ARTICLE 29 DATA PROTECTION WORKING PARTY

14/EN
WP 223

Opinion 8/2014 on the on Recent Developments on the Internet of Things

Adopted on 16 September 2014

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

Having regard to Articles 29 and 30 thereof,

Having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION:

SUMMARY

The Internet of Things (IoT) is on the threshold of integration into the lives of European citizens. The viability of many projects in the IoT still remains to be confirmed but "smart things" are being made available which monitor and communicate with our homes, cars, work environment and physical activities. Already today, connected devices successfully meet the needs of EU citizens on the large-scale markets of quantified self and domotics. The IoT thus hold significant prospects of growth for a great number of innovating and creative EU companies, whether big or small, which operate on these markets.

The WP29 is keen that such expectations are met, in the interests of both citizens and industry in the EU. Yet, these expected benefits must also respect the many privacy and security challenges which can be associated with the IoT. Many questions arise around the vulnerability of these devices, often deployed outside a traditional IT structure and lacking sufficient security built into them. Data losses, infection by malware, but also unauthorized access to personal data, intrusive use of wearable devices, or unlawful surveillance are as many risks that stakeholders in the IoT must address to attract prospective end-users of their products or services.

Beyond legal and technical compliance, what is at stake is, in fact, the consequence it may have on society at large. Organisations which place privacy and data protection at the forefront of product development will be well placed to ensure that their goods and services respect the principles of privacy by design and are equipped with the privacy friendly defaults expected by EU citizens.

For now, this analysis has only been stated in very general terms by a number of regulators and stakeholders, in the EU and elsewhere. The WP29 has decided to take the issue further by adopting this opinion. In this way, it intends to contribute to the uniform application of the legal data protection framework in the IoT as well as to the development of a high level of protection with regard to the protection of personal data in the EU. Compliance with this framework is key to meeting the legal, technical but also, since it relies on the qualification of data protection as a fundamental human right, the societal challenges described above.

Thus, this opinion identifies the main data protection risks that lie within the ecosystem of the IoT before providing guidance on how the EU legal framework should be applied in this context. The Working Party supports the incorporation of the highest possible guarantees for individual users at the heart of the projects by relevant stakeholders. In particular, users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific. To help them meet this end, the Working Party designed a comprehensive set of practical recommendations addressed to the different stakeholders concerned (device manufacturers, application developers, social platforms, further data recipients, data platforms and standardisation bodies) to help them implement privacy and data protection in their products and services.

Indeed, empowering individuals by keeping them informed, free and safe is the key to support trust and innovation, hence to success on these markets. The Working Party firmly believes that stakeholders meeting such expectations will hold an exceptionally strong competitive advantage over other players whose business models rely on keeping their customers unaware of the extent to which their data is processed and shared and on locking them into their ecosystems.

Considering the major data protection challenges raised by the IoT, the WP29 will keep monitoring its developments. To this end, it remains open to cooperation with other national or international regulators and lawmakers on these issues. It also remains open to discussion with representatives of

the civil society as well as of the relevant industry in particular where those stakeholders are operating as a data controller or data processor within the EU.

INTRODUCTION

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. 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.

IoT stakeholders aim at offering new applications and services through the collection and the further combination of this data about individuals – whether in order to measure the user's environment-specific data "only", or to specifically observe and analyse his/her habits. In other words, the IoT usually implies the processing of data that relate to identified or identifiable natural persons, and therefore qualifies as personal data in the sense of article 2 of the EU Data Protection Directive.

The processing of such data in this context relies on the coordinated intervention of a significant number of stakeholders (i.e. device manufacturers – sometimes also acting as data platforms; data aggregators or brokers; application developers; social platforms; device lenders or renters, etc.). The respective roles of these stakeholders will be considered further in the opinion. These different stakeholders may be involved for various reasons, namely to provide additional functionalities or easy-to-use control interfaces that allow the management of technical and privacy settings, or because the user will commonly have access to his/her collected data is via a distinct web interface. Furthermore, once the data is remotely stored, it may be shared with other parties, sometimes without the individual concerned being aware of it[1]. In these cases, the further transmission of his/her data is thus imposed on the user who cannot prevent it without disabling most of the functionalities of the device. As a result of this chain of actions, the IoT can put device manufacturers and their commercial partners in a position to build or have access to very detailed user profiles.

In the light of the above, the development of IoT clearly raises new and significant personal data protection and privacy challenges[2]. In fact, if uncontrolled, some developments of the IoT could go as far as develop a form of surveillance of individuals that might be considered as unlawful under EU law. The IoT also raises important security concerns, as security breaches can entail significant privacy risks for the individuals whose data are processed in such contexts.

The WP29 has therefore decided to issue the present Opinion in order to contribute to the identification and the monitoring of the risks derived from those activities, where the fundamental rights of citizens of the EU are at stake.

[1] http://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf

[2] This opinion should also be read in connection with previous opinions adopted by the Working Party in 2014, namely its opinions on the application of the concepts of necessity and proportionality and data protection in law enforcement (WP211) and on surveillance (WP 215)

1. Scope of the opinion: specific focus on three IoT developments

At this stage, the extent to which the IoT will develop is impossible to predict with certainty. This is in part because the question of how the transformation of all the data possibly collected in the IoT into something useful, and hence commercially viable, remains largely open. Also unclear are the possible convergence and synergies of the IoT with other technological developments such as cloud computing and predictive analytics, which, at this stage, concern only emerging market developments.

The WP29 has therefore decided to essentially focus in this Opinion on three specific IoT developments (Wearable Computing, Quantified Self and domotics) which (1) are directly interfaced to the user and (2) correspond to devices and services that are actually in use, thus actually lending themselves to an analysis under data protection laws. This Opinion thus does not deal specifically with B2B applications and more global issues like "smart cities", "smart transportations", as well as M2M ("machine to machine") developments. Yet, the principles and recommendations in this Opinion may apply outside its strict scope and cover these other developments in the IoT.

