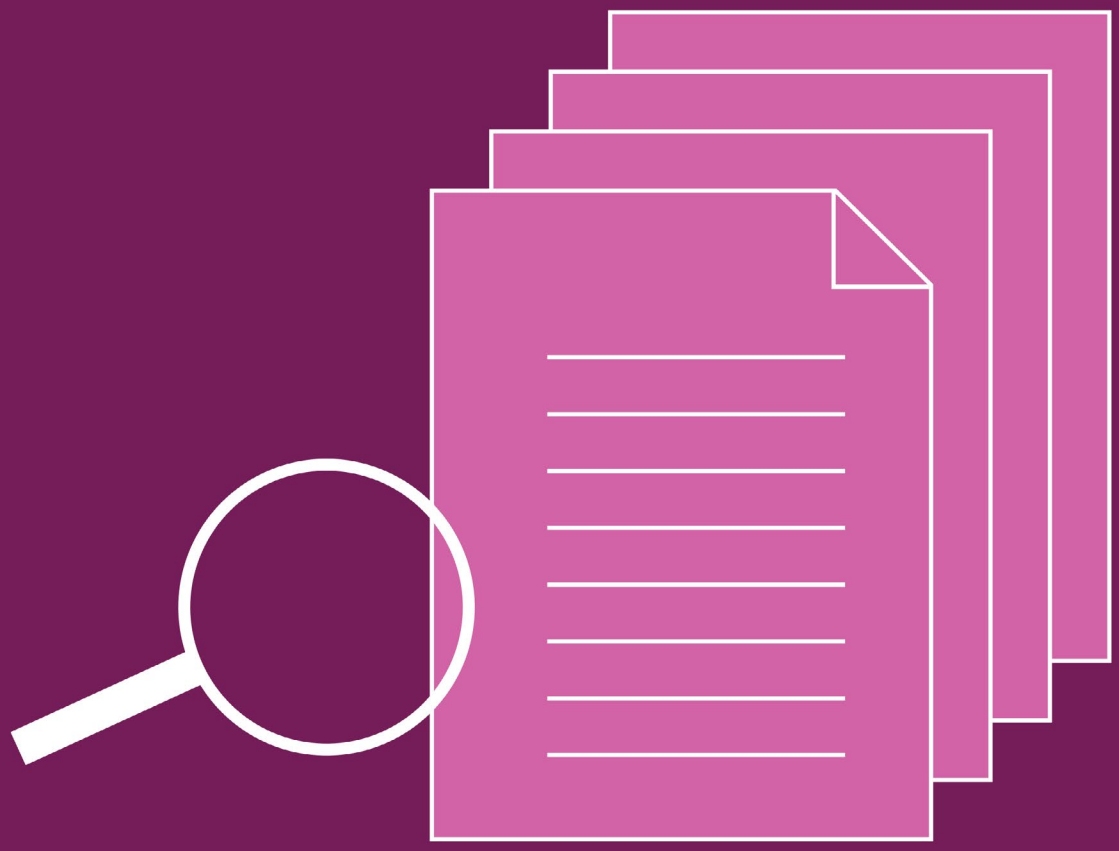
virt·eu



PESIA

Privacy, Ethical & Social Impact Assessment

This project has received funding from the European Union's Horizon 2020
research and innovation programme under grant agreement No 732027

The PESIA questionnaire goes beyond the familiar privacy impact assessment (PIA) tools, also addressing ethical and social issues respectively. This document is geared specifically towards IoT (Internet of Things) system development issues. The questionnaire is developed around the common ethical values recognised by international charters of human rights and fundamental freedoms and draws on results of the VIRT-EU project's extensive research together with IoT designers and developers.

