Project no. 732027

VIRT-EU

Values and ethics in Innovation for Responsible Technology in Europe

Horizon 2020

ICT-35-2016

Enabling responsible ICT-related research and innovation

Deliverable 4.4

Final report on PESIA

Due date: 31st March 2019

Actual submission date: 30th April 2019

Number of pages: 51

Lead beneficiary: POLITO

Author(s): Javier Ruiz, Ed Johnson-Williams (Open Rights Group) and Prof Marcella Sarale, Dr Maria Samantha Esposito, Prof Alessandro Mantelero (Politecnico di Torino)

Project Consortium

Beneficiary no.	Beneficiary name	Short name
1 (Coordinator)	IT University of Copenhagen	ITU
2	London School of Economics	LSE
3	Uppsala Universitet	UU
4	Politecnico Di Torino	POLITO
5	Copenhagen Institute of Interaction Design	CIID
6	Open Rights Group	ORG

Dissemination Level

PU	Public	**X**
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Dissemination Type

R	Document, report	**X**
DEM	Demonstrator, pilot, prototype	
DEC	Websites, patent filling, videos, etc.	
O	Other	
ETHICS	Ethics requirement	

Table of Contents

Executive summary

In the previous deliverable D4.3 we presented the questionnaire for the Privacy, Ethical and Social Impact Assessment. This deliverable contains an updated version of the questionnaire, improved to better serve the specific needs of IoT developers.

This deliverable concerns the second part of the tasks described in T4.3 (Providing general and sector-specific guidelines for PESIA, M15-M27) and in T4.4 (Providing general and sector-specific instruments, M18-M27).

From a methodological perspective, the main challenge to modifying the PESIA questionnaire has been to find the right language and structure that will not make it too daunting for IoT developers to complete without assistance. To address this challenge, we have drawn on the previous ethnographic work of our consortium partners, but we have also carried some original research on IoT companies..

In addition to the updated questionnaire, in this deliverable, we include the results of our research into the policies and materials from IoT companies, where we have found that many companies do not comply with basic requirements to provide privacy policies and generally have a very low understanding of privacy issues. Our examination of their marketing materials and websites has shed light on how some companies construct the needs of their clients, for example in order to market products that implement surveillance in order to provide safety and security.

This research together with the ethnographic research conducted by our partners and reported in prior deliverables has formed basis of the changes in the questionnaire, but it has also formed the basis for consortium dissemination activities. As part of these efforts, we have started a YouTube channel dedicated to “unboxing” IoT devices form the perspective of privacy and ethics.

The questionnaire included here is the final version as such. ORG will now take this work and build it into a digital prototype that will be tested it extensively with stakeholders and eventually deployed into a service for Deliverable D6.3.

1. Introduction

This deliverable builds on the work of the previous report D4.3 to further develop the PESIA questionnaire into a usable tool to be used by Internet of Things (IoT) developers and other interested parties.

In this light, we have further elaborated the first draft of the questionnaire we have been informed by our understanding of the perspective and prior knowledge of potential users: IoT developers. This understanding comes from various sources. The ethnographic work of London School of Economics (LSE), together with the design workshops led by Copenhagen Institute of Interaction Design (CIID) and attended by Open Rights Group (ORG) staff have given us some clear insights into the understanding of privacy and ethics among this community.

This is complemented by our work in section two of this deliverable, where ORG analyse the online presence of some fifty IoT companies to see how the documents made available by them reflect privacy, social and ethical values. The analysed documents range from privacy policies and terms and conditions, to product brochures and the general web pages. Our starting point are the ethical values outlined by LSE and Politecnico di Torino, which have been collated into a single taxonomy.

The report then presents the new version of the PESIA questionnaire. The structure has been redesigned. Where we previously followed a structure around data protection topics we now take users through a linear process that starts with the mapping of the data and activities and ends with mitigations and actions.

We have rewritten most of the questions that were included in D4.3 to make them simpler to understand and removed technical terminology wherever possible and provided explanations where this is not feasible. The questionnaire now includes explanatory texts to help users answer the questions. In a future version we aim to develop a glossary of privacy specific terminology and explore other ways to make it easier to use.

The final section of the questionnaire, which looks at ethical and social aspects, uses a different approach from the privacy section, providing examples using fictitious case studies (based on the examined case law) and context specific questions. The implementation of PESIA into a digital service tool in Deliverable 6.3 will permit the adaptation of this section with further scenarios and case studies. As the VIRT-EU tools will be available under an open licence, we expect that further questions will be added by future re-users, allowing the PESIA to be tailored to various context and sectors. The practical implementation into a digital tool will also enable more sophisticated follow up actions once risks have been identified.

On the basis of our experience with developers in the various workshops we have identified that the quantification of the risks or any matrix organisation, which are the typical approaches for risk management, would benefit from specific exercises and it would not be fruitful to use a questionnaire format for such assessment. Other tools developed in the project will enable the organisation of risks and to record and structure any mitigation actions proposed and will be incorporated in the service tool.

In summary, the first part of this report presents an analysis of IoT companies by ORG that complements the legal work of Politecnico di Torino, and the ethnographic approach of ITU and LSE to improve our understanding of the sector and what are the most appropriate interventions. In the second part, we present a revised version of PESIA more tailored to the needs of IoT developers based on this previous work.

2. An analysis of ethical values within a range of Internet of Things companies

In order to complement the ethnographic and legal work with an enhanced understanding the ethical values held by companies working on Internet of Things (IoT) products we have examined documents made available by the companies themselves. These include contractual agreements such as terms of service, privacy policies, service agreements, and so on. We have also looked for information about their understanding of privacy and ethics in their commercial materials, marketing brochures and public websites. This has given us a better perspective not only of how these companies understand these issues, but also how they portray themselves to their customers and others.

This work was intended to help inform our work detailed elsewhere in this report – restructuring the PESIA and building our understanding of the current state of ethical thinking within IoT companies. Alongside our textual analysis, this report is complemented by the ethnographic research carried out by our consortium partners at the London School of Economics (LSE), who have spent time observing and interviewing people working in the offices of startups.

We compiled a list of fifty EU-based companies working in this area of Internet of Things products. The companies were found through a search of various online sources: general technology news, IoT specific websites, online discussions - e.g. Quora - and websites specialising on start-ups. The companies are all located in the European Union, although several have manufacturing in China and also serve the US market. In some cases, companies that in first instance had appeared as EU-based turned out to have relocated to the USA.

We mainly focussed on IoT companies producing defined physical products for consumers or the home, and not just data integration or other services. Some companies offer both to variable degrees. These fifty companies represent a diverse sample of sectors from toys to security locks and health monitors. The majority are small start-ups, as this is the focus of our project, but we also included more established companies and a couple of product lines that are part of multinational enterprises. The companies are classified around their sector in our own taxonomy of categories such as “wellbeing”, “toys”, or “home security”. We also recorded the country, and the level of maturity the company was at (such as “startup”, “mid-size”, or “big industry”).

For each of those companies, we collated the available information on their websites. We started with web pages for any contractual agreements with consumers (such as privacy policies or terms of service). We expected these more formal documents to contain a clearer understanding of legal obligations. We also collected information about their products, descriptions and additional information for users. We expected these materials to provide information on how privacy and ethics fit with the company's value proposition to their customers.

2.1 Ethical values

The following table of ethical values integrates values that have been identified by VIRT-EU consortium partners at Politecnico di Torino in data protection regulator decisions across the European Union with values identified in ethnographic research by the teams from LSE and ITU.

This has been a useful framework for the assessment of ethical values in language used by companies in contractual agreements and in non-contractual language. We used this framework to help us identify issues around ethical values within the fifty companies.

Consolidated Legal and Ethical Values	Main goals/issues in the Internet of Things context
Privacy	Safeguarding intimacy, identity, and physical integrity.
Data Protection	Providing users access to their collected data, giving them explanations about how personal information is used. Issues concerning the distinction between anonymous and personal data that could allow companies to avoid data protection but still have impacts on groups and individuals. Ensuring the rights to access, rectification, erasure (right to be forgotten) and to object with regard to personal data processed by means of IoT devices and facilitating data portability.
Dignity	Avoiding any forms of surveillance or invasive control over individuals using IoT devices. IoT devices shall not be used to collect unauthorised private information or to publicly disclose private facts.
Well-being	Increase individuals' well-being and fostering "IoT for good".
Non-discrimination	Preventing any forms of discrimination.
Autonomy	Safeguarding individual self-determination and freedom of expression.
Transparency	Providing access to information concerning personal data processing. Encouraging transparency about data operations, device usage and firmware and software upgrades.
Participation	Effectively engaging data subjects in data processing design. Promoting debate and dialogue (e.g. manifestos).