1.1 **Wearable Computing**

Wearable Computing refers to everyday objects and clothes, such as watches and glasses, in which sensors were included to extend their functionalities. Wearable things are likely to be adopted quickly as they extend the usefulness of everyday objects which are familiar to the individual – all the more so as they can hardly be differentiated from their unconnected lookalikes. They may embed cameras, microphones and sensors that can record and transfer data to the device manufacturer. Furthermore, the availability of an API for wearable devices (e.g. Android Wear[3]) also supports the creation of applications by third parties who can thus get access to the data collected by those things.

1.2 **Quantified Self**

Quantified Self things are designed to be regularly carried by individuals who want to record information about their own habits and lifestyles. For example, an individual may want to wear a sleep tracker every night to obtain an extensive view of sleep patterns. Other devices focus on tracking movements, such as activity counters which continuously measure and report quantitative indicators related to the individual's physical activities, like burned calories or walked distances, among others.

Some objects further measure weight, pulse and other health indicators. By observing trends and changes in behaviour over time, the collected data can be analysed to infer qualitative health-related information including assessments on the quality and effects of the physical activity based on predefined thresholds and the likely presence of disease symptoms, to a certain extent.

Quantified Self sensors are often required to be worn in specific conditions to extract relevant information. For example, an accelerometer placed at the belt of a data subject, with the appropriate algorithms, could measure the abdomen moves *(raw data)*, extract information about the breathing rhythm *(aggregated data and extracted information)* and display the level of stress of the data subject *(displayable data)*. On some devices, only this latter information is reported to the user but the device manufacturer or the service provider may have access to much more data that can be analysed at a later stage.

Quantified Self is challenging with regard to the types of data collected that are health-related, hence potentially sensitive, as well as to the extensive collection of such data. In fact, since this movement

[3] http://developer.android.com/wear/index.html

focuses on motivating users to remain healthy, it has many connections with the e-health ecosystem. Yet, recent investigations have challenged the real accuracy of the measures and of the inferences made from them[4].

1.3 **Home automation ("domotics")**

Today, IoT devices can also be placed in offices or homes such as "connected" light bulbs, thermostats, smoke alarms, weather stations, washing machines, or ovens that can be controlled remotely over the internet. For instance, things containing motion sensors can detect and record when a user is at home, what his/her patterns of movement are, and perhaps trigger specific pre-identified actions (e.g. switching on a light or altering the room temperature). Most home automation devices are constantly connected and may transmit data back to the manufacturer.

Obviously, domotics raise specific data protection and privacy challenges as an analysis of usage patterns in such a context is likely to reveal the inhabitants' lifestyle details, habits or choices or simply their presence at home.

The three categories of devices listed above are exemplary of most of the main privacy issues related to the IoT in its current state. It should be noted, however, that these categories are not exclusive: for instance, a "wearable" device like a smart watch could be used for monitoring heart rate, i.e. for Quantified Self assessment.

2. Privacy and data protection challenges related to the Internet of Things

The WP29 decided to issue this specific Opinion upon the consideration that IoT poses a number of significant privacy and data protection challenges, some new, some more traditional, but then amplified with regard to the exponential increase of data processing involved by its evolution. The importance of applying the EU data protection legal framework and the practical corresponding recommendations below must be viewed in the light of these challenges.

2.1 **Lack of control and information asymmetry**

As a result of the need to provide pervasive services in an unobtrusive manner, users might in practice find themselves under third-party monitoring. This may result in situations where the user can lose all control on the dissemination of his/her data, depending on whether or not the collection and processing of this data will be made in a transparent manner or not.

More generally, 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. For instance, 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. Also, 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

[4] http://bits.blogs.nytimes.com/2014/04/27/for-fitness-bands-slick-marketing-but-suspect-results

more challenging when one thinks that these different emerging technologies can be used in combination.

2.2 **Quality of the user's consent**

In many cases, the user may not be aware of the data processing carried out by specific objects. Such lack of information constitutes a significant barrier to demonstrating valid consent under EU law, as the data subject must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under EU law.

Wearable devices such as smart watches are also not noticeable[5]: most observers may not distinguish a normal watch from a connected one, when the latter may yet embed cameras, microphones and motion sensors that can record and transfer data without the individuals being aware of, and even less consenting to such processing. This raises the question of the identification of data processing through Wearable Computing, which might be solved by envisaging appropriate signposting that would be actually visible to the data subjects.

Moreover, at least in some cases, the possibility to renounce certain services or features of an IoT device is more a theoretical concept than a real alternative. Such situations lead to the question of whether the user's consent to the underlying data processing can then be considered as free, hence valid under EU law.

In addition, classical mechanisms used to obtain individuals' consent may be difficult to apply in the IoT, resulting in a "low-quality" consent based in a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, today, it seems that sensor devices are usually designed neither to provide information by themselves nor to provide a valid mechanism for getting the individual's consent. Yet, new ways of obtaining the user's valid consent should be considered by IoT stakeholders, including by implementing consent mechanisms through the devices themselves. Specific examples, like Privacy Proxies and Sticky Policies, are mentioned later in this document.

2.3 **Inferences derived from data and repurposing of original processing**

The increase of the amount of data generated by the IoT in combination with modern techniques related to data analysis and cross-matching may lend this data to secondary uses, whether related or not to the purpose assigned to the original processing. Third parties requesting access to data collected by other parties may thus want to make use of this data for totally different purposes.

Apparently insignificant data originally collected through a device (e.g. the accelerometer and the gyroscope of a smartphone) can then be used to infer other information with a totally different meaning (e.g. the individual's driving habits). This possibility to derive inferences from such "raw" information must be combined with the classical risks analysed in relation to sensor fusion, a phenomenon which is well-known in computer science[6].

Quantified Self also illustrates how much information can be inferred from motion sensors though aggregation and advanced analysis. These devices often use elementary sensors to capture raw data

[5] As described in Opinion 02/2013 on apps on smart devices, wearable computing also highlights challenges stemming from continuous data collection from others within close proximity and for extended periods of time.

