CONSUMER IOT
TRUST BY DESIGN 2019

Guidelines and Checklists

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

CONSUMER IOT TRUST BY DESIGN

Guidelines and Checklists

CONSUMERS INTERNATIONAL
COMING TOGETHER FOR CHANGE

CONSUMER IOT TRUST BY DESIGN

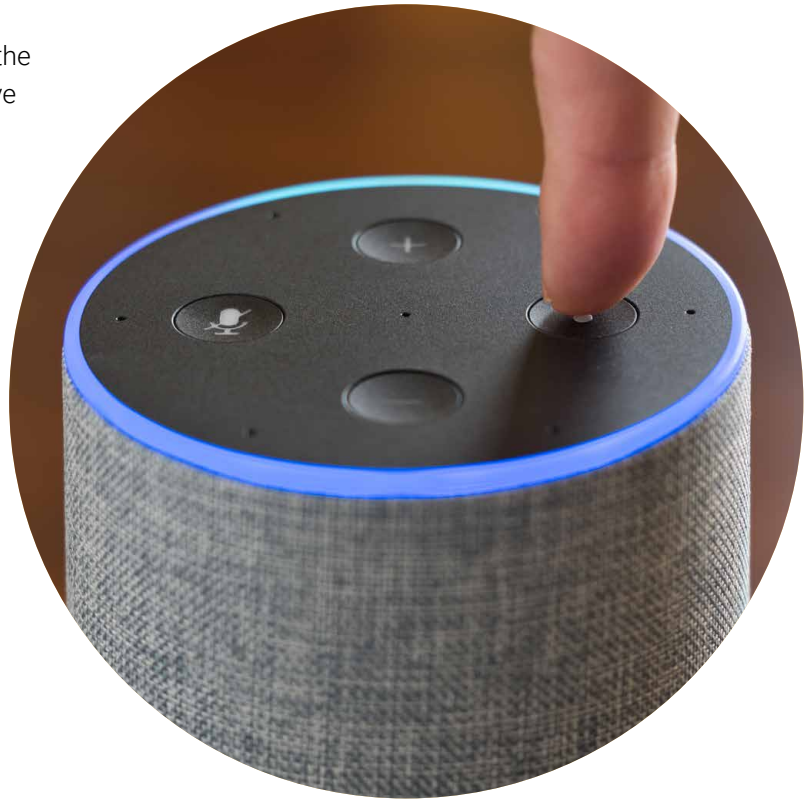
1. INTRODUCTION

Consumer applications in the Internet of Things can bring many benefits to people around the world such as greater convenience, more streamlined services and better information to help with decision making – not to mention the fun and enjoyment of connected products. However, as with all new technologies, there are things that consumers do, or perhaps should, worry about like: poor security, how devices collect and use their data, how they can control what happens with their device, whether it can work with other connected devices - as well as simple things like who to contact when things go wrong or if support for a product is unexpectedly stopped.[1] Many consumer IoT (or CIoT) products are coming onto the market with low levels of security or information about how they work or how to use them safely, which could erode trust and participation across this emerging market at a critical stage in its development.

These things are not just issues for consumer IoT products but for digital technology more generally. As our prior work and research has discussed, and despite high uptake, there is a growing sense that the huge benefits of digital connectivity might also have downsides, with concerns around privacy, transparency, consumer protection and many more areas, which cannot be ignored.

Understanding people's reservations and concerns will be important for any manufacturer wanting to produce quality, safe products that meet consumers' expectations and satisfy their concerns. And creating an environment where consumers can be confident that the products they buy meet a basic standard of trust, privacy, security and transparency will benefit everyone involved.

These useful principles, guidelines and checklists cover the key areas that we believe must be taken into account to create a trusted consumer IoT service or product: security; privacy; transparency; supporting vulnerable consumers; customer support and complaint handling; and environment.



1 Consumers International, Connection and Protection in the digital age: The Internet of Things and challenges for consumer protection 2016

CONSUMER IOT TRUST BY DESIGN

2. HOW TO USE THE GUIDELINES AND CHECKLISTS

These principles, guidelines and checklists provide useful, practical guidance to manufacturers on how to design trusted and safe consumer connected products, with case studies and places to go to find out more about other initiatives and regulations.

This document is divided into three main sections. Starting with a description of the complete set of six principles, it then goes on to give guidance for how to understand and apply each principle in turn. The final section provides a checklist for each principle, to help take the steps required to deliver Trust by Design. At the end of each checklist there is a space for manufacturers to describe their journey to Trust by Design, by explaining the extent to which their products meet the range of requirements, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

Consumers International's convening programme works with partners to tackle consumer challenges and opportunities. These principles, guidelines and checklists have been designed in collaboration with Consumers International, Vodafone, and internet of things manufacturers as part of a convening programme supported by Vodafone which ran from November 2018 to January 2019.

Consumers International intends these guidelines to be used to encourage and help manufacturers understand what they need to do to deliver Trust by Design, and how to do it for the benefit of all. Their use does not imply any endorsement from Consumers International.

CONSUMER IOT TRUST BY DESIGN

3. PRINCIPLES

Providers of consumer IoT Trust by Design products and services (defined as "providers") should meet the essential requirements of these six Trust by Design principles. They should also be working towards meeting more ambitious targets for good and very good practice.

1. Security: Providers should build security by design into CIoT devices and services, including in any software associated with such devices. Providers should adhere to the Global System for Mobile Communications Association (GSMA) or the Internet of Things Security Foundation (IoTSF) security guidelines. Providers should regularly assess cyber security risks, implementing and regularly reviewing the effectiveness of measures to mitigate such risks. In the event of any security breaches, providers should ensure customers are notified and act expeditiously to mitigate the impact of any security breaches.