Accountability	Effectively addressing security and safety issues, adopting adequate risk prevention strategies and measures.
Interoperability	Promoting interoperability as one of the key values to create a trusted IoT ecosystem. Facilitating data portability, both for taking data out and in.
Safety & security	Protecting users against any harm due to IoT devices (hardware and software security). Updatability of devices for security.
Responsibility	Strengthening algorithmic accountability/liability.
Openness and shareability	Promoting open hardware and software with open source code.
Sustainability	Issues concerning the potential impact on social and environmental justice.
Inclusion and equality	Considering diversity and inclusion both in IoT development and with regard to users' experience.

2.2 Issues in the analysis of contractual agreements: a summary of first stage findings

Over the course of our work searching for, reading, and analysing the contractual agreements of the fifty Internet of Things companies in our list, we have found that these documents have not been particularly revealing in terms of the ethical values held by companies.

There are several reasons for this, which are outlined in the following sub-sections. In general, a significant number of the companies we looked at did not make these documents available on their website.

2.2.1 Repetitive and generic language

When companies do publish these contractual agreements, the text within the documents is often generic and repetitive. The terms of service documents usually state the relationship between the company and the customer, what standards the customer can expect from the company, what rights the company asserts it holds, and informs the customer and their rights. In practice, these documents contain information including who owns the company, the minimum age of users, how to buy or cancel a product, who has intellectual property rights, and limitations of liability.

For the most part, ethical values were not particularly evident in the text of these documents. Any assertion that these documents do contain ethical values should be carefully made. These documents use very generic text. It is likely that they are written by filling in placeholders in common, shared templates.

One example that illustrates this re-use of templates is the Terms of Use provided by a company called *Mystery Vibe* – a sex toy company. As of March 2019, these Terms of Use[i] contained over twenty placeholders for details to be added. These placeholders have been in this text since at least 19th September 2015[ii] which is the first time the webpage was captured by the Internet Archive. This means that the Terms of Use has been in this state for over three and a half years. As far as we can tell, the company has been selling products throughout this period.

Few contractual agreements make it so clear as it is here that few resources have been dedicated to ensuring these documents are complete, regularly updated, and accurate. While most companies do have terms of use documents with the correct details, this example suggests that companies' attitude towards these documents is more about ensuring legal compliance and reducing legal liability than it is about ensuring consumers are well-informed. In turn, this reduced our confidence that we could extract meaningful and reliable insights into the ethical values held by companies from these documents. This was because the generic language that is so widely used suggests that we cannot determine how actively a company has decided what to include in the terms of use.

2.2.2 Prohibitions on reverse engineering and the values of openness and shareability and sustainability

We found that many of the terms of use documents state that the user is not allowed to reverse engineer the software that runs on the IoT product. This is a complex area that we will not explore fully here. It is arguably related to the values of openness and shareability and sustainability in that prohibiting reverse engineering could reduce how long a product could be usable. The early obsolescence of IoT products due to the lack of software support, when the actual hardware is perfectly functional, is a very common problem that has hit some well-known brands. For example, thermostat company Nest stopped support for some of its products when it was acquired by Google.[iii] These products stopped functioning when Google and Nest stopped this support.

Reverse engineering could allow users or third parties to continue to support deprecated hardware. In short, reverse engineering is a process of determining the original source code of some (usually closed-source) software by analysing the final, compiled code. This would allow someone to scrutinise the code for security issues, but also to re-use the code for their own purposes. Most companies in this area want to keep their code closed source and private.

One of the advantages of open-source – as opposed to closed-source – software is that the original source code is publicly available. This means that if a product that runs on open-source software is deprecated, someone could theoretically re-use the original source code to ensure their product continues to work. It is vastly more difficult to do this with products that run with closed-source software. Besides, in some cases it is also illegal under intellectual property law.

While terms of service that prohibit reverse engineering do have some impact on the sustainability of a product, it is very unclear that companies are including this in these documents as a result of a position they hold about sustainability *per se*. Partly, this is because it seems likely that companies are attempting to ensure that they can withdraw service from a user who appears to be tampering with software. It is also because the language used is so generic and widely-used that we cannot say that a specific company has actively decided to include this prohibition.

2.2.3 Privacy policies: for websites not products

Where they were available, we looked at companies' privacy policies on their websites.

Several of the companies in our list did not make privacy policies available at all, even when they included analytics software such as Google Analytics on their website. One example of this was the Swedish company *Chatteddy*. *Chatteddy* is a connected teddy bear aimed at children which allows users to send and receive audio messages to and from phones running a linked app. Users can buy access to content such as stories and lullabies.

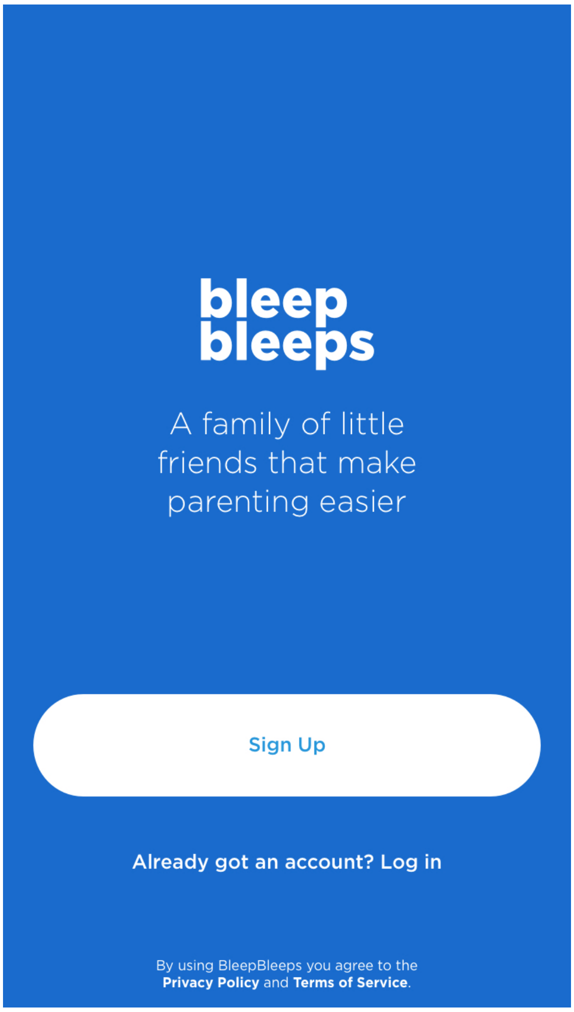
Chatteddy does not make a privacy policy available on its website to communicate to visitors what data they collect and what it is used for. They also do not communicate to potential purchasers of their product what data would be collected. It seems incredibly unlikely that this product would not be collecting personal data and it is a product aimed at children.

Nearly all of the privacy policies we analysed were about the website itself, rather than the products that the company created and sold. In these cases, a consumer could not easily find out – prior to making a purchase – what data these products would collect, how that data would be used, and what the consequences of that would be for the consumer. In such cases, the privacy policy would say, for example, that when the user visited a company's website, the company would collect the user's IP address and keep track of which webpages they visited. The privacy would not say what data the company would collect from the consumer's use of the product on sale. This situation leaves consumers unable to make purchasing decisions informed about how data about them will be used if they buy the product.

2.2.4 The availability of privacy policies in purchased products

We considered the possibility that the companies who were not communicating how their product would collect and use data may make such documents available to consumers when they purchase the products. To explore this possibility, we have bought a range of IoT products from different companies to find out how the companies communicate their use of data to their customers. We are creating unboxing videos to document our findings which are available on YouTube[iv]. Besides issues around privacy and the communication of data use, we are also using the videos to explore some of the other ethical values in our framework such as sustainability, security, and usability.

In the case of *Sammy Screamer* – a motion sensor and alarm by the company *bleepbleeps* – we did not find any paper documentation of a privacy policy in the box. As far as we can tell, the only opportunity a user has to find out what data the product will collect about them and how it will be used in in the signup phase in app that controls the motion sensor device. There are links at the bottom of the signup screen which are very small and difficult to tap accurately. The user does not have to read the privacy policy to create an account. This model of implied consent is not allowed under GDPR.


bleep
bleeps
A family of little friends that make parenting easier
Sign Up
Already got an account? Log in

By using BleepBleeps you agree to the **Privacy Policy** and **Terms of Service**.

A screenshot from the signup screen of the bleepbleeps iOS phone app – Ed Johnson-Williams

This is one case study and we do not wish to single out *bleepbleeps*. It is outside of the scope of this report to purchase, research, and review a very large number of other devices.

We are carrying out a small number of similar reviews as part of our unboxing video series that are presented on the VIRT-EU YouTube channel as we explain elsewhere in this report. The next video focuses on wearable smart watches for children. We recommend that further research is done to follow up on this starting point.

The difficulty we have had in finding privacy policies relating to the products made by the companies in our list does suggest that the communication of data use and data protection rights to consumers is not being prioritised by companies. Many of the companies we looked at were (or are) start-ups. They are likely to have put their resources into ensuring their company grows than in documenting and communicating their privacy policy. This has meant, however, that meaningfully extracting values from privacy policies has been a difficult task.