This questionnaire is organized in 6 sections:

1. **Follows a traditional data mapping approach seen in most data privacy tools, asking questions about the origin of the data, its use and on what bases it is processed, plus establishing any further sharing.**
2. **Determines whether the project involves a high risk in terms of privacy and data protection, and has several subsections.**
3- **Looks at any processes in place or planned to handle the data properly. A lot of these questions indicate compliance of good practice. Some of these measures can be mitigating barriers to risks elicited before.**
4. **Focuses on external relations, from basic compliance with user rights under GDPR to broader participation that may not be necessarily a legal obligation, but rather a social consideration.**
5. **Looks at the risk management practices.**
6. **Presents a set of open questions to consider social and ethical impact.**

The PESIA questionnaire was created as part of the VIRT-EU project by the team at Politecnico di Torino lead by Professor Alessandro Mantelero who carried out the original legal research and drafting. The social and ethical impact question development was based in part on the research conducted by the LSE and ITU teams (VIRT-EU H2020 Project. 2018. Deliverable 4.3). The Open Rights Group, and Politecnico di Torino, tailored the questions further to the IoT context and added clarifying commentary following interviews and feedback elicited from a variety of sources (VIRT-EU H2020 Project. 2019. Deliverable 4.4).

VIRT-EU H2020 Project. 2019. Deliverable 6.3. PESIA (Privacy, Ethical and Social Impact Assessment) questionnaire. (grant agreement No 732027)

1. Data mapping	
What information is collected?	
1. Does the project involve the collection of information about individuals?	Beyond direct forms of "collecting information", IoT devices may generate data through sensors and user interaction which it is then transmitted elsewhere outside the device. Make sure you consider all forms of data and information. Personal data 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 reidentified, for example when linked to other information you may be able to access. If you use anonymisation techniques after collection, answer "yes" here and complete the relevant questions. Include 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.	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 about plans to sell that data, which were later denied by the company. 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 questions. Indeed the Roomba concern generated a great amount of controversy, even if it is unclear privacy laws would have been broken. The company is currently partnering with Google to make that digital home maps data available to other smart home devices.
1.b What kind of information is to be collected? Please LIST	

What do you want to achieve with the information?	
2. What are the purposes of the processing?	Explain how you will use the data
3. Is the collected information necessary to the purposes for which it is processed?	Is it absolutely necessary for you to collect the kinds of information you are collecting, in the way that you are collect it? Are there no other means by which you can achieve the required objectives?
Where does the information come from?	
4. Where do you get the personal data from?	For each type of data explain whether you obtain it from your users directly or from third parties.
5. Are users required to provide information about themselves in order to use the device or access certain functions?	Your users may have a user name and password or other identifier, but this question covers real-life identifiers, such as names, biographical data or personality-related preferences that may be required for configuration . Collecting biographical data that is not strictly necessary is generally bad practice. For a start, it is very difficult or impossible for users to change. If you ask someone where they went to school, and your system is later compromised, they cannot delete that information. In addition, that data is increasingly easy to access, increasing users' vulnerability. Identifiers such as 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 good reason. Above all, avoid using such information for "security questions".
6. 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.

6a. 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 on how to implement proper consent **Freely given** means users should not be forced to agree; it has to be a real choice. If opting out results in 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 collection 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 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 can be challenging . Explain how you try to achieve this. There is no completely right or wrong answer here. **Informed consent** means 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 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.
6b. If not, on what basis do you make use of personal data?	It is very important to have clarity about 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 if you later 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. This 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 collect or process the data by law?	You may not need to explain this to the users in detail (a reference to the specific legal obligation is considered sufficient in several EU countries), but you should know and keep a record for yourself.

iii. Are you processing the data 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 the processing 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 interest include taxation, reporting of crimes, humanitarian purposes, preventive or occupational medicine, public health, social care, quality and safety of products/ services, and election campaigns. However, this is not a blank cheque. The public interest tasks are defined in legislation. Data protection regulations or other laws at the 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 subjects' interests, fundamental rights and freedoms. This is not always easy. The rule of thumb criteria is whether your users would be shocked or surprised about what you are doing. This is termed reasonable expectations. Examples of valid legitimate interests include fraud protection and general uses of employee or client data. Finally, legitimate interest is not sufficient rationale for processing special categories of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for the purpose of uniquely identifying a human being, data concerning health or data concerning a natural person's sex life or sexual orientation).

Special data	
6c. In particular, specify if special categories of data are processed	Create a table listing all the types of personal data collected or generated in the project. 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. For example, in some countries like Spain, consent is not a sufficient justification for the use of 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.
Where does the data go?	
7. Who else has access to the personal information?	For each type of data in the table, list who may receive it.
8. Does the project involve 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 sharing data with partners and be satisfied 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.