[6] Sensor fusion consists in combining sensor data or data derived from different sources in order to get better and more precise information than would be possible when these sources are working in isolation.

(e.g. data-subject motions) and rely on sophisticated algorithms to extract sensible information (e.g. the number of steps) and deduce potentially sensitive information that will be displayed to the end users (e.g. his physical condition).

Such a trend holds specific challenges. In fact, while the user was comfortable with sharing the original information for one specific purpose, he/she may not want to share this secondary information that could be used for totally different purposes. Therefore it is important that, at each level (whether raw, extracted or displayed data), IoT stakeholders make sure that the data is used for purposes that are all compatible with the original purpose of the processing and that these purposes are known to the user.

2.4 **Intrusive bringing out of behaviour patterns and profiling**

Even though different objects will separately collect isolated pieces of information, a sufficient amount of data collected and further analysed can reveal specific aspects of individual's habits, behaviours and preferences. As seen above, generating knowledge from trivial or even anonymous data will be made easy by the proliferation of sensors, and foster important profiling capabilities.

Beyond this, analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behaviour patterns.

In fact, this trend is likely to have an impact on the way the individual actually behaves, in the same way that it has been demonstrated that the intensive use of CCTV has correspondingly influenced citizen's behaviour in public spaces. With the IoT, such potential surveillance might now reach the most private sphere of the individuals' life, including homes. This will put a pressure on the individual to avoid non-usual behaviour so as to prevent the detection of what might be perceived as anomalies. Such a trend would be very intrusive on the private life and the intimacy of individuals and should be very closely monitored.

2.5 **Limitations on the possibility to remain anonymous when using services**

Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.

For instance, wearable things kept in close proximity of data subjects result in the availability of a range of other identifiers, such as the MAC addresses of other devices which could be useful to generate a fingerprint allowing data subject location tracking. The collection of multiple MAC addresses of multiple sensor devices will help create unique fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals. These fingerprints and identifiers could be used for a range of purposes, including location analytics[7] or the analysis of movement patterns of crowds and individuals.

Such a trend must be combined with the fact that such data can later be combined with other data issued from other systems (e.g. CCTV or internet logs).

In such circumstances, some sensor data are particularly vulnerable to re-identification attacks.

[7] Location analytics refers to the analysis of how many people are in a certain place at a certain time and for how long they dwell there.

In the light of the above, it is clear that remaining anonymous and preserving one's privacy in the IoT will become increasingly difficult. The development of the IoT entails significant data protection and privacy concerns in that regard.

2.6 **Security risks: security vs. efficiency**

The IoT raises several security challenges, namely as security and resource constraints force device manufacturers to balance battery efficiency and device security. In particular, it is not yet clear how device manufacturers will balance the implementation of confidentiality, integrity and availability measures at all levels of the processing sequence with the need to optimise the use of computational resources – and energy – by objects and sensors.

Therefore, there is a risk that the IoT may turn an everyday object into a potential privacy and information security target while distributing those targets far more widely than the current version of the Internet. Less secure connected devices represent potentially efficient new ways of attack including the ease of surveillance practices, data breaches resulting in personal data being stolen or compromised that can have widespread effects on consumer rights and individual's perception of the security of the IoT.

IoT devices and platforms are also expected to exchange data and store them on service providers' infrastructures. Therefore the security of the IoT should not be envisioned by considering only the security of the devices but also the communication links, storage infrastructure and other inputs of this ecosystem.

In the same way, the presence of different levels of processing whose technical design and implementation are provided by different stakeholders does not ensure the adequate coordination amongst all of them and may result in the presence of weak points that can be used to exploit vulnerabilities.

For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries. With regard to the end-to-end security, the result of the integration of physical and logical components provided by a set of different stakeholders only guarantees the level of security provided by the weakest component.

3. Applicability of EU law to the processing of personal data in IoT

3.1 **Applicable law**

The relevant legal framework to assess privacy and data protection issues raised by the IoT in the EU is composed of Directive 95/46/EC as well as specific provisions of Directive 2002/58/EC as amended by Directive 2009/136/EC.

This framework applies where the conditions of its applicability are met as set forth in article 4 of Directive 95/46/EC. The Working Party has provided extensive guidance on the interpretation of the provisions of Article 4, namely in its Opinion 8/2010[8] on applicable law.

In particular, according to Article 4-1(a) of the Directive, the national law of a Member State is applicable to all processing of personal data carried out "in the context of an establishment" of the controller on the territory of that Member State. This notion of establishment in the context of the Internet-based economy has recently been interpreted in a very large manner by the European Court of Justice[9].

The national law of a Member State is also applicable in cases where the controller is not established on Community territory but makes use of "equipment" situated on the territory of that Member State (article 4-1(c)). Therefore, even when an IoT stakeholder that qualifies as a data controller under Directive 95/46/EC is not established in the EU in the meaning of Article 4-1(a) (whether involved in the development, distribution or operation of IoT devices), it will still likely be subject to EU law in as much as it processes data collected through the "equipment" of users located in the EU.

In fact, all objects that are used to collect and further process the individual's data in the context of the provision of services in the IoT qualify as equipment in the meaning of the Directive. This qualification obviously applies to the devices themselves (step-counters, sleep trackers, "connected" home devices like thermostats, smoke alarms, connected glasses or watches, etc.). It also applies to 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.

The identification of the role of the different stakeholders involved in the IoT will be essential to qualify their legal status as data controllers, and thus identify the national law applicable to the processing which they implement, as well as their respective responsibilities. The identification of the role of the parties involved in the IoT will be analysed below in section 3.3.

3.2 **The notion of personal data**

EU law applies to the processing of personal data as defined in article 2 of Directive 95/46/EC. The Working Party has provided extensive guidance on the interpretation of this notion, namely in its Opinion 4/2007 on the concept of personal data[10].