2.2.5 Ethical values within privacy policies

It is clear from our research is that it is relatively rare for the examined IoT companies to communicate how they will collect and use data from the products they sell to potential consumers prior to purchasing. An example of an exception to this is the privacy policy from a company called *nello* which makes a Wi-Fi connected intercom and linked app. This privacy policy explicitly covers the "Products, Platform, App and Website".[v] The app-connected toothbrush *Playbrush* also make a privacy policy available that covers what data will be collected while the user uses the toothbrush[vi]. They say, for example, that they carry out "storage of brushing data for the purpose of in-app advertisement: based on the tooth brushing performance (frequency, duration, accuracy)". Potential purchases can find this out before they decide whether to purchase the product or not. It is not clear how likely it is for someone actually to be aware of this prior to purchase, however.

Even in such cases, it is very difficult to extract ethical values such as sustainability, inclusivity, or equality from a privacy policy like this. Similarly to terms of service, the language used is quite matter of fact and deals in concrete terms about what data will be collected and for what purpose.

One interpretation of companies' use of tracking pixels, remarketing techniques across social media and search engines, and detailed data collection for behavioural advertising is that there is a prioritisation of marketing and a company's financial and commercial interests over users' privacy and control over data about them.

2.3 Ethical values in non-contractual language: a summary of findings from analysing other language on company websites

The terms of service, privacy policies and other contractual information available are not enough to build a good understanding of the ethical values held by these companies. Many start-ups may not provide enough compliance documentation of this kind, and if they do these texts are generally too formulaic. We turned to the other pages on the companies' websites as an additional source of material to carry out this research.

While the other areas of these companies' websites have been more fruitful in terms of getting an insight of a company's ethical thinking, there are important caveats to this. Because the content on companies' websites is, to a large extent, marketing, it does not necessarily reveal the ethical values of the company in a full and unmediated way. In some cases, this material may actually show the values that a company wants to communicate to public audiences, and not their actual practice or values. Such an analysis revealed that relying on primarily online information about any company to understand their ethical position is impossible and requires in-depth work, such as that conducted by our partners LSE and ITU and previously reported in D2.2 and D1.3. This ongoing research forms the foundation for the applied analysis and tool development we are currently developing and that will be reported in D6.2. Nevertheless, we have made some interesting findings from our analysis of these websites.

2.3.1 Surveillance as a personal good

We found a number of companies selling products that celebrated self-surveillance and relied on detailed data collection by the company to enable the customer to monitor themselves. In many of these cases, surveillance was presented as being good for you with messages about surveillance keeping you, your family, your property and your pets safe and well. It was sometimes presented as useful and even fun.

2.3.1.1 Smartfrog

One example of this is *Smartfrog* – a company that makes a Wi-Fi connected camera and an app that lets the user see what the camera sees. *Smartfrog*'s homepage[vii] has a carousel of images and text at the top of the homepage. The website presents various use cases presented with language including:

- **Home, business and property security**
    - "Keep an eye on things at home": image of a lounge/sitting room
    - "Protect your Home. No matter where you are, see what's happening right now in your house or apartment."
    - "Keep everything at home in sight. Monitor your holiday house. Prevent false alarms."
    - "For Business. Keep watch over your premises. Protect your business and customers. Watch the shop. Watch the checkouts. Watch the car park. Prevent theft and burglaries.
- **Pet safety and wellness**
    - "See what your pets are doing": image of a dog
    - "Watch your Pets. Is your furry friend getting up to mischief?"
    - "Tell the cat to get off the sofa. Listen to the birds singing"
- **Child safety**
    - "Keep your children in sight": image of a child playing with a toy
    - "Baby Monitor. Keep an eye on your kids round the clock. Say goodnight from wherever you are."
    - "Keep babies, toddlers and children in sight. Get a notification when your baby cries"

- **Elderly care and healthcare**
    - “Keep in touch with the grandparents”: image of an elderly woman
    - “Loved ones who need care. Keep in touch with your grandparents. Talk to them from anywhere. Watch over your loved ones. Monitor and supervise medication intake. Talk to them through microphone and speaker”
- **Property security**
    - “The easiest way to protect your home and family”: image of a man wearing a balaclava
    - “Protect your Home. No matter where you are, see what's happening right now in your house or apartment.

Other copy on the *Smartfrog* website included “Enjoy the feeling of a safe and secure home” and “See what's happening at home from anywhere with your smartphone, tablet or computer”.

The language on the website presents a series of people, animals, and property which the company presents as things that it is normal to want to protect or maintain and the connected camera is the best way to achieve that. This appears to be aimed at highlighting needs that consumers may have, but, to some extent, also at creating the perception of those needs.

Some of these actions were not possible without this technology of Internet- and app-connected cameras. If someone wanted to “[t]ell the cat to get off the sofa”, they would have to be present in the room. Similarly, other technologies could achieve some of these tasks before the existence of connected cameras. If someone wanted to “[t]alk to them [an elderly relative] through microphone and speaker”, they would use the telephone. Finally, some of these tasks required hiring a person to do the task. Somebody who wanted to “[k]eep watch over your premise, protect your business and customers, watch the shop, watch the checkouts, watch the car park, prevent theft and burglaries” would probably have to hire a security guard.

This is an example of language and the new technology being combined in an attempt to create a market and the perception of a user need. That need is fulfilled with a value proposition that positions surveillance as an inevitable and benevolent personal good.

2.3.1.2 Bellabeat

Another example of this presentation of surveillance as a personal good can be found in the connected jewellery startup *Bellabeat*. *Bellabeat*’s website[viii] sells app-connected watches and amulets that look like conventional, non-connected jewellery. The amulets can be worn as a necklace or clipped on to clothing This is clearly a subjective thing to say, but, in our view, these are attractive devices that can easily blend in with outfits. The company has prioritised aesthetic appearance and clearly made it a design goal to reduce how obviously it is a tech product rather than a piece of jewellery.

These devices connect to a smartphone app and monitor sleep quality, and steps and calories burned, log meditation, predict stress, and track periods and fertility.

Bellabeats '*Mission*' page[ix] says that, "Through beautifully designed technology, we aim to inform, inspire and motivate women around the world to become the best version of themselves." Elsewhere on that same page, they make the following statements:

- "The first step to improved wellness. Collecting data on activity, sleep, and reproductive health also allowed us to create a unique algorithm that will let you know when you are physically more susceptible to stress. And as they say, with knowledge comes power."

- "What can influence physical wellness. There are many factors that will influence your physical health. What can often be most difficult is staying motivated and remembering to create personalized goals. We will help you build healthy habits and view your health through a complete picture."

- "How to reach mental wellness. Our Bellabeat app is constantly growing in content we offer, as well as connecting all of our products into the perfect wellness experience. It will keep you motivated through supportive card prompts, give you a chance to share your progress online and offer ways to deal with stress."

- "Creating a spiritual wellness experience. You will get a chance to clear your mind and relax through breathing and meditation exercises. They come in the form of audio guided meditations, and ambient sounds inspired by binaural beats. It can be hard to shut the world out and let go, so we'll help you create a calming environment that will recharge you after or during a hard day."

The effect of this language is to present data collection and self-surveillance as a route to mental and physical health, reduced stress, greater self-control, higher levels of motivation, and an increased ability to switch off. There is an implicit assumption that you will not be "the best version of yourself" without this quantification-supported striving that buying and using *Bellabeat*'s products will enable.

It is important to note that *Bellabeat*'s privacy policy[x] does contain information about what data is collected by the devices and the app. Because of this, we can see that the devices collect, for example:

- "Your communications within our applications", and

- "[i]Information related to pregnancy and general health, such as the first day of the last period, menstrual cycle, date of conception, *audio recordings*, estimated due date, activity goals and other health goals." (emphasis added).

We should point out that it is not clear how “audio recordings” are relevant to pregnancy or general health and collection of audio recordings could be potentially very invasive. It is possible that the app allows for some sort of audio journalling or diary but we have not been able to establish the purpose of this data collection.

The listed purposes of data collection included:

- “To operate and improve our products and services;
- To manage the Service;
- To provide features available in the Service;
- To develop, improve, and protect the Service;
- For market research;
- To audit and analyze the Service; and
- To ensure the technical functionality and security of the Service.”

One of the reasons that *Bellabeat* says it may share data with third parties is:

> “To our subsidiaries and affiliates or a subsequent owner, co-owner or operator of the Service and their advisors in connection with a corporate merger, consolidation, restructuring, or the sale of substantially all our stock and/or assets or other corporate reorganization, in accordance with this Privacy Policy.”

The softness, inclusivity, and openness of the language on the *Mission* page is absent in the abstract and legalistic language of the privacy policy. The privacy policy appears to be treated as a legal compliance document which minimises the company’s legal liability rather than a way of ensuring that customers are actively aware of how data about them will be collected, used, and shared.

