NEW PESIA structure

NEW 1 Data mapping (Section 1)	
What information is collected?	
1. Does the project involve the collection 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[i] 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[ii]. 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.[iii]
4a. What kind of	

information is to be collected? LIST	
What do you do want to achieve with the information?	
5. Which are the purposes of the processing?	Explain how you will use the data
~~6. Which means are used for the processing (e.g. electronic means, non-automated means)?~~	
12. Is the collected information necessary in relation to the purposes for which they are processed?	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.
Where does the information come from?	
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?
3. 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, 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.[iv] 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.[v] 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	Legitimate interest is a controversial concept in data

necessary for the satisfaction of the legitimate interest of the controller?	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)
Special data	
4b. In particular, specify if special categories of data are processed)	List all the types of personal data collected or generated in the project. 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[vi]. 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.
10. Who else has access to the persona information?	In the table, list for each type of data who may receive it
Section 4. Transfer	
34. 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 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.
36. Is there an adequacy	If there is an official decision on the adequacy of the data

decision in relation to the third State importer of personal 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.
36a. If no, skip to section 5XX	
37. 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.[vii] 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.

38 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.
a. Have you obtained consent from 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.
b. 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.
c. 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	
d. The transfer is necessary for important reasons of public interest	Considering the very specific nature of this case, you should justify in detail.
e. Is the transfer necessary for the establishment,	

exercise or defence of legal claims?	
f. 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.
g. 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.
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.
NEW 2 Technology, Activities and Risks (Section 7)	
TECHNOLOGY	
7. Are new technologies used which might be perceived as being privacy intrusive (e.g. facial recognition, use of biometrics)?	
73. 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.

74. Am I using a product/component developed by others who have already carried out an impact assessment?	
a. If yes, check whether the producer is willing to share the assessment and integrate their work in your own assessment.	
75. Am I developing a technology similar to others that are being developed?	
a. If yes, consider the possibility to carry out a joint DPIA.	
78. Have I identified the assets on which the personal data rely (e.g. hardware, software, people, paper…)?	
AUTOMATION & PROFILING	
58. Does the technology allow to perform evaluation or scoring of the data subjects?	
69. 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.
70. Do such decisions affect legal rights of the	

~~data subjects (for instance, if the data collected by the device allows to detect alleged non-performance of the data subject and therefore prevents the device to work properly)?~~	
71. 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. |
72. Does the technology allow for human intervention in the decision process?	
a. 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.
SCALE & BREADTH	
59. Does the technology allow the collected data to be easily matched or combined with other data sets?	
60. 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[viii]. 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.[ix]
65. 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.
CONTEXT & SPACE	
61. 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.
66. 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.
67. 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.
68. 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.
New question: Do you track the location of data subjects?	
NOTE: EDPB does not see a risk in location but some DPAs do	
OTHER RISKS	
62. 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 .
63. 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.
64. Does the technology allow the collection of	European data protection bodies have issued guidance on this issue[x].

personal data referring to vulnerable people?	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.
77. Have I clearly identified the nature, scope, context and purposes of the processing operations?	Review your responses to this section and check that they describe the activities you intend to pursue.
RECAP	
13. 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 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.

NEW 3 How do you handle data accurately and securely (Section 6. Security)	
TECHNICAL	
81. 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?	
50. Are there procedures or mechanisms to create backups?	
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?	
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.
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)	
POLICIES	
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.
16. For how long is information stored?	
51. Does the controller periodically verify the proper functioning of security procedures and measures?	
54. Is there a data breach management action plan in place?	
19. Is there a records management policy in place which includes a retention and destruction schedule?	
56. Does the controller join code of conducts or adopt certification mechanisms?	
57. Does the controller adopt data protection seals and marks?	

76. Are there codes of conduct that could be taken into account?	
ORGANISATION	
42. Is a data protection officer or an information security officer appointed?	
49. Do you keep an access register to the IT systems containing personal data?	
a. For how long is the access register stored?	
b. Do procedures exist which allow the DPO or the IT security officer periodically to check the access register?	
52. 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.
a. No -> Then this	
b. Yes –> then this	
STAFF	
45. 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.
46. How are staff informed of your security procedures?	
47. Can you be sure that staff only access data that is	

necessary for their functions?	
48. 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.
39. 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.
40. 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)[xi]. In an IoT environment you can have situations with more than one controller and even joint controllers.[xii] In that case you need to identify the responsibilities and the applicable supervisory authorities and may need to consult guidance on this topic[xiii]
41. 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.

43. Does the controller implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation?	
53. 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.[xiv]
44. 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.
NEW 4 How do you treat users and people whose data you use (Section 3. Rights of data subjects)	
INFORMATION	
8. At the moment of the data	There is a requirement for concise, transparent, intelligible

collection, is a clear notice (and if applicable consent) given to the user?	and clear information to be provided. This is independent of whether you rely on consent or other legal bases.
33. Are there procedures which allow data subjects to know the evaluation criteria of the automated individual decision-making?	
New question: Do you explain data subject rights?	
CONSENT	
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.
New question: Do you delete data after withdrawal of consent?	
COMPLIANCE WITH BASIC RIGHTS	
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. Might data subjects have the opportunity to obtain from the controller	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

the erasure of personal data concerning him or her without undue delay?	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[xv].
83. Does the technology allow the collected data to be modified and erased?	
24. If someone asks, and are able to provide the required identification, are you able to confirm whether or not you process their data?	
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?	
HOW WELL DO YOU SUPPORT RIGHTS?	
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 say they are?	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.
23. Do you have systems in place to make sure you reply to every request from data subjects?	
How can your users know you have complied with their requests for rectification, erasure or restriction?	

PORTABILITY	
87. . 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?	
30. If requested, is 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 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 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.

82. Does the technology makes 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. 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.
79. Have I consulted all the subjects that are involved in the processing operations (e.g. the DPO, the processors)?	
90. 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?	
NEW 5 RISK MANAGEMENT	
55. 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?	
a. Did the data protection impact	b.

	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?	
	c. Since the high risk indicated by the data protection impact assessment, did the controller consult the supervisory authority prior to processing?	d.
	e. Will the controller carry out a data protection impact assessment?	f.
84. Have I clearly identified the risks to the rights and freedoms of natural persons?		
85. Have I assessed the severity of such risks?		
86. Have I assessed the likelihood of such risks?		
88. Have I identified specific measures for each of the assessed risks?		
89. Have I identified		

measures to mitigate risks of illegitimate access, modification or disappearance of the data collected by the devices?	
91. 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?	

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

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

iii https://betanews.com/2018/11/01/google-irobot-house-mapping/

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

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

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

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

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

ix http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

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

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

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

xiii http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

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

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