2. Privacy: Providers should build privacy by design into CIoT devices and services. This means ensuring that privacy standards are met during the conception, design and life cycle of their devices. Providers should provide customers with a clear, comprehensive and easy to understand privacy policy and handle data collection and processing in a transparent way, in line with the EU's General Data Protection Regulation (GDPR) and other applicable privacy laws. In the event of any data breach, Providers should notify customers and act expeditiously to mitigate any such issues, as required under the GDPR and the privacy laws applicable in the countries where the devices are sold.

3. Transparency: Providers should provide consumers with clear and easy to access information about CIoT devices and services they have purchased. Such information will include at a minimum the name of the supplier, the price, a description of the device and any associated service, including any limitations or restrictions. It should be clear who the consumer can contact if they have any problems with the device or the communications service.

4. Supporting vulnerable customers: Particular care should be taken in relation to vulnerable customers. When designing CIoT devices and services, accessibility features need to be incorporated. Devices and services designed for minors need to have additional levels of care in relation to security and privacy features.

5. Customer support and complaint handling: Providers should provide adequate customer support and handle customer complaints in a timely manner and make independent redress mechanisms available to consumers where complaints cannot be resolved directly.

6. Environment: Providers should aim to reduce the environmental impacts of their CIoT devices and services, empowering their customers to make more sustainable choices. In order to do this, devices and services should be designed and built with resource efficiency in mind and clear guidance should be provided to customers on the most efficient use, re-use, repair and disposal of the devices and services and its components.

CONSUMER IOT TRUST BY DESIGN

4. GUIDELINES

These consumer IoT Trust by Design guidelines should help you to understand why and how the Trust by Design principles should be interpreted and applied by you. These guidelines are intended to help you meet these requirements for privacy, security, transparency and many other areas.

However, adherence to the guidelines does not necessarily mean that you are fully compliant with all legal obligations. It is important that you take advice to understand and comply with all legal obligations that apply to you.

For each principle, this document outlines why it is important and provide additional explanation including case studies and links to further guidance and information.

1. SECURITY

Principle 1:

Providers should build security by design into CIoT devices and services, including in any software associated with such devices. Providers should adhere to the Global System for Mobile Communications Association (GSMA) or the Internet of Things Security Foundation (IoTSF) security guidelines. Providers should regularly assess cyber security risks, implementing and regularly reviewing the effectiveness of measures to mitigate such risks. In the event of any security breaches providers should ensure customers are notified and act expeditiously to mitigate the impact of any security breaches.

Your devices, services and business need to be secure and resilient. Your customers need to have a safe and reliable experience which builds trust and confidence in not only your products, but the wider ecosystem of CIoT devices. In a widely connected digital world, security is a must. Poor security can lead to personal inconvenience, fraud, privacy breach, or even loss of money. This section explains how you can ensure security during the design, development and rolling out of your devices and services.

Security by design: Design your devices and services with security in mind throughout – from the very first stages of product development and through the entire product lifecycle.

Here are some ways you can build your devices and services with security in mind:

- Design your devices and services with built in security functions – like encryption, software execution control, and firewalls.
- Explain to your customers the security measures you have taken in a clear and easily accessible way eg, via your website's FAQ page and/or the terms and conditions (T&Cs). To help consumers understand, plain language should be used and FAQs and T&Cs should be easily understandable and relevant to their region and the product or service they are using.
- Set high security as the default setting.
- Make customers aware of the consequence of any choice they make to improve functionality which may impinge on security before they change the high default setting. For example, customers may select a faster access process (tick box to automatically remember a password) but if so, they need to be reminded that this should not be done if other people can access the device.
- Continually monitor for security weaknesses.
- Design your devices and services so that you can remotely update them during the lifetime of the product and where there is a consumer interface, provide information to consumers if an update is essential for security.
- Where there is not a consumer interface, ensure that the product can be updated remotely.
- Make sure your devices, services, and businesses are resilient to security attacks.
- Make sure your devices' default passwords are unique (or must be set to a customer-defined password on first use) and not resettable to any universal factory default value and require passwords to have a minimum level of complexity.
- Implement a vulnerability disclosure policy.
- Tell consumers how long you plan to support the product with security updates.
- Ensure all security certifications required for your device are obtained.

Conduct a regular assessment of cyber security risks and the effectiveness of your security measures

Regularly assess cybersecurity risks - for your devices, services, and your whole business - and confirm you are taking all the appropriate steps to minimise the risk, identify issues and mitigate the consequences. Appropriate times to conduct these reviews include: during the design phase for your device; when device is being tested for release; when you are about to rollout a software update; when a new vulnerability has been disclosed; and at other regular intervals.

As part of this review, you should also regularly measure how effective the security measures you've taken are. How you do this will depend on the security measures you have in place – for example, it could include security audits, measuring customer satisfaction, assessing how quickly customers apply updates and how many lower their security settings, and testing how often your security measures have successfully identified and defeated intrusion attempts.

In general, the higher the risks of your device and service, the more often you should assess the risks, measure the effectiveness of your security measures and consider whether it is necessary to introduce new measures.

Adhere to recognised industry standards for IoT security

There are several widely accepted security guidelines for devices and services, which include the GSMA Internet of Things Security Guidelines (click here [2] to access the document) and the Internet of Things Security Foundation (IoTSF) Best Practice Guidelines (click here [3] to access the document). These guidelines give you good examples of security best practice and provide many practical examples of steps to help you meet the security principles. Please read them and follow them where they are practical and relevant for your device, service or business. In deciding what is 'practical and relevant' for you, keep in mind that:

- the guidelines recognise that different devices and services have different levels of risk, and different consequences if there is a security issue;
- security features can be constrained – eg, by cost, available processing power and size - the way you implement the guidelines (and the steps you need to take to comply with them) will depend on these risks and constraints;
- therefore, you need to consider the right trade-off between security risks and real-world constraints; and
- you should be clear with your customers about these trade-offs.