9. 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.
10. 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 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 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. 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 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 yet available at the time of writing, so beware of any claims by suppliers in this regard.
11. 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 retrospectively justify any transfers using such exceptions as an argument. You still have to inform your users of any transfers and the mechanisms applied.

11a. Have you obtained consent from users?	A common mechanism for sending personal data outside the EU is by obtaining 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.
11b. 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.
11c. Is the transfer is 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?	
11d. Is the transfer is necessary for important reasons of public interest?	Considering the very specific nature of this case, you should justify in detail.
11e. Is the transfer necessary for the establishment, exercise or defence of legal claims?	
11f. Is the transfer is 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.
11g. Is the the transfer is 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.
12. Are you using exceptional legitimate interests?	GDPR provides 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.

2. Technology, Activities and Risks	
TECHNOLOGY	
13. Are new technologies used which might be perceived as being privacy intrusive (e.g. facial recognition, use of biometrics)?	
14. Is the technology you are 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 facial recognition for improved physical access control.
15. Are you using a product/component developed by others who have already carried out an impact assessment?	If yes, check whether the producer is willing to share the assessment and integrate their work in your own assessment.
16. Are you developing a technology similar to others that are being developed?	
17. If yes, consider the possibility to carry out a joint Data Protection Impact Assessment.	
18. Have you identified the assets on which the personal data rely (e.g. hardware, software, people, paper...)?	
AUTOMATION & PROFILING	
19. Does the technology allow the performance of evaluation or scoring of data subjects?	

20. Does the technology allow (full or partial) automated decisions to be taken with regard to the data subjects?	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 qualifies as profiling.
21. Do such decisions affect legal rights of the data subjects? For instance, if the data collected by the device detects alleged non-performance and possibly prevents the device from working properly.	
22. 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 who use it? 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.
23. Does the technology allow for human intervention in the decision-making process?	
23a. If yes, is such human intervention enough to prevent risks to the rights of the data subjects?	Is the human intervention able to steer the process and have a significant impact on the outcome? Rubber-stamping an automated decision may not be enough.
SCALE & BREADTH	
24. Does the technology allow the collected data to be easily matched or combined with other data sets?	

25. 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, such as 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. It is important to keep in mind this does not mean 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.
26. Does the technology allow the observation, monitoring or control of data subjects in a systematic way?	Systematic monitoring is considered a higher risk because it is more likely people will not be fully aware of its occurrence. 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 some people will not be aware.

CONTEXT & SPACE	
27. 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. Some contexts will have an added level of confidentiality. For examples, journalists dealing with sources, lawyers with clients, or doctors with patients.
28. Does such collection take place in a publicly accessible area?	Collecting data in publicly accessible spaces increases the risk that people affected will be unaware. Additionally, it may be impossible for individuals to avoid having their data recorded.
29. Does the technology allow the users or other people affected 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.
30. 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 with wearable IoT devices — for example, glasses with cameras and microphones.
31. Does the device track the location of data subjects?	
OTHER RISKS	
32. 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; trade union membership; biometric data; or 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, including all sensitive and special categories. At this stage, have another look at your technical system and think about whether you may be collecting such data, even if inadvertently .
33. Does the technology allow for the collection of personal data which, if leaked, 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.

34. Does the technology allow the collection of personal data about vulnerable people?	European data protection bodies have issued guidance on this issue. Vulnerable data subjects may include: • children, or any people who 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 the handling, • segments of the population requiring special protection: mentally ill persons, asylum seekers, the elderly, medical patients, etc.
35. Have you clearly identified the nature, scope, context and purposes of the processing operations?	Review your responses to this section and check they describe the activities you intend to pursue.
RECAP	
36. Is the personal data you collect or generate used for different purposes 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 you should only use the data for the purposes for which it was collected and never for “incompatible purposes”. Incompatible purposes are not defined as such in the law, but the general criteria relate to how removed the use is from the original purpose and its subsequent 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 the least, you may want to change the information you provide to your users.