These are wider issues with the growing ‘wellbeing’ industry which this kind of IoT devices are part of. Critics such as Barbara Ehrenreich, working mainly in the US context, have taken issue with the turning of natural processes of ageing into a pathology to be treated.[xi] William Davies takes aim at what he terms *The Happiness Industry,* which he claims has turned us into self-obsessed narcissists.[xii] However, it is difficult to see where to draw the line. It seems to be near ubiquitous that companies that sell products which are designed to improve mood, circumstances, and other aspects of someone’s life point out where you could make improvements to make their product appealing. This seems an inescapable trend in marketing and commerce, which is amplified in this sector to a point that can raise ethical questions in some cases.

2.3.2 Efficiency and cost-cutting in products aimed at businesses

Finding ethical values within the websites of companies whose business model relies on sales to business is particularly difficult. The predominant proposition by such 'b2b' companies is efficiency: lowering costs, saving time, optimising use of space, increasing employee productivity.

We have two examples of this here. The first example is of Ubiquisense which sells sensor equipment for buildings and the software to analyse the data from the sensors.[xiii]

Ubiquisense presents these use cases of Smart Office, Smart Building and Smart Retail for their product.

> **Smart Office**
> *Smart sensor solutions enhance workforce productivity*
>
> Right-sizing: re-size and re-arrange your meeting rooms according to your occupancy data.
>
> Contextualise: Understand your room usage and performance by adding another layer of building data.
>
> Seat vacancies: easily spot where the nearest available work station is located
>
> **Smart Building**
> *Smart Building Technology and sensors enable energy savings*
>
> Availability: better forecast your floor space demand by calculating data on how it is being used by occupants.
>
> Room status: control indoor lighting and air quality as a function of occupancy. Achieve optimal working conditions throughout the day.
>
> Presence detector: Support your worker' need to concentrate and be creative by ensuring efficient utilisation of phone booths, breakout spaces and office pods
>
> Better services: adjust cleaning and catering according to the actual usage of each meeting room.
>
> **Smart Retail**
> *Smart Retail solutions based on sensors – Know your customer behaviour*
>
> Path analysis: track how your customers move around your store and adjust shelf design and product display accordingly

The second example is H&D Wireless[xiv] which makes chips which allow real-time locating of items or people to which the chips are attached. The use cases suggested on the H&D

Wireless website include tracking materials as they travel through factories and tracking people as they walk around amusement parks and shopping centres. In the area of hospitality, these capabilities are communicated using language such as the following:

- Increase your revenue by customized marketing inside or outside the park.
- Efficient flow - Plan and improve your business based on real guest movements.
- The management of the facility can simplify and lower the operation cost of the hospitality facility.
- The user gets a map of the facility and can monitor events and position in real time.

The company communicates the benefits of its products in industry using this language:

- Full visibility of your material handling processes.
- 20-30% reduction of transport damages.
- 20-30% utilization improvement of Returnable Transport Packages (RTP:s) [sic].
- Improve production flow.
- Identify and eliminate production logistics bottlenecks.
- Real time Work-In-Process (WIP) monitoring.
- Pre-Integrated for SAP Users.”

The language used by these two companies is very firmly in the area of finding quantifiable efficiencies. In the previous section, we discussed the presentation of surveillance as a personal good. We could see surveillance being presented here as being a commercial good and for the purposes of cost-cutting. We might expect a product with the potential to save energy consumption such as the workplace sensors made by Ubiquisense to make some mention of how they could reduce a company’s environmental impact. We could not find any examples of this, however. In summary, ethical values have been difficult to identify in the language used by these companies which market to other businesses. We have seen far greater emphasis placed on how a product can help a company reduce costs.

3. Reworked PESIA Structure and Questions – Privacy section

We have reorganised the original PESIA questionnaire as described in Deliverable 4.3. We have also provided commentary which would be intended to help users of the PESIA know how to answer the questions.

The adopted approach in the restructuring and commentary is informed by the company analysis above, ORG’s experience of working in the policy area of data protection, our experience of analysing privacy policies and the communication of privacy-related information, and our own experiences of creating privacy policies. All of this has given us insight into how we can make the PESIA questionnaire easier for practitioners to understand, use, and put into practice. A large part of the added value of this new questionnaire is in our efforts to consider the users of this questionnaire and think about how

Question	Comments to help PESIA users answer the questions

this would need to be presented for it to be useful to them. This includes the reordering of the questions and the comments that give some insight into how to go about answering the questions.

We fully expect to make further changes to the structure and wording of the questionnaire once it has been translated into a digital product and tested with real users.

SECTION 1. PROCESSING AND LAWFULNESS BASIS	
1. Does the project involve the collection or generation of information about individuals?	IoT devices may not just "collect information" but generate data through sensors and user interaction that it is then transmitted elsewhere outside the device. Make sure that you consider all forms of data that and information. Personal data[xv] is information that relates to an identified or identifiable individual. This will be easy to establish when you are dealing with names or other clear identifiers such as IP addresses or cookies. In some cases, it may be difficult to establish whether the data is personal, for example if you only collect sensor data without any identifiers. In this situation you need to consider whether that data can be linked to other information you may be able to access. If you use anonymisation techniques after collection answer yes here and fill the relevant questions, including details about the anonymisation process in the section on technical measures. There are growing concerns about the risks of re-identification of anonymised data.
1a. If no, consider other ethical and social aspects. Go to the section on ethical and social assessment	Many IoT devices will generate data that may not be directly linked to an individual, but which will still have privacy or ethical implications. For example, the advanced models of robotic vacuum cleaners from Roomba make digital maps of users' homes in order to improve their efficiency. A minor scandal broke out when their CEO was quoted over plans to sell that data, which were later denied by the company[xvi]. That data may not be personal if it is not linked to an individual. It will just be the plan of a house somewhere in the world. However, selling that data would still raise ethical issues, and indeed the idea generated a great amount of controversy, even if it is unclear that privacy laws would have been broken. The company is currently partnering with Google to make that data available to other smart home devices.[xvii]
2. What authorisation or rationale do you have to use that information?	
3. Are users required to provide information	Your users may have a user name and password or other identifier, but this question covers real life identifiers, such as

about themselves in order to use the device or access certain functions?	names biographical data, or personality related preferences that may be required for configuration, etc. Collecting biographical data that is not strictly necessary is generally a bad idea. For a start it is very difficult or impossible to change. If you ask someone where they went to school, they cannot undo that if your system is later compromised. In addition, that data is increasingly easier to access. Old schools, place of birth and mother's maiden name can be available in public online registers. Finally, such data is the basis of identity theft. If you need to collect biographical records make sure you have a god reason. Above all avoid using such information for "security questions".
4. Are users required to give consent in order to proceed at any point?	You should explain how you obtain the consent of the user. E.g. whether asserting consent is required for the system to function or whether you operate on the basis of consent but there is no barrier.
4a. If yes, do you follow GDPR requirements?	Under EU data protection law, GDPR, consent must be "freely given, specific, informed and unambiguous". This is one of the areas that has generated a lot of concern among companies. There is very detailed guidance from many data protection authorities.[xviii] Freely given means that users should not be forced to agree, it has to be a real choice. If there is a detriment to the user, e.g. very negative consequences or the device is useless without the data, there is no real choice. Imbalances of power, such as an employment context, make freely given consent inviable. Consent bundled with general Terms and Conditions will be presumed not to be freely given. If the data is necessary for the performance of the service you should not use consent, but see below. If it is not necessary, then you cannot bundle it. Specific consent means that users agree to each different use of the data with a good level of granularity. Agreeing to have your data processed for an enhanced service is not the same as agreeing to the sale of the data.

	Using generalities is not OK but neither is confusing users with too much detail. Finding the right balance between detail and overwhelming users is not straightforward. Explain how you try to achieve this. There is no completely right or wrong answer here. Informed consent mean that the user needs to be provided with enough information in plain language about the data you will use and how, as per above. The requirement for unambiguous consent means that you cannot use pre-ticked boxes or rely on the user simply continuing to use your device or systems. You need an affirmative action, typically ticking a box. It is OK to ask for consent in the context of a specific process, like with a pop up.
4b. If no, on what basis do you make use of personal data?	It is very important to have clarity on the separate legal bases for processing data. Different data processes can have a different basis. For example, you could use consent to obtain financial data, but later on if you have to disclose that data to the authorities you will likely do it under a legal obligation. Think this through and make sure you separate all the uses of personal data and can justify why you can do each of these. Importantly, other than consent, all other provisions require *necessity* for the use of data. The barrier is higher.
i. Is the use of data necessary for the delivery of the agreed service or under a contract?	As mentioned above, be careful not to mix this up with consent.
ii. Are you required to do this by law?	You may not need to explain this to the users in detail (a reference to the specific legal obligation is considered enough in several EU countries), but you should know yourself and keep a record.
iii. Are you doing it in order to protect someone’s life?	In life or death situations, you are allowed to use personal data, for example by sharing it with emergency services. This can mean the life of anyone, not just your users. But you have to be careful not to overstretch this provision, particularly with health data. Long term damage to health or other risks are not covered, only emergencies.