It is recommended that you to comply with both GSMA and IoT SF sets of security guidelines as they are complementary, in order to achieve a 'best in class' secure ecosystem of IoT devices and services that benefits your customers. It is permissible however

to comply with only one set of the guidelines – in such case you need to objectively determine your preference and should be able to demonstrate the measures you have undertaken to comply with your chosen guidelines.

Notify customers and act expeditiously to mitigate security breaches

You need to notify customers of any security breach, if it could have any impact on them – for example, from loss of service, or risking disclosure of their information. The notice to customers should be clear, in plain language, and include: name and contact details of the data protection officer or other contact person; the security breach's likely consequences; and the measures taken to address the security breach including measures to mitigate potential adverse effects.

You should have a policy and resources in place to respond to a security breach quickly, identify the damage (eg loss of information), provide support/compensation to your customers and get your service and business back up and running again quickly. The GDPR requires you to notify customers and regulators in some cases – see the privacy principle below.

2 GSMA, GSMA IoT Security Guidelines and Assessment, 2017
3 IoT Security Foundation, Best Practice Guidelines, 2018

HOW WATCHNETWORKS MADE SURE THEIR SMART WATCH STAYED SECURE

WatchNetworks wants to launch a smart watch which will collect, store and transmit sensitive information about users. They carry out a risk assessment which finds that the risk of exposing personal data is high as it is transmitted over the public internet, and that it will have severe consequences as the data could include things like credit card details or location data.

Although **WatchNetworks** already has good security standards as a default, like requiring the user to set their own complex password, the high risks lead them to adopt additional features such as a secure element in the watch. This will increase costs and the physical size of the device. They decide this is an appropriate trade-off given the high risks and severe consequences of a security issue.

But **WatchNetworks** doesn't stop there. They also want to reassure people that they have thought about and designed in features that will minimise any future security risks, for example:

- software is designed so that updates are downloaded and validated by the smart watch automatically.
- updates are applied "behind the scenes" without customer input, except where the watch needs to be restarted for the update to work.
- regular prompts will appear to the user, if they delay installing an update that requires a restart, which explains why the update is important.
- not applying security updates that reset or change user-configured security settings, restrict existing functionality (eg to encourage a customer to upgrade to a new model) or could discourage a customer from applying the update, unless there is a good security reason for this.

MORE INFORMATION

- ENISA - Baseline Security Recommendations for IoT
- UK Government, Department for Digital, Culture, Media & Sport – Secure by Design
- IEEE – Internet of Things (IOT) Security Best Practices

2. PRIVACY

Principle 2:

Providers should build privacy by design into CIoT devices and services. This means ensuring that privacy standards are met during the conception, design and lifecycle of their devices. Providers should provide customers with a clear, comprehensive and easy to understand privacy policy and handle data collection and processing in a transparent way, in line with the General Data protection Regulation (GDPR) and other applicable privacy laws. In the event of any data breach, Providers should notify customers and act expeditiously to mitigate any such issues, as required under the GDPR and the privacy laws applicable in the countries where the devices are sold.

Privacy is a critical requirement for consumers and for trust in the IoT ecosystem. IoT devices are designed to collect or share data. Some of this data may not be considered 'personal data' (eg information about the physical state of the device, or metrics regarding the network status), while other data is about or related to consumers and will be subject to general data protection and privacy laws and regulations. As IoT markets grow larger, more consumer data will be created, processed and shared between several parties across national borders. That is why privacy by design is much more than simple legal compliance – it's about building a culture that respects privacy and justifies the trust placed in us.

Your devices and services need to protect customers' personal data. Your customers need to have confidence that their personal data will not be used or disclosed, except in a way they would expect and are informed about. If you collect, process or store any personal data of customers in the European Union, you'll need to be familiar with and comply with GDPR (Regulation 2016/679) and any other laws regulating privacy and data protection.

'Personal data' is generally information about an individual through which they can be identified (for example, through a name, ID number, location data, etc), however it is worth noting that this definition is quite broad and due to advances in correlation techniques will also include unique identifiers such as hashed or pseudonymised data, IP address or cookie IDs.

The GDPR and other privacy laws are complex and you should consider seeking your own legal advice because the consequences of violation are substantial.
Here is a summary of the key requirements:

1. Process personal data lawfully, fairly and transparently.
2. Collect personal data only for specific and legitimate purposes.
3. Only process personal data where you need to and do not collect for future as-yet unknown uses.
4. Ensure personal data you process is accurate and up to date (including allowing customers the opportunity to view and amend their data).
5. Only store personal data in an identifiable format for the minimum period necessary.
6. Ensure the integrity and confidentiality of personal data you process.
7. Be able to demonstrate your compliance with the GDPR.

The above provides only general guidance. GDPR rules can be complex so you need to become familiar with the detail about how these principles apply and seek your own legal advice to ensure compliance. For example:

- Special categories of consumers eg minors where additional requirements apply or additional care is needed.
- Special categories of data which are particularly sensitive may only be processed in limited circumstances. The most relevant situation is with the user's explicit consent.
- Special protections and restrictions apply if you intend to transfer the personal data to a third country (outside the EEA) or an international organisation.

Keep in mind that, depending on your business and devices, you may need to follow additional data protection requirements. Check which specific requirements are relevant to you. For example, if your device facilitates payments, the Payment Services Directive 2 (PSD2) imposes additional and more prescriptive security and privacy requirements.