In the context of the IoT, it is often the case that an individual can be identified based on data that originates from "things". Indeed, such data may allow discerning the life pattern of a specific

[8] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf
[9] Judgment of the court (Grand Chamber), 13 May 2014, Case C-131/12 (paragraphs 45 to 60)
[10] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

individual or family – e.g. data generated by the centralised control of lighting, heating, ventilation and air conditioning.

Furthermore, even data relating to individuals that is intended to be processed only after the implementation of pseudonymisation, or even of anonymisation techniques may have to be considered as personal data. In fact, the large amount of data processed automatically in the context of IoT entails risks of re-identification. On this point, the Working Party refers to the relevant developments described in its recent opinion on anonymisation techniques, which helps identifying these risks and makes recommendations as to the implementation of these techniques[11].

3.3 IoT stakeholders as data controllers based in the EU

The concept of data controller and its interaction with the concept of data processor are central in the application of Directive 95/46/EC, as they condition the respective responsibilities of the various organisations involved in the implementation of a data processing with regard to EU data protection rules. Stakeholders can refer to the WP29 Opinion 1/2010 on the concepts of "controller" and "processor" [12] which provides guidance on the application of this concept to complex systems with multiple actors, where many scenarios involve controllers and processors, alone or jointly, with different degrees of autonomy and responsibility.

Indeed, the implementation of the IoT casually implies the combined intervention of multiple stakeholders – such as device manufacturers, social platforms, third-party applications, device lenders or renters, data brokers[13] or data platforms.

The complex mesh of stakeholders involved asks for/implies the necessity of a precise allocation of legal responsibilities among them with regard to the processing of the individual's personal data, based on the specificities of their respective interventions.

3.3.1 Device manufacturers

Device manufacturers in the IoT do more than only sell physical items to their clients or white label products to other organisations. They may also have developed or modified the "thing's" operating system or installed software determining its overall functionality, including data and frequency of collection, when and to whom data be transmitted for which purposes (for instance, companies could price the insurance of their employees based on the data reported by the trackers they make them wear[14]). Most of them actually collect and process personal data which is generated by the device, for purposes and means which they have wholly determined. They thus qualify as data controllers under EU law.

---

[11] Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014 (WP 216), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[12] Opinion 01/2010 on the concepts of controller and processor adopted on 16 February 2010 (WP 169) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

[13] Data brokers buy data by companies in order to establish list of individuals belonging to a same category or group. These categories and groups are established by the data brokers but may reflect demographic attributes, incomes or expressed interest for a particular topic or product.

[14] With tracking devices, employers may track workers' health "http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

3.3.2 Social platforms

Data subjects are even more likely to make use of connected things when they can share such data publicly or with other users. In particular, users of Quantified Self devices tend to share data with others on social networks to foster a form of positive competition within the group.

Such sharing of data collected and aggregated by "things" on social networks will often take place automatically, once the user has configured the application in that sense. Then, sharing capability commonly belongs to the standard default settings of applications provided by the manufacturer.

The aggregation of these reports on social platforms means specific data protection responsibilities now apply to them. As this data is pushed by the user onto them, when it is processed by social networks for distinct purposes which they have determined themselves they then qualify as data controllers in their own right under EU law. For instance, a social network may use information collected by a pedometer to infer that a particular user is a regular runner and shows her ads about running shoes. The consequences of this qualification have been detailed in the earlier WP9 Opinion on social networks.[15]

3.3.3 Third party application developers

Many sensors expose APIs to facilitate application development. To use these applications, data subjects have to install third-party applications which enable them to access their data, as stored by the device manufacturer. Installing these applications often consists in providing the app developer with an access to the data through the API.

Some applications may reward users of specific things, for instance an application developed by a health insurance company could reward users of Quantified Self "things" or a home insurance company could develop a specific application to make sure that their clients' connected fire alarms are correctly configured. Unless these data are properly anonymised, such access constitutes a processing under Article 2 of Directive 95/46/EC, so that the app developer that has organised this access to the data must be considered as a data controller under EU law.

Such apps are traditionally installed on an opt-in basis. Indeed, 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 authorisation requests made by third-party application developers do not display sufficient information for the user's consent to be considered as specific and sufficiently informed, hence valid under EU law (see below).

3.3.4 Other third parties

Third parties other than device manufacturers and third party application developers may use IoT devices to collect and process information about individuals. For instance, health-insurances may wish to give pedometers to customers to monitor how often they exercise[16] and adapt their insurance premiums accordingly.

Unlike device manufacturers, such third-parties have no control over the type of data collected by the thing. Yet, they qualify as data controllers for these processing, in as much as they collect and store the data generated by such IoT devices for specific purposes which they have determined themselves.

---

[15] Opinion 5/2009 on online social networking adopted on 12 June 2009 (WP 163) - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf

[16] With tracking devices, employers may track workers' health , http://www.advisory.com/Daily-Briefing/2013/01/04/With-tracking-devices-employers-may-track-workers-health

Example: An insurance company launches a new challenge and offers a step counter to subscribers who want to apply for lower fees. Subscribers who accept the offer receive a step counter configured and registered by the company. While the subscribers can access the data recorded by their step counter, the devices themselves are owned by "FeelGood", which also has access to their subscribers' data. In that context, subscribers should be considered as data subjects and be granted access to their account on the step counting application, whereas the insurance company qualifies as a data controller.

3.3.5 IoT data platforms

Due to a lack of standardisation and interoperability, the Internet of Things is sometimes seen as an "Intranet of Things" in which every manufacturer has defined its own set of interfaces and data format. Data is then hosted in walled environments, which effectively prevents users from transferring (or even combining) their data from one device to another.

Yet, smartphones and tablets have become the natural gateways of data collected through many IoT devices to the internet. As a result, manufacturers have progressively developed platforms that aim to host the data collected through such different devices, in order to centralise and simplify their management.

Such platforms may also qualify as data controllers under EU data protection law, when the development of such services actually implies that they collect the users' personal data for their own purposes.