iv. Is it needed for some public purpose defined in law?	This applies where you are not mandated by law to do anything but if you do it, it would be under a legal provision. Public interest is typically applicable to public sector organisations but, in some cases, it can cover private actors. Examples of tasks carried out in the public interests include taxation, reporting crimes, humanitarian purposes, preventive or occupational medicine, public health, social care, quality and safety of products/services, and election campaigns.[xix] However, this is not a blank cheque. The public interest tasks are defined by law and data protection regulations or other laws at national level may require you to adopt specific safeguards to comply with. If you are not sure you are almost certainly not able to use this justification.
v. Is the processing necessary for the satisfaction of the legitimate interest of the controller?	Legitimate interest is a controversial concept in data protection. These are catch all terms that can cover anything an organisation does that is *necessary* for its business. Another important requirement is that the uses of data under legitimate interests must not be overridden by the interests or fundamental rights and freedoms of the individual. For this reason, you need to carefully balance your interests with data subject's interests, fundamental rights and freedoms and this is not always easy. The rule of thumb criteria is whether your users would be shocked or surprised (reasonable expectations). Examples of valid legitimate interests include fraud protection and general uses of employee or client data. Finally, legitimate interest is not enough to process special categories of personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation)
5. List all the types of personal data collected or generated in the project (specify sensitive data)	You should make a table with all the types of personal data that you collect or generate. Special categories of sensitive data are defined in GDPR: racial or ethnic origin; • political opinions; • religious or philosophical beliefs; • trade union membership; • data concerning health or sex life and sexual orientation; • genetic data; and • biometric

	data where processed to uniquely identify a person. These categories of data receive a higher level of legal protection[xx]. For example, in some countries like Spain you cannot even use consent to handle such data. Using such sensitive data automatically triggers a risk flag in your assessment and requires specific checks to ensure compliance. In some countries other types of data can be treated as sensitive; for example, criminal convictions and offences in the UK.
6. Which are the purposes of the processing?	Explain how you will use the data
7. Are new technologies used which might be perceived as being privacy intrusive (e.g. facial recognition, use of biometrics)?	
8. At the moment of the data collection, is a clear notice (and if applicable consent) given to the user?	There is a requirement for concise, transparent, intelligible and clear information to be provided. This is independent of whether you rely on consent or other legal bases.
9. Can users easily withdraw their consent?	You should make it as easy to revoke consent as it was to obtain it in the first place. For example, if you used a simple tick box on a website you should not require a postal letter.
10. Who else has access to the persona information?	In the table, list for each type of data who may receive it.
11. Where do you get the personal data from?	For each type of data explain whether you obtain it from your users themselves or from third parties?
SECTION 2. QUALITY OF THE COLLECTED	

INFORMATION	
12. Is the personal data you collect or generate necessary for the stated purposes?	Are you satisfied that you cannot use other means to achieve the required objectives? Check for each data and purpose. Data minimisation is a fundamental principle of data protection to consider in everything you do.
13. Is the personal data you collect or generate used for different than those established and communicated to your users?	At this point you should have a good understanding of what you thought - and told your users - you were doing with their personal data and what you may actually be doing in reality. Now is time to check whether there is too much divergence. One of the fundamental principles of data protection is “purpose limitation”, meaning that you should only use the data for the purposes you collected it for and never for “incompatible purposes”. Incompatible purposes are not defined as such in the law, but the general criteria are how removed it is from the original purpose and what would be the impacts. As a rule of thumb anything your users may find creepy or shocking could be incompatible Incompatible purposes may be a breach of data protection law and you should check this further if unsure. At least you may want to change the information you provide to your users.
14. Do you have any procedures in place to check the information you collect is accurate and up to date?	You should make a reasonable effort to maintain the quality if the data you process.
15. Do you store personal data?	Yes or no Storage could cover building persistent databases, temporary logs, etc. Data stored in RAM or other transient copies may not count, unless there is a clear risk that it can be exploited. You may need to check with your partners and suppliers whether they store data.
15a. If no, skip to section 3.	
16. For how long is information stored?	

17. Are there any technical impediments to supporting access rights due to how data is stored?	Some companies keep personal data in separate databases, ostensibly to protect the confidentiality of the information. But in so doing they may make it very difficult to ensure that data can be accessed, corrected or deleted by data subjects. For example, a company could store the recordings of its voice assistant in a database with a device identifier that is not directly linked to the user name. When users try to obtain a copy of their own recordings the company would be unable to comply with their request because it cannot easily link their recordings to the person. The company's feature provides more "privacy", but it also clashes with privacy rights.
18. Which storage mechanisms/procedures are provided? (centralized databases, archives, smart card, and so on)	
19. Is there a records management policy in place which includes a retention and destruction schedule?	
20. If information is converted in anonymous information, are there procedures which ensure the irreversibility of the process and the impossibility to re-identify data subjects?	
SECTION 3. RIGHTS OF DATA SUBJECTS	
21. Can your users exercise their rights in a simple way free of charge?	
22. How do you check the people who ask for their data are who they	You should not give someone other people's data, but neither should you impose excessive conditions that make the exercise of data subject's rights too difficult.

say they are?	
23. Do you have systems in place to make sure you reply to every request from data subjects?	
24. If someone asks, and are able to provide the required identification, are you able to confirm whether or not you process their data?	
25. Can you give users access to their personal data?	There may be some limitations to the right to access due to competing interest and rights.
26. Can you rectify and wrong or mistaken information after being notified by users?	Is the information stored in such a way that you cannot change it?
27. Might data subjects have the opportunity to obtain from the controller restriction of processing?	
28. Can users get their personal data erased upon requests without undue delay?	The right to erasure, also known as the right to be forgotten has generated a lot of controversy. In principle you have to delete the data when asked to do so, including when a user withdraws their consent. There will be circumstances where you don't have to delete the data, for example to keep it for auditing or security purposes. This can be a complex issue and you may want to check guidance from the relevant authorities[xxi].
29. How can your users know you have complied with their requests for rectification, erasure or restriction?	
30. If requested, is information provided by the controller in a structured, commonly	GDPR creates a new right to data portability. This is very important to avoid people being locked into a particular platforms or technical system. Being a new right there is little best practice to follow upon, but in principle you should provide data in a

used and machine-readable format?	structured, commonly used and machine-readable format such as CSV. It is important to understand the difference between data portability and the right of access. Portability only applies to information provided by users and not that created by you. This can be a grey area sometimes. For example, your device may collect data like heart rate -covered by portability – which you then convert into an estimate of effort or stress, not covered. You may want to consider how strictly you want to apply the scope of portability and be more generous with your users. Also keep in mind that users still have the right to have a copy of their data, just not in a specific format with the view to take it somewhere else.
31. Might data subjects have the opportunity to transmit those data to another controller without hindrance from the controller to which the personal data have been provided?	Ideally the portability format should be a standard that other similar products would use. Many fitness and sports applications with GPS use the proprietary file formats such as FIT and TCX, from the company Garmin, for data exchange. There is less consistency in other sectors. The law does not compel a company to accept the data from another company, but you should not cause any undue issues to users who want to use your data elsewhere.
32. If decisions are based solely on automated processing, including profiling, which produces legal effects concerning, might data subjects refuse to be subject to this kind of decision?	
33. Are there procedures which allow data subjects to know the evaluation criteria of the automated individual decision-making?	

SECTION 4. TRANSFER	
34. Does the project involved transfers of personal data outside the EU?	The UK is in a special case here. Until Brexit takes place transfers of data to the UK are the same as to any other EU country. International transfers of data outside the EU can only take place under fairly strict conditions. European countries have identified a high privacy risk in the handling of personal data in countries that lack adequate levels of data protection in their laws. This is not just about bureaucracy for its own sake. IoT devices in the home can offer a window into people's private lives. In some cases, quite literally, as in the case of unsecured IP cameras without proper security. Check where your partners and service suppliers (e.g. cloud service providers) have their operations. You need to have a proper system for your sharing of data with partners and be satisfied that they have systems in place for any transfer they may do outside the EU. Independently of any arrangements, organisations anywhere in the world that offer services to people in the EU must comply with GDPR. These companies need to have privacy policies and security mechanisms in place, be able to delete data on request, etc. List all non-EU countries where personal data may be handled or stored.
35. Is there an adequacy decision in relation to the third State importer of personal data?	If there is an official decision on the adequacy of the data protection regime of the country, personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework) as providing adequate protection.
35a. If no, skip to section 5.	