Privacy Impact Assessments are living documents that demonstrate commitment to the concept of privacy by design which means safeguarding privacy and adopting data protection principles right from the start of the design process – from device and service development through to the entire product lifecycle. If your product's processing changes, it's advisable to revisit your Assessment to determine whether the changes require any additional controls.

The key control to identify any privacy by design considerations and the legal requirements applicable to your product/service is to conduct a Privacy Impact Assessment.

HOW SERIOUSHEALTH'S FITNESS TRACKER HELPED PRIVACY GET IN SHAPE

SeriousHealth is designing a fitness tracker, which can provide health information to customers based on data collected about their movement and calories, for example, about their movement and calories burned during a day. They conduct a Privacy Impact Assessment of its processing activities to ensure compliance with the GDPR. It identifies each function of the device, identifies which personal data it needs to collect to allow that function to work, and designs the software so that it only collects that information, eg:

Function: Personal data SeriousHealth must collect for this function
Calories burned: GPS information to calculate distance travelled, weight, age, unique device identifier

To give customer's data the best level of protection, **SeriousHealth** designs the service so that calculation of calories burned is performed on the device itself. This means the customer's weight and age can be stored on the fitness tracker only and are not sent to **SeriousHealth**.

SeriousHealth's has a privacy policy, where it explains all the types of personal data it collects and why, how the data will be used, how it will be kept and disclosed, and the customer's rights. It makes sure that customers provide clear and unambiguous consent to their personal data being used in this way. It sets up a system so that customers can obtain a copy of their data, amend it where it is inaccurate, and request that all information be deleted. It amends its data retention practices, so that information is deleted as soon as it is no longer needed.

SeriousHealth is adopting good practices by designing the device and service so that the collection of personal data is minimised, no weight or age data is sent is sent to **SeriousHealth**, and so that it is clearly explained to customers why their personal data is required and how it is used.

MORE INFORMATION

- The General Data Protection Regulation
- European Commission – Rules for business and organisations
- European Commission – Principles of the GDPR
- Article 29 Working Party – Guidelines on Personal Data Breach Notification
- Article 29 Working Party – Guidelines on Data Protection Impact Assessment (DPIA)
- UK Information Commissioner's Office – Guide to the General Data Protection Regulation
- UK Information Commissioner's Office – Data Protection Self Assessment
- Internet of Things Privacy Forum Guidance

3. TRANSPARENCY

Principle 3:

Providers should provide customers with clear and easy to access information about CIoT devices and services they have purchased. Such information will include at a minimum the name of the supplier, the price, a description of the device and any associated service, including any limitations or restrictions. It should be clear who the customer can contact if they have any problems with the device or the communications service.

Your customers should be given clear and complete information at different stages about the device and services, such as the price and any limitations on how they can use it, so that they are informed and empowered to make choices that are right for them. You should provide your customers with clear, easy-to-understand information about how the device works, and ensure the device works as expected.

There are several market players involved in providing an IoT service to the end customer, and some may have several different roles. Clarity and transparency can help build customers' trust, so you should show who is responsible for what in the value chain, and understand how and why things happen. Here's a simple example of what the IoT value chain might look like:

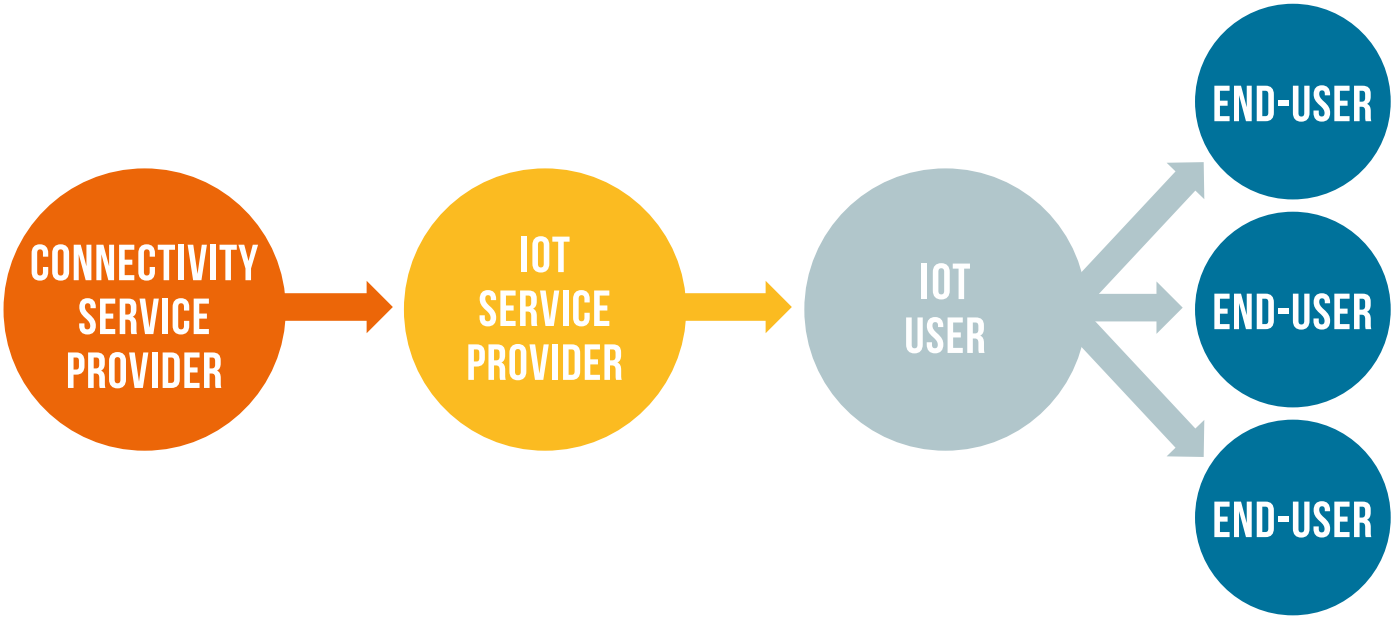


Figure 1: *IoT value chain, BEREC, Report on enabling the Internet of Things, BOR (16) 39 o* [4]

