake (see the "Integrity and confidentiality" section in the "Principles" Part II of these Guidelines)

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 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.

Box 11:

An IoT application that makes it possible to control lightbulbs remotely from a mobile device, supported by wireless communications by means of the protocol or specification Zigbee, and that at the same time uses a gateway to connect to the Internet, can be a useful example of the key aspects for consideration for the functionality mentioned above.

Checklist: data subjects' rights

 The controllers 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.

 The controllers have introduced the necessary procedures to ensure that the data subject rights are satisfied in time (maximum one month after request).

 The controllers 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

 The IoT developers 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

 The controllers 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.

 The controllers 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.

 The controllers have ensured that withdrawal schemes should be fine grained and should cover:

(1) any data collected by a specific thing;

(2) a specific type of data collected by anything;

(3) a specific data processing.

 Data subjects are offered the option to disable the "connected" feature of the thing and allow it to work as the original, unconnected item (i.e. disable the smart watch or glasses connected functionality).

 IoT developers have introduced user-friendly interface for users who want to obtain both aggregated data and/or raw data that they still store. These tools enable data subjects to easily export their data in a structured and commonly used format.

 The controllers have documented all the information regarding these issues.