36. In the absence of adequacy, are there any other safeguards?	Sending data to a non-EU country not covered by an adequacy decision is not straightforward. The rules are complex and can be daunting for a small company. You should be able to explain how any data you send out of the EU is not creating a risk for your users. GDPR provides several mechanisms and safeguards for this to happen. Many of these safeguards, such as Binding Corporate Rules, are not adequate for SMEs or independent developers. However, if you use a third-party service there is a chance that they rely on Binding Corporate Rules or EU approved model or standard contract clauses. Check for these terms in their documentation. Standard model clauses approved by the European Commission can be added to contracts with partners or service suppliers.[xxii] Data protection authorities are legally allowed to authorise bespoke contracts but at present the authorities of many European countries refuse to do this, so standard model clauses from the EU remain a better option. If you try to use standard model clauses yourself in a contract with a non-EU suppliers we would recommend you obtain legal support. Other mechanisms will become available in the near future, such as certification schemes or codes of conduct. These are not ready at the time of writing so beware of any claims by suppliers in this regard.
36a. If no, skip to section 5.	
37. Can you use any of the exceptions approved in the law?	GDPR provides for various exceptions to the rule. As the name indicates these provisions are designed to provide avenues for the routine uncontrolled flow of data towards places without safeguards. You should not try to justify retrospectively any transfers using such exceptions as an argument. You still have to inform your users of any transfers and the mechanisms applied.
37a. Have you obtained consent form users?	A common mechanism to send personal data outside the EU is to obtain consent. This should follow the principles outlined

	elsewhere. You cannot just ask for consent for international transfers in general. You must explain what data is going where and what the risks may be, such as the lack of appropriate enforcement in case of any problems.
37b. Is the transfer necessary for the performance of a contract?	The transfer can be allowed if it is *necessary* for the performance of a contract between you and your users or clients, or for the implementation of pre-contractual measures taken at their request. Contracts between you and third parties to provide a service to your users are also allowed. It is important to remember that this and other exceptions only apply to occasional transfers. If you need to routinely send data you need to get consent or find an approved safeguard. For example, you may include standard model clauses in your contract.
37c. Is the transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person?	
37d. Is the transfer necessary for important reasons of public interest?	Considering the very specific nature of this case, you should justify in detail.
37e. Is the transfer necessary for the establishment, exercise or defence of legal claims?	
37f. Is the transfer necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent?	This exception mainly applies to medical emergencies, for example, but not general treatment.

37g. Is the transfer made from a public register?	This only covers registers created under a legal basis, e.g. company or land registers, and not private registers such as credit reference. You cannot make wholesale transfers.
37h. Are you using exceptional legitimate interests?	GDPR provides for a final very restrictive backstop mechanism for when a transfer is absolutely necessary for your legitimate interests, there are no other options, and it concerns only a limited number of data subjects. In order to do this, you need to inform the data protection authority of your country. You should be very careful if claiming this exception.
SECTION 5. PROCESSORS AND PERSONNEL AUTHORISED TO ACCESS INFORMATION	Data *processors* are the partners and service suppliers that handle personal data on your behalf. As data processors, they have a specific and detailed legal status in GDPR. If they breach any privacy laws you could be held responsible, so you need to be very careful.
38. Do you have contracts with any processors or other legal documents defining your relation and the sharing of data?	This may be straightforward with companies where you pay for a service but check any online tools you may use for their terms and conditions. It is a legal requirement to have some form of GDPR compliant contract with processors.
39. Are the instructions to the processor outlined?	The difference between you as a data controller and a processor is precisely control. If your providers set out the terms on which they use data without your say they may well also be a controller. Online service providers – analytics, cloud or AI workbench - could fall in either category and establishing this may not be completely clear. For example, there has been a lot of controversy over Google setting in its terms of service when it is a processor (e.g. Google Cloud or Analytics) and when it is a controller (ad exchange)[xxiii]. In an IoT environment you can have situations with more than one controller and even joint controllers.[xxiv] In that case you need to identify the responsibilities and the applicable supervisory authorities and may need to consult guidance on this topic[xxv]
40. Might the processor engage another processor under the prior	Your data processors are not allowed to further outsource the handling of any personal data without your permission.

authorisation of the controller?	
SECTION 6. SECURITY	
41. Is a data protection officer or an information security officer appointed?	
42. Does the controller implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation?	
43. How do you minimise the data to what is necessary?	The principle of data minimisation is central to data protection. In previous sections, you have already considered whether all the data you use is *necessary.* Now you should explain what specific practical measures you have taken or will take to make sure this minimisation happens. This could include design decisions to restrict certain sensors, delete data that is automatically generate, etc.
44. How do you control access to personal data and its use by staff?	If you have subcontracted some of your work or engage collaborators, you should have clarity on who has access to what data and what they can do with it, whether they are staff or external providers (likely processors). The company is responsible for their staff. You cannot treat them as if they were processors, but this gets complicated. Many small organisations rely on a very dynamic and flexible structure and the definition of employee, external contractor or temporary worker varies in different countries. You will need to make an assessment.
45. How are staff informed of your security procedures?	
46. Can you be sure that	

staff only access data that is necessary for their functions?	
47. Do you use unique individual accounts for your staff members that allow for personalised authentication and access controls?	
48. Do you keep an access register to the IT systems containing personal data?	
48a. For how long is the access register stored?	
48b. Do procedures exist which allow the DPO or the IT security officer periodically to check the access register?	
49. Are there procedures or mechanisms to create backups?	
50. Does the controller periodically verify the proper functioning of security procedures and measures?	
51. If you maintain your own infrastructure, are there controls of physical access to the places where personal data are stored?	Please consider that, in many cases, developers will use cloud systems.
52. What security measures do you have in place for personal data?	The security of personal data is a fundamental principle in data protection. You need to make sure you protect information against theft, loss, unauthorised access, use or disclosure or unauthorised copying, modification or disposal.

	Security measures could be: - Technical: encryption and pseudonymisation techniques, disaster recovery plans, backups, operational continuity plans. - Physical: locks, reinforced doors, window bars. - Organisational: rules and procedures.[xxvi]
53. Is there a data breach management action plan in place?	
54. Did the controller, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data?	
54a. Did the data protection impact assessment indicate that the processing would have resulted in a high risk in the absence of measures taken by the controller to mitigate the risk?	
54b. Since the high risk indicated by the data protection impact assessment, did the controller consult the supervisory authority prior to processing?	
54c. Will the controller carry out a data protection impact assessment?	
55. Does the controller join code of conducts or adopt certification mechanisms?	

SECTION 7. RISKS MANAGEMENT	
56. Does the technology allow to perform evaluation or scoring of the data subjects?	
57. Does the technology allow the collected data to be easily matched or combined with other data sets?	
58. Does the technology allow the collection of personal data on a large scale?	Your intuitive assessment of your project will likely include an understanding that size and volume matter and that something that affects large numbers of people will be inherently riskier than a project that only impacts a small number. This principle is embedded in EU privacy law. Large scale is a very important term in privacy compliance, but unfortunately there is no simple clear definition. There is some guidance on what may constitute large scale, considering: • The number of people concerned - either as a specific number or as a proportion of the relevant population. • The volume of data and/or the range of different data items being processed. • The duration, or permanence, of the data processing activity. • The geographical extent of the processing activity. Accepted examples of large-scale data processing include: • travel data of individuals using a city's public transport system (e.g. tracking via travel cards); • real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialized in these activities; • customer data in the regular course of business by an insurance company or a bank; • behavioural advertising by a search engine; and • processing of data (content, traffic, location) by telephone or internet service providers. Some national data protection bodies have set clearer criteria, such as specific thresholds, say 5,000 people if dealing with criminal convictions, but this is not the case in every European

	country[xxvii] . It is important to keep in mind that this does not mean that individual breaches of the right to privacy are not important. If you are dealing with large scale processing, you will need to take a formal data protection impact assessment. See official guidance if required.[xxviii]
59. Does the technology allow the collection of personal data in contexts that are private?	Private contexts could refer both to private spaces, such as the home, or to private situations, such as devices that could record private conversations. By the way, some contexts will have an added level of confidentiality. For examples, journalists dealing with sources, lawyers with their clients or doctors and patients.
60. Does the technology allow for the collection of sensitive personal data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, biometric data, data concerning health, sex life or sexual orientation) or data relating to criminal convictions and offences?	In the first section you listed all the types of data involved in the project, included all sensitive and special categories. At this stage, have another look at your technical system and think whether you may be collecting such data even if inadvertently .
61. Does the technology allow for the collection of personal data whose leak could risk damaging the data subject?	This question aims at establishing whether there are any special concerns above the legal and ethical obligation to deal with personal information in a fair and secure manner. Examples of enhanced risk could be financial data that could be used for fraudulent payments.
62. Does the technology allow the collection of personal data referring to vulnerable subjects?	European data protection bodies have issued guidance on this issue[xxix]. Vulnerable data subjects may include: • children, or any people that can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data,