4 Connectivity service provider - is the provider of an electronic communication service;
- o IoT service provider – is the Provider of an IoT service, which can comprise the provision of an IoT platform and/or other IoT-related IT-services/solutions;
- o IoT user - Purchaser of an IoT service who incorporates the IoT service as one component in his own products (i.e. connected devices);
- o End-user – is the customer at the end of the value chain who purchases a connected device and/or utilises a service (including an IoT service and/or IoT device)

It's also important that your customers are not misled or disappointed by your device and service. Disclose information beforehand, so that customers don't need any special expertise or to take difficult steps to understand how your device works and what it does. The functionality itself should also be transparent. For example, you should explain whether your device works without connection to the internet, how to port data, and whether it is possible for the customer to switch communications provider.

The Consumer Rights Directive (2011/83/EU) explains the information that has to be provided to customers, whether they are buying something in a physical shop, online or off-premises (for example, at their own homes or somewhere else that is not the seller's usual place of business). Off-premises contracts require more information, and the checklist below sets out the information required for physical/online sales, and the additional requirements for off-premises sales. Different EU member states can have different requirements, so it is important that you check the national obligations and comply with them as well.

WHO WORKS TOGETHER TO MAKE PETCAFE'S PET TRACKER WORK?

PetCafe has designed a device that allows cat and dog owners to track the movements of their pets. **PetCafe** is selling its device face to face at a local shop (using an on-premises contract), and by allowing customers to place orders on the phone (via an off-premises contract) or the website (distance contract).

PetCafe's value chain:

In order for **PetCafe's** device to deliver its functionalities, the company cooperates with Sens-data, a small business whose sensors are integrated into the device to capture information about the pet's movements. **PetCafe** has also contracted and utilizes a specific IoT platform and application designed and run from AppMore. AppMore translates, processes and prepares the data captured from the sensors for transmission to the owner. Data connectivity is enabled by Rolling Telecoms, a mobile network company that establishes and manages the data exchange between the tracking device (which has a SIM slot) and the pet-owner's mobile phone. As a result of the successful integration and cooperation of all these actors in the IoT value chain, the pet owner is able to access the PetCafe application in their mobile phone and track the location of their pet.

PetCafe makes it clear to the consumer that for any queries or issues relating to the device, **PetCafe** can provide support and provides contact details for Rolling Telecoms who are responsible for questions relating to connectivity.

HOW PETCAFE HELPS CONSUMERS UNDERSTAND THEIR PRODUCT

PetCafe has to ensure that its sales and order processes for each sales channel complies with the law. It therefore reviews its advertising, packaging, pre-sales scripts for telephone calls, the training for retail staff, its website, and the detailed product information inside the box. Using the transparency checklist, it ensures that it provides all the information required to customers and that customers are likely to fully understand everything they would expect to know before buying the service.

PetCafe changes the order process to comply with its obligations, which includes ensuring that when orders are placed online or via the phone, customers will be provided with the required information via email when they receive their order confirmation.

MORE INFORMATION

- European Commission – Consumer rights directive
- Consumers International – G20 recommendations for Building a Digital World Consumers can trust

4. SUPPORTING VULNERABLE CUSTOMERS

Principle 4:

Particular care should be taken in relation to vulnerable customers. When designing CIoT devices and services, accessibility features need to be incorporated. Devices and services designed for minors need to have additional levels of care in relation to security and privacy features.

Consumers can be vulnerable in many different ways, perhaps because of their age (for example: children or the elderly), their behaviours, their cognitive ability or particular personal circumstances. Treating everyone the same way may seem fair, but it could actually be detrimental to some people who are not in a position to make the best decision for themselves, or to fully understand the nature of products. You should take into account and cater for the needs of a wide range of customers when you design your product and make sure that it is accessible for everyone and can interact with other services that people rely on, like personal alarms or health services.

If restrictions such as age limits are needed, these should be clear and, as far as possible, you should prevent people below that age from accessing the device or service. Care for vulnerable customers extends beyond the design and manufacture: you should give vulnerable customers assistance to be able to use your device or service and make it easy for them to contact you for help. Train your staff on what factors to look out for in order to identify and respond to a customer that may need special assistance. Your staff need to be aware of, and trained, on how to interact and assist these customers.

You should consider additional security requirements that you may want to introduce in order to address the needs of minors/vulnerable customers and help to mitigate risk in these conditions. For that purpose, it is suggest you engage and identify acute risks for these target groups so that you can make a tangible difference. A good starting point is to establish whether the application or service is being used appropriately and by whom and whether additional security controls should be adjustable or default features.

HOW A ONE-CLICK PURCHASING DEVICE SUPPORTS VULNERABLE CONSUMERS:

Supermarket Enterprises is a 'one-click' purchasing device that lets customers buy from the website from anywhere – they just enter the product they want to buy, confirm the purchase and it arrives at a pre-set delivery address. **Supermarket Enterprises** use the vulnerable customer checklist to ensure that the device is designed in a way that it can be used by as many customers groups as possible. It adapts the design of the device so that the following options can be used on the device:

- commands can be voice activated to assist visually impaired customers
- text can be increased in size and set to alternative languages
- security passwords can be set up for all purchases, or for particular groups of items eg, in relation to purchases of age restricted items like alcohol

MORE INFORMATION

- European Commission – Consumer rights directive
- W3C – Making the web accessible
- BSI – new code of practice on protecting vulnerable customers

5. CUSTOMER SUPPORT AND COMPLAINT HANDLING

Principle 5:

Providers should provide adequate customer support and handle customer complaints in a timely manner and make independent redress mechanisms available to customers where complaints cannot be resolved directly.