3.4 Individuals as data subjects: subscribers, users, non-users

Subscribers and more generally users of the IoT qualify as data subjects under EU law. If the data which they collect and store are used exclusively for their personal or domestic purposes, they will fall under the so-called "Household Exemption" of the Directive 95/46/EC[17]. However, in practice, the business model of the IoT implies that the user's data are systematically transferred to device manufacturers, application developers and other third parties who qualify as data controllers. The "Household Exemption" will therefore be of limited application in the context of the IoT.

The processing of data in the IoT may also concern individuals who are neither subscribers nor actual users of the IoT. For instance, 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, whoever the individual concerned by this data is.

4. Obligations weighing on IoT stakeholders

IoT stakeholders qualifying as data controllers (whether alone or jointly with others) under EU law must comply with the different obligations that weigh on them in application of Directive 95/46/EC and relevant provisions of Directive 2002/58/EC, if applicable. This Opinion only deals with the application of provisions that deserve specific attention in this context, but this limited focus does not preclude the application of other remaining provisions.

[17] See Opinion 5/2009 on online social networking adopted on 12 June 2009 (WP 163)

4.1 **Application of Article 5(3) of the e-Privacy directive**

Article 5(3) of Directive 2002/58/EC is applicable to situations when an IoT stakeholder stores or gains access to information already stored on an IoT device, in as much as IoT devices qualify as "terminal equipment " in the meaning of this provision[18]. This provision demands that the subscriber or user concerned then consents to such storage of access for these actions to be legitimate, unless they are "strictly necessary in order to provide a service explicitly requested by the subscriber or user" [19]. This requirement is particularly important as stakeholders other than the user or subscriber can have access to privacy-sensitive information stored on such terminal equipment[20].

The consent requirement in Article 5(3) primarily concerns the device manufacturer, but also all stakeholders that want to have access to this aggregated raw data stored in this infrastructure. It also applies to any data controller who wants to store additional data on a user's device.

In such circumstances, stakeholders in the IoT must ensure that the person concerned has effectively consented to such storage and/or access, after obtaining clear and comprehensive information from the controller about, *inter alia*, the purposes of the processing.

Therefore, the user's consent must be obtained before accessing device information that can be used to generate a fingerprint of any device (including wearable devices). The Working Party already issued guidance on the notion of consent for cookies or similar tracking technologies in its Working Document 02/2013 (WP-208) and it will provide further guidance on this issue in its future opinion on Fingerprinting.

Example: A pedometer records the number of steps made by its user and stores this information in its internal memory. The user installed an application on his computer to download directly the number of steps from his device. If the device manufacturer wants to upload the data from the pedometers to its servers, he has to obtain the user's consent under Article 5(3) of directive 2002/58/EC.

Once the device manufacturer has uploaded the data on its servers, it only keeps aggregated data about the number of steps per minute. An application requesting access to such data, in as much as it is stored on the server of the device manufacturer, is then not subject to article 5(3) of the e-Privacy Directive but to the provisions of Directive 95/46/EC relating to the legitimacy of this further processing.

Furthermore, the owner of an IoT device and the person whose data will be monitored (the data subject) might be different persons. This situation may lead to a distributed application of Article 5(3) of Directive 2002/58/EC and of Directive 95/46/EC.

Example: a car rental service installs a smart vehicle tracking device in its rental cars. Although the car rental service will be considered the owner/subscriber of the device/tracking service, the individual renting the car qualifies as the device user. Article 5(3) then requires the device manufacturer to (at least) obtain the consent of the device user, in this case the individual renting the car. Moreover, the legitimacy of the processing of personal data related to the individuals renting cars will be subjected to the distinct requirements of article 7 of Directive 95/46/EC.

4.2 **Legal basis for the processing (Article 7 of Directive 95/46)**

[18] The notion of "terminal equipment" in Article 5(3) must be understood in the same manner as that of "equipment" in Article 4(1)(c).

[19] Opinion 02/2013 on apps on smart devices (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[20] Cf. Recital 25 of Directive 2002/58/EC

Stakeholders in the IoT that qualify as data controllers (see Section 4.3 above) need to fulfil one of the requirements listed in Article 7 of this Directive for the processing of personal data to be legitimate. These requirements apply to some of these stakeholders on top of the application of Article 5(3), when the processing at stake goes beyond the storage of, or the gaining access to information stored in the user/subscriber's terminal equipment[21].

In practice, three legal bases are relevant in this context.

Consent (Article 7(a)) is the first legal basis that should be principally relied on in the context of the IoT, whether by device manufacturers, social or data platforms, devices lenders or third party developers. On several occasions, the Working Party has also issued guidance on the simultaneous application of the requirements of Article 7(a) and Article 5(3) of Directive 2002/58/EC[22]. The conditions for such consent to be valid under EU law have also been specified in a previous Working Party opinion[23].

Article 7(b) also provides that the processing is legitimate when it is necessary for the performance of a contract to which the data subject is party. The scope of this legal ground 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.

Thirdly, Article 7(f) permits the processing of personal data where it is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which require protection under Article 1(1) of the directive.

In its judgment in the *Google Spain* case[24], the European Court of Justice has provided substantial guidance on the interpretation of this provision, in addition to the one already provided in the previous joint cases ASNEF and FECEMD (C-468/10 and C-469/10). In the context of the IoT, the processing of an individual's personal data is likely to affect significantly his/her fundamental rights to privacy and to the protection of personal data in situations where, without IoT devices, data could not have been interconnected or only with great difficulty. Such situations may happen when the data collected relate to the individual state of health, home or intimacy, his/her location and many other aspects of his/her private life. In the light of the potential seriousness of that interference, it is clear that such processing will hardly be justified by merely the economic interest which an IoT stakeholder has in that processing. Other interests pursued by the controller or by the third party or parties to whom the data are disclosed must come into play[25].