3. How do you handle data accurately and securely?	
TECHNICAL	
37. Have you envisaged measures to restrict the collection and further processing and storage of data to what is strictly necessary for the purposes of the processing?	The principle of data minimisation is central to data protection. You should restrict the collection and further processing and storage of data to what is strictly necessary for the purposes of the processing through appropriate technical and organisational measures, such as pseudonymisation. 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 generated, etc.
38. Are there procedures or mechanisms to create backups the collected data?	
39. If information is anonymised, are there procedures which ensure the irreversibility of the process and the impossibility of re-identifying data subjects?	
40. 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 it can be exploited. You may need to check with your partners and suppliers about whether and how they store data.

41. 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 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 the privacy right of access.
42. Which storage mechanisms/procedures are provided? (e.g. centralized databases, archives, smart cards, etc.)	
POLICIES	
43. 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 of the data you process.
44. For how long is information stored?	
45. Does the controller periodically verify the proper functioning of security procedures and measures?	
46. Is there a data breach management action plan in place?	
47. Is there a records management policy in place which includes a retention and destruction schedule?	
48. Does the controller join codes of conduct or adopt certification mechanisms?	
49. Does the controller adopt data protection seals and marks?	
50. Are there codes of conduct that could be taken into account?	
ORGANISATION	
51. Has a data protection officer or an information security officer been appointed?	

52. Do you keep an access register to the IT systems containing personal data?	
52a. For how long is the access register stored?	
52b. Do procedures exist which allow the DPO or the IT security officer to periodically check the access register?	
53. 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.
STAFF	
54. How do you control access to personal data and its use by staff?	If you have subcontracted some of your work or engage with collaborators, you should have clarity about who has access to what data and what they can do with it, and whether they are staff or external providers (likely processors). The company is responsible for their staff. You cannot treat them as if they are 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.
55. How are staff informed of your security procedures?	
56. Can you be sure staff only access data that is necessary for their functions?	
57. Do you use unique individual accounts for your staff members that allow for personalised authentication and access controls?	
SUBCONTRACTORS AND SERVICE PROVIDERS	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.

58. Do you have contracts with any processors or other legal documents defining your relationship 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.
59. Have you outlined the instructions to the processor?	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). In an IoT environment, you can have situations with more than one controller and even joint controllers. In that case, you need to identify the responsibilities and the applicable supervisory authorities, and may need to consult guidance on this topic.
60. Might the processor engage another processor under the prior authorisation of the controller?	Your data processors are not allowed to further outsource the handling of any personal data without your permission.
61. Does the controller implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation?	
62. 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.
63. How do you minimise the data collection t˘o 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 generated, etc.

4. How do you treat users and people whose data you use?	
INFORMATION	
64. At the moment of data collection, is a clear notice (and, if applicable, consent) given to the user?	There is a requirement for the provision of concise, transparent, intelligible and clear information . This is independent on whether you rely on consent or other legal bases.
65. Are there procedures which allow data subjects to know the evaluation criteria of the automated individual decision-making?	
66. Do you explain data subject rights?	
CONSENT	
67. 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 for withdrawal.
68. Do you delete data after withdrawal of consent?	

COMPLIANCE WITH BASIC RIGHTS	
69. Can you give users access to their personal data?	There may be some limitations to the right to access due to competing interests and rights.
70. Can you rectify wrong or mistaken information after being notified by users?	Is the information stored in such a way that you cannot change it?
71. Might data subjects have the opportunity to obtain from the controller restriction of processing?	
72. Might data subjects have the opportunity to obtain from the controller the erasure of personal data concerning them 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.
73. Does the technology allow the collected data to be modified and erased?	
74. If someone asks and is able to provide the required identification, are you able to confirm whether or not you process their data?	
75. Can data subjects refuse to be subject to this kind of decision based solely on automated processing, including profiling, which produces legal effects?	
HOW WELL DO YOU SUPPORT RIGHTS?	
76. Can your users exercise their rights in a simple way, free of charge?	
77. How do you check that people who ask for their data are who they say they are?	You should not give someone other people's data, and neither should you impose excessive conditions that make the exercise of data subjects' rights too difficult.
78. Do you have systems in place to make sure you reply to every request from data subjects?	