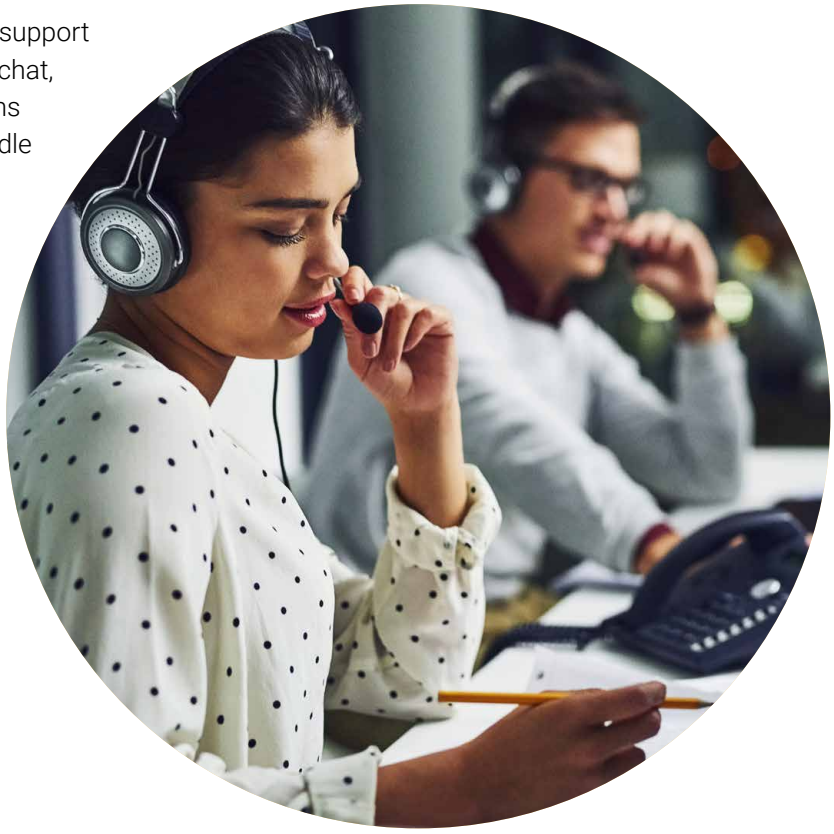
Customers will often need support to understand how to install, setup and operate a device or service and if they have issues or complaints. IoT devices often involve services which are supplied by different providers and this must be made clear to the customer so that they know who to contact and who is responsible. You can ensure adequate customer support by:

- designing your devices and services so they are easy to use in the first place
- making your manuals and instructions concise, simple and easy to follow
- explaining to your customers where they can obtain support
- providing different ways to contact customer support – eg online instructions and FAQs, email, webchat, phone, in-app support, in-store and web forums
- ensuring you have enough staff trained to handle the expected amount of support needed
- training your customer support staff, so they understand your devices and services, and can provide clear advice and assistance
- making use of chat bots and social media in customer support, these must be developed to the highest possible standard of customer care, and give the customer the possibility of escalating the case to a human agent if required

The specific steps you need to take will depend on your business and your particular devices and services. For example, the more serious the harm or inconvenience caused by a customer not being able to use your device or service, the more important it is that the customer can:

- speak to a real individual (eg not be directed to an online forum)
- obtain a speedy response (eg not wait several days for an email response)
- have a response which is specific to their questions and provides clear advice and instructions for how to resolve the question

Should a customer complain, you need to have an internal complaints process which allows for speedy resolution of issues. In the event an issue cannot be resolved with the customer directly, you should consider mediation or alternative dispute resolution options.



HOW HOMEFROMHOME LTD. DELIVERED TOP SERVICE FOR THEIR SMART THERMOSTAT

HomefromHome Ltd. have developed and launched a device that allows customers to log in to an app and adjust the temperature of their house when they are away from home. Before launching the service, it gave as much attention to complaints handling as it did to the technical functionality of the device, and:

- developed a clear and robust complaints procedure – explaining exactly how customers could complain, and the process, steps and timeframes for resolving complaints
- Designed systems to manage the internal steps that need to be taken to handle complaints and ensure all complaints are logged and tracked
- published the complaints procedure on its website, and in the information provided with the device; it became a member of an ADR scheme which gives customers access to an independent third party if **HomefromHome Ltd.** can't resolve a complaint
- trained call centre and complaint handling staff on the complaints procedure and how to manage complaints
- arranged for a third party to oversee the website, online order process, and call centre for any queries and complaints

MORE INFORMATION

- European Commission – Resolve your consumer complaint
- European Commission – Consumer dispute resolution

6. ENVIRONMENT

Principle 6:

Providers should aim to reduce the environmental impacts of their CIoT devices and services, empowering their customers to make more sustainable choices. In order to do this, devices and services should be designed and built with resource efficiency in mind and clear guidance should be provided to customers on the most efficient use, re-use, repair and disposal of the devices and services and its components.