Example: In the framework of a plan to promote the use of public transport and to reduce pollution, the City council wants to regulate parking in the city centre by imposing access restrictions as well as

[21] On the articulation of Article 5(3) and Article 7(a), see in particular Opinion 02/2013 on apps on smart devices adopted on 27 February 2013 (WP202) – (pp. 14 and ff.) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf and Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (WP217) – (pp. 26, 32, 46)
[22] Opinion WP202, p.14 ff.
[23] Opinion 15/2011 on the definition of consent adopted on 3 July 2011 (WP187), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
[24] Judgment of the court (Grand Chamber), 13 May 2014, Case C-131/12 (paragraphs 74 ff.)
[25] Opinion WP217

parking fees. The amount of the fee depends on various parameters, including the type of engine (diesel, gasoline, electric) and the age of the vehicle. Once a vehicle approaches a free parking slot, a sensor can read the license plate in order to figure out, after checking with a database, the surcharge or discount to be automatically applied according to predefined criteria. In this case, the processing of the license plate information for determining the fee could satisfy the legitimate interest of the data controller. Further processing, like getting information – un-anonymised – on the movement of vehicles through the restricted area would require the use of another legal basis.

4.3 **Principles relating to data quality**

Taken together, the principles enshrined in Article 6 of Directive 95/4/EC constitute a cornerstone of EU data protection law.

Personal data should be collected and processed fairly and lawfully. The fairness principle specifically requires that personal data should never be collected and processed without the individual being actually aware of it. This requirement is all the more important in relation to the IoT as sensors are actually designed to be non-obtrusive, i.e. as invisible as possible. Yet, data controllers acting in the IoT (first and foremost device manufacturers) must inform all individuals in the geographical or digital vicinity of connected devices when data related to them or their environment is collected. Complying with this provision goes beyond a strict legal requirement: fair collection belongs to the user's most crucial expectations in relation to the IoT, in particular as to Wearable Computing.

Example: A health-related device uses a small light to monitor how blood flows in veins, and to derive heartbeat information. The device includes another sensor that measures blood oxygen level but no information is available on this collection of data neither on the device nor on the user interface. Even if the blood oxygen sensor is fully functional, it should not be enabled without first informing the user. Explicit consent will be required to enable this sensor.

The purpose limitation principle implies that data can only be collected for specified, explicit and legitimate purposes. Any further processing that would be incompatible with these original purposes would be illicit under EU law. This principle aims at enabling users to know how and for what purposes their data will being used and decide whether to entrust a data controller with his/her data. These purposes must be defined *before* the data processing takes place, which excludes sudden changes in the key conditions of the processing. This implies that IoT stakeholders have a good overview of their business case before they start collecting any personal data.

Also, the data collected on the data subject should be strictly necessary for the specific purpose previously determined by the data controller (the "data minimisation" principle). Data that is unnecessary for that purpose should not be collected and stored "just in case" or because "it might be useful later". Some stakeholders consider that the data minimisation principle can limit potential opportunities of the IoT, hence be a barrier for innovation, based on the idea that potential benefits from data processing would come from exploratory analysis aiming to find non-obvious correlations and trends. The Working Party cannot share this analysis and insists that the data minimisation principle plays an essential role in the protection of data protection rights granted by EU law to individuals, so that it should be respected as such[26]. This principle specifically implies that when

[26] In any case, exploratory research is never operated at total random in practice: the general purpose of any research is traditionally defined, partially at the very least, should it only be for organisational and budgetary

personal data is not necessary to provide a specific service run on the IoT, the data subject should at the least be offered the possibility to use the service anonymously.

Article 6 also requires that personal data collected and processed in the context of IoT is kept for no longer than is necessary for the purpose for which the data were collected or further processed. This 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 a user when he subscribes to a specific service on the IoT should be deleted as soon as the user puts an end to his subscription. Similarly, information deleted by the user in his account should not be retained. When a user does not use the service or application for a defined period of time, 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.

4.4 **Processing of sensitive data (Article 8)**

Applications in the IoT may process personal data that can reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, which actually qualify as "sensitive data", deserving special protection in the sense of Article 8 of Directive 95/46/EC. In practice, the application of Article 8 to sensitive data in the IoT requires that data controllers obtain the user's explicit consent, unless the data subject has made himself the data public.

Such a situation is likely to arise in the specific contexts like Quantified Self devices. In these cases, the relevant devices are mostly registering data relating to the well-being of the individual. This data does not necessarily constitute health data as such, yet it may quickly provide information about the individual's health as the data is registered in time, thus making it possible to derive inferences from its variability over a given period. Data controllers should anticipate this possible shift in qualification and take adequate measures accordingly.

Example: Company X has developed an application that, by analysing 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. Explicit consent of the user should be gathered to process the data for that purpose. Compliance with this consent requirement can be satisfied in the same conditions and at the time as when the consent is collected from the data subject under Article 7(a).

4.5 **Transparency requirements (Articles 10 and 11)**

Beyond the requirement of fair collection of data in Article 6 (a), data controllers must communicate specific information to data subjects in application of Articles 10 and 11: the identity of the controller, the purposes of the processing, the recipients of the data, the existence of their rights of access and right to oppose (which includes information about how to disconnect the object to prevent disclosure of further data).

---

reasons. It is hard to imagine that the processing of data for a specific research will be compatible with the original purpose of the data collection, hence fall afoul of EU law.

Depending on the applications, this information could be provided for instance on the object itself, using the wireless connectivity to broadcast the information, or using location through privacy-preserving proximity testing done by a centralised server to inform users that are located close to the sensor.

This information must further be provided in a clear and comprehensible manner, in accordance with the principle of fair processing. For instance, the device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections.

4.6 **Security (article 17)**

Article 17 of the Data Protection Directive provides that the controller "*must implement appropriate technical and organisational measures to protect personal data*" and that "*the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out*".