	• employees or any case where there is an imbalance of power in the relationship between the person whose data is handled and the person or organisation doing it, • segments of the population requiring special protection: mentally ill persons, asylum seekers, or the elderly, patients, etc.
63. Does the technology allow to observe, monitor or control data subjects in a systematic way?	Systematic monitoring is considering a higher risk because it is more likely that people will, not be fully aware. This could be because the people affected will at some point normalise the collection of data and "lower their guard" or simply because by collecting data all, the time you increase the likelihood that some people will not be aware.
64. Does such collection take place in a publicly accessible area?	Collecting data in publicly accessible spaces increase the risk that people affected will be unaware. Additionally, it may be impossible for individuals to avoid having their data taken.
65. Does the technology allow the data subjects to be aware of the monitoring in process?	This is a particularly relevant issue in the context of IoT. Ambient computing and devices without an obvious interface can make it hard to know when data is being collected.
66. Is the data subject able to avoid such monitoring and control?	This may be the case in public spaces, but also in other circumstances such as when wearable IoT devices are worn by users. Glasses with cameras and microphones, for example.
67. Does the technology allow (full or partial) automated-decisions to be taken with regard to the data subjects?	Examples of automated decisions are common in computing. Scoring systems and online recommendation systems are clear examples, but a core premise of IoT is to automate daily life to provide convenience. Automation does not always require the creation of personalised profiles, but these two activities tend to go together. Learning your users' habits will be profiling.
68. Do these automated decisions have a significant effect on the users of the system?	Will the decision have the potential to significantly influence the circumstances, behaviour or choices of the individuals concerned? At its most extreme, could the decision lead to the exclusion or discrimination of individuals? The typical examples of such effects would be credit applications or recruitment. In the world of IoT a prime example of significant effects would be systems that trigger medical alerts.
69. Does the technology allow for human intervention in the decision process?	

69a. If yes, is such human intervention enough to prevent risks to the rights of the data subjects?	Is the intervention able to steer the process and have a significant impact on the outcome? Rubberstamping a computer decision may not be enough.
70. Is the technology that I am developing new in terms of the potential impact on data subjects?	If the technology in the system is new in terms of how it processes personal data you will likely require a formal data protection impact assessment. Defining what counts as a new technology is of course open to debate, but similar problems with defining what is the state of the art are encountered in other areas, such as patents. New applications of existing technologies to solve novel organisational issues will also count as new. For example, combining the use of fingerprint and face recognition for improved physical access control.
71. Am I using a product/component developed by others who have already carried out a DPIA?	
71a. If yes, check whether the producer is willing to share the DPIA and integrate such a DPIA in your own assessment.	
72. Am I developing a technology similar to others that are being developed?	
72a. If yes, consider the possibility to carry out a joint DPIA.	
73. Are there codes of conduct that could be taken into account?	
74. Have I clearly identified the nature, scope, context and	Review your responses to this section and check that they describe the activities you intend to pursue.

purposes of the processing operations?	
75. Have I identified the assets on which the personal data rely (e.g. hardware, software, people, paper…)?	
76. Have I consulted all the subjects that are involved in the processing operations (e.g. the DPO, the processors)?	
77. Is it feasible to consult the data subjects or their representatives on the impact of the technology on their rights and interests? If yes, have I done so?	Consider doing some focus groups or interviews. You could incorporate privacy and ethics research as part of your general user or market research. The best way to avoid conflicts and potential rejections from users is to ask them early for their views.
78. Have I envisaged measures to restrict the collection and further processing and storage of data to what is strictly necessary for the purposes of the processing?	
79. Does the technology make it possible to provide the data subject with all the necessary information regarding the processing?	You may have an issue if you use “black box” components or third party services, but remember that if they are processors they should only be doing what you tell them with the personal data of your users.
80. Does the technology allow the collected data to be modified and erased?	
81. Have I clearly identified the risks to the rights and freedoms of natural persons?	

82. Have I assessed the severity of such risks?	
83. Have I assessed the likelihood of such risks?	
84. Is there anything inherent in the technology that would hinder you being able to give your users their data to take it to another provider of a similar device or service?	
85. Have I identified specific measures for each of the assessed risks?	
86. Have I identified measures to mitigate risks of illegitimate access, modification or disappearance of the data collected by the devices?	
87. Is it possible to publish the DPIA partially or in a summarised way without hindering the rights of the technology developers or of the data subjects?	
88. Are the measures that I have designed sufficient to mitigate the risks to the rights and freedoms of the data subjects? If the answer is no, have I consulted the national supervisory authority?	

4. Reworked PESIA Structure and Questions – Social and Ethical sections

The PESIA questionnaire includes social and ethical aspects, but we are dealing with these in a different manner at this stage. These questions require more context and will be more closely associated to scenarios and case studies. In the tables below we include some of the questions we are currently exploring based on the scenarios from the previous deliverable D4.3.

In deliverable D6.3, which will consolidate the tools into a service after further testing with users, we will expand the case studies and eventually aggregate the questions into a structured library around values, for the user to pick the relevant ones for her case.

The final service tool will fully integrate the ethical and social aspects into a single impact assessment process. The tool will enable the users to introduce mitigation strategies and measures for any risks identified. We will build different user experiences for developers working at different stages of development. For example, the questions for early concept ideation will be very different from those for a project that modifies an existing operational system.

The corresponding measures will also be different. In some cases, the concept can be modified, or the design changed in a simple manner, while existing systems may require organisational measures to reduce the risks.

Another aspect that we will incorporate in the final service is a better integration of the risk-based approach with wider ethical deliberations. Impact assessments are by their very nature tools that support a specific approach to risks: a graduated response proportional to the perception of the severity and likelihood of specific risks. This approach has many advantages in allowing for limited resources to be focussed, but it also has many potential issues: limitations in the identification of risks, uncertainty and subjectivity in assessment and ranking of priorities are well known.

More broadly a risk-based approach can lead to the substitution of fundamental limitations in technologies with mitigations ex-facto. This problem has been identified in the field of cleaning operations for environmental contamination, where risk-based approaches have been blamed for hindering developments on source removal technologies, being displaced by containment technologies.[xxx] A similar issue appears in digital technologies, with a clear preference by developers for technologies such as anonymisation instead of data minimisation at source.
Risk based approaches fit very well with the more utilitarian perspectives on ethics but can be harder to square with other ethical perspectives. Making assessments will be a core element of the practical wisdom – *phronesis* – proposed in the virtue ethics

approach, but this is a much broader consideration than risk. Our service tools will open up these issues to users for reflection.

<table>
<tr><td colspan="2"><em>A company adopts an IoT-based technology to improve work productivity. All employees receive a wearable IoT device (an <strong>electronic bracelet</strong>) equipped with a GPS technology able to monitor their movements within the working spaces, including the restrooms, in order to better monitor and manage the production cycle.</em></td></tr>
<tr><td><strong>Dignity</strong></td><td>✓ Does the IoT device need to be implanted into the user's body?
✓ Is the IoT device able to transmit sensations to the user's body (e.g. vibrations, sounds, etc.)?
✓ Could the device interfere or limit the normal functionality of the user's body (e.g. exoskeletons)?
✓ Will you have any areas of the building free of monitoring?</td></tr>
<tr><td><strong>Non-discrimination</strong></td><td>✓ Will the system take into account any particular characteristics of the employees when determining their productivity, such as age, gender or disability?</td></tr>
<tr><td><strong>Autonomy</strong></td><td>✓ Will the bracelet reduce individuals ability to make their own decisions about the best route or work pace?</td></tr>
<tr><td><strong>Responsibility</strong></td><td>✓ Will there be a way to challenge any decisions on productivity made by the system?
✓ Will there be clear lines of responsibility for any outcomes, particularly between the developers of the tools and the managers to ensure that any issues are always dealt with?</td></tr>
</table>

<table>
<tr><td colspan="2"><em>A company is developing a <strong>connected doll</strong> which, to reduce its cost, will be sponsored by other companies. These sponsors cover part of the production costs and obtain that the doll provides users some advertising messages about their products.</em></td></tr>
<tr><td><strong>Accountability</strong></td><td>✓ Will you be sharing personal data with the sponsors?
✓ Have you set clear limits on what partners can do with that information?
✓ Will the doll receive advertising messages from</td></tr>
</table>

	sponsors? ✓ Will the microphone in the device have a physical switch?
Sustainability	✓ Will the servers providing remote functionalities keep functioning?
Safety & security	✓ Will the doll receive software updates for the lifetime of the product? ✓ How will you ensure the security of the data transmission? ✓ How can you ensure that children are not reached by strangers using the doll?
Openness	✓ Will the doll allow for third party add-ons or user re-programming? ✓ Will the software in the doll be open source?
Responsibility	✓ Will there be a way to challenge any decisions on productivity made by the system? ✓ Will there be clear lines of responsibility for any outcomes, particularly between the developers of the tools and the managers to ensure that any issues are always dealt with?

*A company decides to produce wearable devices that can be used to monitor health conditions. The devices are **health wristwatches** that can gather information about the number of steps walked, user’s heartbeat, her blood pressure, and other personal data concerning fitness training. The collected data can be shared with private insurance companies, credit companies and employment agencies.*	
Non-discrimination	✓ Are the IoT device and associated software used for predictive purposes or classifying users according to their conditions, behaviour and preferences? ✓ What measures will be in place to avoid discrimination?
Dignity	✓ Are the expectations of increased health realistic? Do they justify this invasive and continuous monitoring? Do you take into account the socio-economic characteristics of the users?
Well-being	✓ If you allow for comparisons among users, how will you deal with the risks to self-esteem?