CIoT devices and services offer new opportunities to improve energy efficiency and reduce customers' impact on the environment. You should be committed to responsible management of environmental issues – both within your business and across the supply chain. This could include:

- conducting all necessary due diligence to ensure compliance with environmental laws
- putting in place environmental management systems and controls eg ISO 14001:2015, ISO 50001
- setting environmental performance targets
- monitoring the effect of your business practices on the environment
- designing devices and services in a way that minimises environmental impacts

INTELLIGENT IOT INC IS A LARGE COMPANY THAT MANUFACTURERS A NUMBER OF DEVICES AND SERVICES

Intelligent IoT Inc reviewed its business practices to find ways to reduce its environmental impact and find more sustainable ways to manufacture devices and services. **Intelligent IoT Inc** appointed an employee with the role of reviewing its manufacturing processes (and the resulting carbon footprint) in order to develop a policy which will work towards improving processes and reducing Intelligent IoT Inc's impact on the environment.

They have also looked into ways that the software on the device can be updated and made changes so that customers will be able to continue to use devices, without the need for replacements in the near future.

MORE INFORMATION

- One Planet Network – Exploring Product Lifetimes

CONSUMER IOT TRUST BY DESIGN

5. CHECKLISTS

USING THE CHECKLISTS

As described in the introduction, consumer Internet of Things (CIoT) products bring many benefits but as with all new technologies, there are things that consumers worry about such as: poor security, how devices collect and use their data, how they can control what happens with their device, how long they can expect to use it for, as well as simple things like who to contact when things go wrong or if support for a product is unexpectedly stopped.

Demonstrating that you understand these concerns and have thought through how to address them in your CIoT products will help build trust and participation across this emerging market.

Each checklist below relates to one of the principles and is designed to help you meet the steps to take to deliver Trust by Design for each one. Together they demonstrate a holistic approach to Trust by Design. Most of the checklists divide requirements into three categories, except for Security which has two categories and Privacy which has one):

Essential – a checklist of what this guide considers to be essential is essential for delivering Trust by Design

Good – a more ambitious checklist for actions that by meeting or working towards meeting, show you are a company who takes trust by design seriously, based on existing best practice

Very good – an even more ambitious set of actions, showing you can think ahead about a range of things that can impact on trust, and be a leader in Trust by Design

For each one, you will have the opportunity to say if you are meeting the requirement or not, or whether you are working towards it. There is also a space to give your commentary on how you are meeting the principle, and an opportunity to explain what you are doing to improve your practice or develop new practice in the future.

The Consumer IoT is broad, and so the steps you need to take to ensure you are meeting the guidelines and principles will depend on your business and your particular devices, your intended customers and the amount and type of personal data you collect or process. The checklist also enables you to note where elements are not applicable to you.

CHECKLIST 1: SECURITY

The requirements for Security are divided into two categories:

Essential – a checklist of what this guide considers to be essential for delivering Trust by Design

Good – a more ambitious checklist for actions that by meeting or working towards meeting, show you are a company who takes trust by design seriously, based on existing best practice

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have you conducted a 'risk assessment' to document and understand all the security risks of the device or service, and the likelihood and severity of the risks?	☐	☐	☐	☐	
In relation to children, has a high bar of security by default been taken into account, and does this apply to features and functionalities that are likely to be accessed by a child? Externally developed and recognized traffic light systems for security that provide age ratings advice should be considered and incorporated where appropriate.	☐	☐	☐	☐	
When using a password, have you ensured default device passwords are unique or that customers are forced to change passwords on first use?	☐	☐	☐	☐	
When using a password, have you ensured device passwords cannot be reset to a universal factory default?	☐	☐	☐	☐	
When using a password, have you ensured device passwords have a minimum level of complexity?	☐	☐	☐	☐	
Are you measuring the success of your security monitoring on a regular basis?	☐	☐	☐	☐	
Have you put in place a process so that security vulnerabilities are fixed quickly?	☐	☐	☐	☐	
Have you ensured software in your device can be easily updated to enable security updates to be provided throughout the expected lifetime of the IoT product?	☐	☐	☐	☐	
Have you made it is easy for customers to understand why updates are needed and how often/for what purpose updates are provided?	☐	☐	☐	☐	

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have you established a process to respond to attacks, contain the damage and get the service or your business back up and running normally as quickly as possible?					
Have you ensured all sensitive data is encrypted when transferred over networks and at rest, including when hosted by a third-party cloud service provider?					
Are you managing all encryption keys securely?					
Have you minimised exposed "attack surfaces" – eg, minimised the user's privileges to the lowest level possible for the service to work?					
Have you set the default security settings as high as possible?					
Are you considering security issues on an ongoing basis, especially when you roll out new devices and services or make changes to your systems?					
Are you continuously monitoring your system data for security anomalies and attacks?					
Have you ensured there is a public point of contact, so that the public can report security vulnerabilities which should include either a freephone number or email address as part of their contact information, and information on when a customer can expect to receive a response?					
Are store security credentials in a secure element and not hard-coded in software?					
Have you ensured your device has software integrity assurance – eg, in the boot mechanism?					

Commentary: Use this space to describe the extent to which your device meets the range of requirements for this principle, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

CHECKLIST 2: PRIVACY

Essential – all requirements in the privacy checklist are essential for delivering Trust by Design

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Accountabilities, and Privacy by Design	1. Have you assigned a qualified person responsible for privacy? This person will act as single point of contact on privacy related questions and oversees the Privacy by Design process and supports the development of the IoT product. Where necessary assign a formal Data Protection Officer.	☐	☐	☐	☐	
	2. Have you conducted a legal analysis to ensure the product conforms with the laws in the countries where the product is offered?	☐	☐	☐	☐	
	3. Have you conducted a privacy risk assessment to identify potential harmful impacts to end-users and identify mitigating controls? The assessment should ensure these requirements, including requirements arising from any legal analysis, are communicated to the development teams for the product, that the requirements are taken into account in the design of the product and that the product is tested for conformance with these requirements prior to its launch to end-users.	☐	☐	☐	☐	
	4. Have you ensured all necessary notification/approval requirements to national regulators have been complied with prior to offering the product to end-users, including any possible requirement for prior consultation with the data protection authority in case risks to end-users still remain?	☐	☐	☐	☐	