Consequently, any stakeholder that qualifies as a data controller remains fully responsible for the security of the data processing. If security flaws resulting in breaches of the security principle are the result of an inadequate design or maintenance of the devices used, it engages the responsibility of the data controller. In that sense, it is necessary for these data controllers to perform security assessments of systems as a whole, including at components' level, applying principles of composable security. In the same line, use of certification for devices as well as the alignment with internationally recognised security standards must be implemented to improve the overall security of the ecosystem of the IoT.

Subcontractors who design and manufacture hardware components on behalf of other stakeholders without actually processing any personal data cannot, strictly speaking, be held responsible under article 17 of Directive 95/46/EC in case a data protection breach occurs because of a flaw in the security of these devices. Yet, these stakeholders play a key role in maintaining the security of the IoT ecosystem. Stakeholders that bear direct data protection responsibilities towards data subjects should make sure that these subcontractors are actually held by high security standards with regard to privacy when designing and manufacturing their products.

As said before, security measures are to be implemented taking into account the specific operational constraints of IoT devices. For instance, today, most sensors are not capable of establishing an encrypted link because of the priority given to the physical autonomy of the device or to cost control.

Furthermore, devices operating in the IoT are also difficult to secure, both for technical and business reasons. As their components usually use wireless communications infrastructure and are characterised by limited resources in terms of energy and computing power, devices are vulnerable to physical attacks, eavesdropping or proxy attacks. Most common technologies currently in use – i.e. PKI infrastructures – are not easily ported on IoT devices since most of the devices do not have the computing power needed to cope with the required processing tasks. The IoT entails a complex supply chain with multiple stakeholders assuming different degrees of responsibility. A security breach might have origins from any of them, especially when considering M2M environments based on exchange of data among devices. Therefore, account should be taken of the need to use secure and lightweight protocols that can be used in low resource environments.

In this context where reduced computing capacity may put at risk secure and efficient communication, the WP29 stresses that it is even more important to comply with the data minimisation principle and restrict processing of personal data, in particular its storage on the device, to the minimum required.

Furthermore, devices that are designed to be accessed directly via the Internet are not always configured by the user. They may thus provide an easy access path to intruders if they keep running with the default settings. Security practices based on network restrictions, disabling by default non critical functionalities, preventing use of un-trusted software update sources(thus limiting malware attacks based on code alteration) could contribute to limiting the impact and the extent of possible data breaches. Such privacy protections should be built-in from the very outset, in application of the "Privacy by Design" principle.

Additionally, the absence of automatic updates results in frequent unpatched vulnerabilities that can easily be discovered through specialised search engines. Even in those cases were the users are aware of vulnerabilities affecting their own devices, they may not have access to the vendor's updates, whether because of hardware limitations or of out-dated technologies preventing the device from supporting software updates. Should a device manufacturer stop supporting a device, alternative solutions to support it should be provided (e.g. opening the software to the open-source community). Users must be notified that their devices are likely to become vulnerable to unfixed flaws.

Some of the self-tracker systems (e.g. pedometers, sleep trackers) on the market also suffer from security flaws allowing attackers to tamper observed values that are reported to the applications and device manufacturers. It is essential that these devices should offer adequate protections against data tampering, in particular if values reported by these sensors indirectly impact health-related decisions of users.

Last but not least, an adequate policy of data breach notification can also help to contain the negative effects of software and design vulnerabilities by spreading knowledge and providing guidance on those issues.

5. Rights of the data subject

IoT stakeholders must respect the rights of data subjects in accordance with the provisions laid down in Articles 12 and 14 of Directive 95/46/EC and take organisational measures accordingly. These rights are not limited to the subscribers of IoT services or device owners and concern any individual whose personal data are processed.

5.1 Right of access

Article 12(a) provides that data subjects are entitled to obtain from the data controllers communication in an intelligible form of the data that is subjected to processing and any available information as to their source.

In practice, users in the IoT tend to be locked to specific systems. Devices usually first send data to the device manufacturer, which then makes this data accessible to the user through a web portal or an app. This design allows manufacturers to provide online services that leverage the device capabilities, but it may also prevent users from freely choosing the service that interacts with their device.

Additionally, today, end-users are rarely in a position to have access to the raw data that are registered by IoT devices. Clearly, they hold a more 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. Also, availing of this raw data would give them a capacity to transfer their data to another data controller and switch services - for instance, if the original data controller changes its privacy policy in a way that does not satisfy them. Today, in practice, these persons have in practice no other possibility than to stop using their devices as most data controllers do not provide such functionality and provide access only to a degraded version of the stored raw data.

The WP29 believes that such attitudes prevent the effective exercise of the right of access granted to individuals by Article 12(a) of Directive 95/46/EC. It believes that, on the contrary, stakeholders in the IoT should take steps to enable users to effectively enforce this right and offer users a possibility to choose another service that might not be proposed by the device manufacturer. Data interoperability standards could be usefully developed to that effect.

Such steps would be all the more relevant to take as the so-called "right to portability", which the draft General Data Protection Regulation is likely to consecrate as a variation of the right of access, aims at putting a clear end to situations of user "lock-in"[27]. The ambition of the European lawmaker on this point consists of unlocking competition impediments and helping new players to innovate on this market.

5.2 **Possibility to withdraw consent and to oppose**

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

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. a user could require that both his pedometer and his watch stop counting his 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[28].

Example: a user installs a connected fire alarm in his apartment. The alarm uses an occupancy sensor, a heat sensor, an ultrasonic sensor and a light sensor. Some of these sensors are required to detect fire while some of them only provide additional features about which he was previously informed. The user should be able to disable these features to make use of the fire alarm only, hence disconnect the sensors used to provide these features.

[27] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[28] Opinion 13/2011 on Geolocation services on smart mobile devices adopted on 16 May 2011 (WP185) - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

Interestingly, some recent developments in this field are trying to empower data subjects by giving them more control over consent management features, for example through the use of sticky-policies[29] or privacy proxies[30].

6. Conclusions and recommendations

A number of recommendations are listed below, which the WP29 has deemed useful to make in order to facilitate the application of EU legal requirements to the IoT, listed above.