<table>
<tr><td colspan="2"><i>A company is developing a smart transport system that improves traffic management and driving safety. The system requires the installation of an IoT <b>vehicle tracking device</b> inside each vehicle to collect data on vehicle position, driving styles, speed and other users' behaviours. The data collected can be shared with roadside assistance services, insurance companies and other third parties.</i></td></tr>
<tr><td><b>Autonomy</b></td><td>✓ Will the tool include some form of remote control?
✓ If any limitations to user control exist, do they happen in contexts characterised by power asymmetries (e.g. workplace)?</td></tr>
<tr><td><b>Transparency</b></td><td>✓ Has any information been provided about the project to the public? Will the vehicles display a sign?
✓ Has information about the logic of data processing been provided to drivers?</td></tr>
</table>

<table>
<tr><td colspan="2"><i>A municipality decides to adopt IoT technology to find people in the crowd (e.g. in the event of health emergency) during concerts or other large-scale events organised in the local stadium. A <b>tracking wearable</b> IoT device is provided to all participants in these events. The collected data can be shared with the private companies that organise these events, public health services and local police department.</i></td></tr>
<tr><td><b>Transparency</b></td><td>✓ Has any information been provided about the project to the interested persons or to the public at large?
✓ Has the project adopted any procedure to give the opportunity to persons to ask information about the project?
✓ Has information about the logic of data processing been provided to data subjects?</td></tr>
<tr><td><b>Sustainability</b></td><td>✓ Are the trackers reusable? How will they be disposed of otherwise?</td></tr>
<tr><td><b>Dignity</b></td><td>✓ Will users be monitored in private areas such as bathrooms?
✓ Will users be tracked outside the stadium?</td></tr>
</table>

<table>
<tr><td colspan="2"><i>A regional transportation authority develops a new multimodal service that gives passengers the opportunity to use different transportation services with the same personal IoT-based <b>smart card</b>. The regional system can potentially collect an extensive amount of mobility data concerning passengers and share them with transportation service providers and third parties.</i></td></tr>
<tr><td><b>Participation</b></td><td>✓ Have you planned to engage stakeholders in the project development?</td></tr>
</table>

	✓ In which manner have you identified the relevant stakeholders? ✓ Which forms of engagement of the stakeholders have you adopted? ✓ Do you intend to implement the suggestions provided by the stakeholders? Do you plan to present to the stakeholders this implementation for a further discussion?
Transparency	✓ Have you considered to provide publicly available information about this consultation? ✓ Which kind of information about the project and data processing have been disclosed to the stakeholders?
Inclusion and equality	✓ Will the data be used to potentially restrict transport to areas or users' groups that are deemed uneconomical?

Appendix One: The companies whose websites we analysed

This is a list of the companies, focussing on Internet of Things products, whose websites we analysed

Company	Product	Website
Little Riot	Pillow Talk	http://www.littleriot.com/
Ultra IoT		https://www.ultra-iot.com
Ubiqisense	IoT sensor solutions for Smart Buildings	https://www.ubiqisense.com/
Team Zwatt	Connected power meter that measures power output when cycling (people use this to measure their training progress) It is also a study where people buy a subsidised power meter on their crankset in return for contributing data to improving the algorithms used to analyse power output on road bikes	https://teamzwatt.com/
Kemuri	smart power sockets	http://www.kemurisense.com
M-PAYG	The pay-as-you-go solar energy system for families in the developing world	http://mpayg.com
Beryl	cycle lights	http://beryl.cc/
BleepBleeps	children bedside lamp	https://bleepbleeps.com
Idemolab/ForceTech/ Delta	IdemoLab bridges the gap between technology and design. We focus on the important early stages of the design process and strive to create meaningful experiences for users and customers.	https://idemolab.madebydelta.com/
Leapcraft	City and domestic environmental sensors	http://www.leapcraft.dk/
Provenance	supply chain	https://www.provenance.org
Tech Will Save Us	educational toys	https://www.techwillsaveus.c

		om/
Buffalo Grid	mobile charging unit	https://buffalogrid.com/
Hiber	global LGPAN	https://hiber.global/
Airtame	screen sharing device for schools and businesses	https://airtame.com
Platoscience	PlatoScience has developed the world’s first headset for enhancing cognitive performance and increasing productivity. Backed by +15 years of clinical research, neurostimulation lets you take control of your brain and release your full potential in a safe and simple manner.	http://platoscience.com/
Olitool	digital worry bead	http://www.ogenblikltd.com/
U-toys	outdoor toys	http://usmarttoys.com/
Philips	Hue lighting ecosystem	https://www2.meethue.com/en-gb
Chat Teddy	Teddy bear	http://www.chatteddy.se/?lang=en
HD Wireless	GEPS™ - Hospitality Connected wristband	https://www.hd-wireless.com/enterprise-rtls/products/hospitality/
EVRYTHNG	IoT Platform	https://evrythng.com/
Smartfrog	Camera	https://www.smartfrog.com/en-gb/
Netatmo	smart home ecosystem - heating system	https://www.netatmo.com/en-gb
ADVEEZ	Devices to monitor wellbeing of the elderly	http://www.adveez.fr/residents-safety
Sensolus	GPS trackers	https://www.sensolus.com/trackers/
Sentiance	Behaviour analysis platform	http://www.sentiance.com/platform/
Wia	IoT Platform	https://www.wia.io/

Hive	smart home ecosystem	https://www.hivehome.com/
Mystery Vibe	sex toys	https://www.mysteryvibe.com/
Nello	intercom and locks	https://www.nello.io/
Playbrush	children toothbrush	https://www.playbrush.com/en/
Zembro	Zembro Bracelet	https://www.zembro.com/uk-EN/
Filo	location tag	https://www.filotrack.com/
Narrative	wearable camera	http://getnarrative.com/#
Tado	thermostat	https://www.tado.com/gb/
CubeSensors	home sensors	https://cubesensors.com/
Noa	bikeshare locks	http://www.noa.one/
Intelclinic	Neuroon Sleep Mask	https://inteliclinic.com/projects/
iSocket	smart socket	https://www.isocket.eu/
Nokia	Whitings	https://health.nokia.com/uk/en/
Momit	thermostat	https://www.momit.eu/en/
KIWI	home lock	https://kiwi.ki/en/the-electronic-locking-system/
Teddy the guardian	cuddly toys	http://teddytheguardian.com/
Bellabeat	Leaf health tracker	https://webshop.bellabeat.com/collections/health-trackers
Visiobike	smart e-bike	https://www.visiobike.com/
Wattio	smart home ecosystem	https://wattio.com/en/
Good Night Lamp	lamp	http://goodnightlamp.com/
Keecker	multimedia robot	https://www.keecker.com/
Sensyne	certified health monitoring	https://www.sensynehealth.com/edge

Footnotes

[i] https://www.mysteryvibe.com/terms-of-use

https://web.archive.org/web/20190111052838/https://www.mysteryvibe.com/terms-of-use

[ii] https://web.archive.org/web/20150919031136/https://www.mysteryvibe.com/terms-of-use

[iii] https://www.bbc.co.uk/news/technology-35984185

[iv] https://www.youtube.com/watch?v=JDy8-sBXB1c&list=PLFNuPhM8NUdwHpxeG9y-TkBzf6pYJ01Yx

[v] https://www.nello.io/en/privacy#products

[vi] https://www.playbrush.com/en/privacypolicy

[vii] https://www.smartfrog.com/en-gb

[viii] https://www.bellabeat.com

[ix] https://www.bellabeat.com/pages/bellabeat-mission

[x] https://www.bellabeat.com/pages/privacy

[xi] https://newrepublic.com/article/148296/barbara-ehrenreich-radical-crtique-wellness-culture

[xii] https://www.theguardian.com/books/2016/aug/03/the-happiness-industry-by-william-davies-review

[xiii] https://www.ubiqisense.com

[xiv] https://www.hd-wireless.com/enterprise-rtls/applications

[xv] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

[xvi] https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html

[xvii] https://betanews.com/2018/11/01/google-irobot-house-mapping/

[xviii] https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030

[xix] https://community.jisc.ac.uk/blogs/regulatory-developments/article/gdpr-whats-your-justification

[xx] https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/25--guide-to-the-gdpr--sensitive-data-and-lawful-processing.pdf?la=en

[xxi] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

[xxii] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

[xxiii] https://techcrunch.com/2018/05/01/google-accused-of-using-gdpr-to-impose-unfair-terms-on-publishers/?guccounter=1

[xxiv] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[xxv] http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[xxvi] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[xxvii] https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/

[xxviii] http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[xxix] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[xxx] National Research Council (1999), *Environmental Cleanup at Navy Facilities: Risk-Based Methods*. Washington DC.