79. How can your users know you have complied with their requests for rectification, erasure or restriction?	
PORTABILITY	
80. Is there anything inherent in the technology that would hinder your ability to give your users their data to take to another provider of a similar device or service?	
81. If requested, is the information provided by the controller in a structured, commonly used and machine-readable format?	GDPR creates a new right to data portability. This is very important for avoiding locking people into particular platforms or technical systems. Because this is a new right, there are few best practice precedents to follow, but in principle, you should provide data in a 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 which is created by you. This can sometimes be a grey area. 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 users still have the right to obtain a copy of their data, just not in a specific format with the option of taking it somewhere else.
82. 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 other similar products would use. Many fitness and sports applications with GPS capabilities use 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 one company to accept the data from another, but you should not cause any undue issues to users who want to use your data elsewhere.
PARTICIPATION & TRANSPARENCY	
83. 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 processors should only be doing what you tell them with the personal data of your users.

84. Is it feasible to consult data subjects or their representatives about the impact of the technology on their rights and interests? If yes, have you 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 for their views in the early stages.
85. Have you consulted all the subjects that are involved in the processing operations (e.g. the DPO, the processors)?	
86. 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?	
5. Risk Management	
87. 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?	
87a. 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?	
87b. Following the high risk indicated by the data protection impact assessment, did the controller consult the supervisory authority prior to processing?	
87c. Will the controller carry out a data protection impact assessment?	
88. Have you clearly identified the risks to the rights and freedoms of natural persons?	
89. Have you assessed the severity of such risks?	
90. Have you assessed the likelihood of such risks?	

91. Have you identified specific measures for each of the assessed risks?	
92. Have you identified measures to mitigate risks of illegitimate access, modification or disappearance of the data collected by the devices?	
93. Are the measures you have designed sufficient to mitigate the risks to the rights and freedoms of the data subjects? If the answer is no, have you consulted the national supervisory authority?	

6. Ethical and Social Impact Sample Questions

Dignity

- 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)?
- Are the expectations of benefits realistic? Do they justify this invasive and continuous monitoring?
- Will users be monitored by the device in private areas such as bathrooms?
- Will there be any spaces free of monitoring?

Non-discrimination

- Will the system take into account any particular characteristics of the users when making any determination, such as age, gender or disability?
- Are the IoT device and associated software used for predictive purposes or for classifying users according to their conditions, behaviour and preferences?
- What measures will be in place to avoid discrimination?
- Do you take into account the socio-economic characteristics of the users?

Autonomy

- Will the device reduce individuals' ability to make their own decisions?
- Will the tool include some form of remote control?
- If any limitations to user control exist, do they occur in contexts characterised by power asymmetries (e.g. workplace)?

Responsibility

- Will there be a way to challenge any decisions made by the system?
- Will there be clear lines of responsibility for any outcomes, particularly between the developers of the tools and the operators to ensure any issues are always dealt with?
- Will there be a way to challenge any decisions on productivity, resource allocation or treatment made by the system?

Accountability

- Will you be sharing personal data with third parties?
- Have you set clear limits on what third parties or partners can do with that information?
- Will the device receive advertising messages from third parties?
- Will the microphone in the device have a physical switch?

Sustainability

- Are the devices reusable? How will they be disposed of otherwise?
- Will the servers providing remote functionalities keep functioning for the lifetime of the product?

Safety & security

- Will the device receive software updates for the lifetime of the product?
- Is there a unique user name and password for each user/device?
- Is there a point of contact to report security vulnerabilities?
- How will you ensure the security of the data transmission?
- How can you ensure vulnerable users are not reached by malicious actors using the device?

Openness

- Will the device allow for third-party add-ons or user re-programming?
- Will the software in the device be open source?

Well-being

- If you allow for comparisons among users, how will you deal with the risks to self-esteem?

Transparency

- Does the device display any signs when recording video and/or audio in its surroundings?
- Has information about the logic of data processing been provided to users?
- 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 allow users to ask information about the project?

Participation

- Have you planned to engage stakeholders in the project development?
- In which manner have you identified the relevant stakeholders?
- Which forms of stakeholder engagement have you adopted?
- Do you intend to implement the suggestions provided by the stakeholders? Do you plan to present this implementation to the stakeholders for a further discussion?

Inclusion and equality

- Will the device be used to potentially restrict services to users or groups that are deemed uneconomical?
- Will data collected be used to influence socio-economic policies that may be detrimental to certain people, even if others benefit?

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 732027