The recommendations below provide only guidance that is additional to documents that were previously adopted by the WP29.

In this respect, the Working Party wishes to draw specific attention to its earlier recommendations on apps on smart devices[31]. Because smartphones are part of the environment of the IoT and both ecosystems involve a comparable set of stakeholders, these recommendations are directly relevant to the IoT. In particular, app developers and device manufacturers should provide an adequate level of information to end users, offer simple opt-outs and/or granular consent, when applicable. Furthermore, when consent has not been obtained, the data controller should anonymise the data before repurposing it or sharing them with other parties.

7.1 Recommendations common to all stakeholders

- Privacy Impact Assessments (PIAs) should be performed before any new applications are launched in the IoT. The methodology to be followed for such PIAs can be based on the Privacy and Data Protection Impact Assessment Framework which the WP29 has adopted on 12 January 2011 for RFID Applications[32]. Where appropriate/feasible, stakeholders should consider making the relevant PIA available to the public at large. Specific PIA frameworks could be developed for particular IoT ecosystems (e.g smart cities).

- Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing. As a principle, deletion should take place at the nearest point of data collection of raw data (e.g. on the same device after processing).

- Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default.

- User empowerment is essential in the context of IoT. Data subjects and users must be able to exercise their rights and thus be "in control" of the data at any time according to the principle of self-determination of data.

---

[29] In that regard, 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.

[30] A 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 authorised, limited or simply rejected.

[31] Opinion 02/2013 on apps on smart devices (WP202), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

[32] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf

- The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. In particular, information and consent policies must focus on information which is understandable by the user and should not be confined to a general privacy policy on the controllers' website.

- Devices and applications should also be designed so as to inform users and non-user data-subjects, for instance via the device physical interface or by broadcasting a signal on a wireless channel.

6.1 **OS and device manufacturers**

- Device manufacturers must inform users about the type of data that are collected by sensors and further processed, the types of data that they receive and how it will be processed and combined.

- Device manufacturers should be able to communicate to all other stakeholders involved as soon as a data subject withdraws his consent or opposes the data processing.

- Device manufacturers must provide granular choices when granting access to applications. The granularity should 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.

- To prevent location tracking, device manufacturers should limit device fingerprinting by disabling wireless interfaces when they are not used or should use random identifiers (such as random MAC addresses to scan wifi networks) to prevent a persistent identifier from being used for location tracking.

- To enforce transparency and user control, device manufacturers should provide tools to locally read, edit and modify the data before they are transferred to any data controller. Furthermore, personal data processed by a device should be stored in a format allowing data portability.

- Users are entitled to a right of access to their personal data. They should be provided with tools enabling them to easily export their data in a structured and commonly-used format. Therefore, device manufacturers should provide a user-friendly interface for users who want to obtain both aggregated data and/or raw data that they still store.

- Device manufacturers should provide simple tools to notify users and to update devices when security vulnerabilities are discovered. When a device becomes deprecated and is no longer updated, the device manufacturer should notify the user and make sure that he is aware that the device will no longer be updated. All the stakeholders that are likely to be impacted by the vulnerability should also be informed.

- Device manufacturers should follow a Security by Design process and dedicate some components to the key cryptography primitives.

- Device manufacturers should limit as much as possible the amount of data leaving devices by transforming raw data into aggregated data directly on the device. Aggregated data should be in a standardised format.

- Unlike smartphones, IoT devices may be shared by several data subjects or even rented (e.g. smart homes). A setting should be available to distinguish between different individuals using the same device so that they cannot learn about each other's' activities.

- Device manufacturers should work with standardisation bodies and data platforms to support a common protocol to express preferences with regard to data collection and processing by data controllers especially when such data is collected by unobtrusive devices.

- Device manufacturers 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.

6.2 **Application developers**

- Notices or warnings should be designed to frequently remind users that sensors are collecting data. When the application developer does not have a direct access to the device, the app should periodically send a notification to the user to let him know that it is still recording data.

- Applications should facilitate the exercise of data subject rights of access, modification and deletion of personal information collected by IoT devices.

- Application developers should provide tools so that data-subjects can export both raw and/or aggregated data in a standard and usable format.

- Developers should pay special attention to the types of data being processed and to the possibility of inferring sensitive personal data from them.

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

6.3 **Social platforms**

- Default settings of social applications based on IoT devices should ask users to review, edit and decide on information generated by their device before publication on social platforms.

- Information published by IoT devices on social platforms should, by default, not become public or be indexed by search engines.

6.4 **IoT device owners and additional recipients**

- Consent to the use of a connected device and to the resulting data processing must be informed and freely given. Users should not be economically penalised or have degraded access to the capabilities of their devices if they decide not to use the device or a specific service.

- The data subject whose data is being processed in the context of a contractual relationship with the user of a connected device (i.e. hotel, health-insurance or a car renter) should be in a position to administrate the device. Irrespective of the existence of any contractual relationship, any non-user data subject must be in a capacity to exercise his/her rights of access and opposition.

- Users of IoT devices should inform non-user data subjects whose data are collected of the presence of IoT devices and the type of collected data. They should also respect the data subject's preference not to have their data collected by the device.

6.5 Standardisation bodies and data platforms

- Standardisation bodies and data platforms should promote portable and interoperable as well as clear and self-explanatory data formats in order to facilitate both transfers of data between different parties and helping data subjects understand what data is actually being collected on them by IoT devices.

- Standardisation bodies and data platforms should not only focus on the format for raw data but also on the emergence of formats for aggregated data.

- Standardisation bodies and data platforms should promote data formats that contain as few strong identifiers as possible in order to facilitate the proper anonymisation of IoT data.

- Standardisation bodies should work on certified standards that would set the baseline for security and privacy safeguards for data subjects.

- Standardisation bodies should develop lightweight encryption and communication protocols adapted to the specificities of IoT, guaranteeing confidentiality, integrity, authentication and access control.