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Data Minimisation, Proportionality	5. **Minimisation**: Do you only collect and process personal data which you need to deliver the product? When doing so do you identify what personal data / other user information is collected? You should identify and document data flows between various components of the product and justify why said data is necessary in each stage.	☐	☐	☐	☐	
	6. **Lawful basis, proportionality:** Have you ensured you have a justifiable purpose for collecting and processing the personal data in question for each data attribute in each stage of the processing and in each component of the product?	☐	☐	☐	☐	
	7. **Lawful basis:** Have you verified whether you have a lawful basis to process the personal data in question?	☐	☐	☐	☐	
Privacy Notice and permissions	8. **Privacy Notice:** Are you ensuring that applications that collect personal data provide users with a clear and understandable prior privacy notice detailing such data collection so that users may make informed decisions about whether or not to use the product or certain features? See Guidance Note on page 41.	☐	☐	☐	☐	
	9. **Privacy Notice:** Have you ensured that applications make the above notice available to users prior to the initial collection of personal data through the application (both in relevant app store and as part of the first use of the application) and the user must acknowledge and agree to the Privacy Statement and Terms and Conditions (OK/Cancel – or similar binary choice without default)? Not agreeing must lead to product not being usable.	☐	☐	☐	☐	

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
	10. **Privacy Notice:** Have you ensured that Privacy Notices are separate from Terms and Conditions and the first use of application must refer to both of them separately? Both Privacy Notice and T&Cs must be available to the end-user via links or otherwise as part of the first use of the product.					
	11. **Privacy Notice:** Is the notice viewable anytime thereafter within or through the a pplication (eg, through the application's help menu, a link to a website hosted by you, or similar effective method)?					
	12. **Highlight notice:** Have you presented a timely highlight notice to users in the application user interface to draw attention to potentially unexpected or sensitive collection or use of personal data to get end-user consent for such processing? The highlight notice is shown prior to such data being collected (either at first use of the product or just-in-time prior the collection/processing commences).					
	13. **Highlight notice:** Are you ensuring that a highlight notice is made available in at least the following instances, and that it explains the details (what data, for what purpose) relating to: i) any of the following information collected through the product: location, audio, video or other images, biometrical information such as facial recognition, fingerprints or other such data, any measurements from the IoT device, information about apps running on the device, communications logs, documents, special categories of personal data or any other data stored on the application, IoT device or Back-end ("User Information") ii) any personal data is shared with 3rd parties (other than those merely processing personal data on behalf of you)					

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
	14. **Highlight notice:** Has the user consented to the processing as described in the highlight notice (OK/Cancel – or similar binary choice without default)? Not agreeing must lead to the defined features not being usable.					
	15. **Highlight notice:** If the first use experience cannot accommodate the detailed explanation required, have you ensured the highlight notice refers to an additional explanation, either as part of your Privacy Notice or a specific supplement to your Privacy Notice? This information must be available to the end-user anytime through application settings.					
	16. **Highlight notice:** Does the highlight notice refer to settings on the application or on the IoT dwhich allow end-user to control the collection / processing of personal data?					
	17. **Highlight notice:** Are end users able to access any highlight notices after having been initially presented to themselves? (eg through application settings).					
	18. **Highlight notice/Privacy Notice:** Has the highlight notice incorporated the Privacy Notice related requirements, if presented as part of the product first use?					
	19. **Website Privacy notice:** In addition to the above, have you made the Privacy Notice accessible through the website of the product?					

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
	20. **Settings:** In addition to highlight notices as defined above, have you ensured that the product enables the following user controls (enable/ disable): i) Collection of any user information from the IoT device ii) Collection of any user information from the application or the device platform on which the application runs iii) Collection of any diagnostics data from the IoT device or thea iv) Turning on/off the IoT device remotely	☐	☐	☐	☐	
	21. **Consent**: Are you aware that consent dialogue prompted by the mobile operating system qualifies as consent only insofar as they provide the end-user with sufficient information to make an informed choice and satisfies legal requirements for consent?	☐	☐	☐	☐	
	22. **APIs:** Have you ensured that applications only use defined APIs to access user information?	☐	☐	☐	☐	
	23. **Periodical reminders of collection:** Are applications periodically reminding users or providing a visual indicator when location data or user information is being sent to back-end, any other service, service provider, user or other third party continuously or periodically on an on-going basis?	☐	☐	☐	☐	
	24. **Analytics:** Have you obtained end user consent for IoT devices and/or the applications that embed analytics software which sends any information from the IoT device and/or application to the Back-end or elsewhere? And is the end-user able to disable the collection? (eg, through application settings).	☐	☐	☐	☐	

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
	25. **Marketing Permission:** If your application is used to provide direct marketing electronic messages (for example, email, SMS or MMS messages) to users, or intended to collect user information to accomplish that purpose, have you obtained the user's prior consent, and provided an effective means to opt-out from such messages in the future as required by applicable laws?					
	26. **Parental consent:** If the product is targeted to children, have effective mechanisms been put in place to ensure the parent or legal guardian expresses the consents required by law and these requirements?					
Data management	27. **Personal Data Processing Register:** Do you have effective processes to maintain an up to date personal data processing register? See Guidance Note on page 41 for minimum content of personal data processing register.					
	28. **Data Quality:** Do you have an effective process to maintain the accuracy and up-to-datedness of the personal data?					
	29. **Control effectiveness:** Do you have effective technical and process controls to ensure any changes in user permissions "flow" to each component of the product and is effective and up to date?					
	30. **Data deletion:** Have you defined a data deletion schedule for each data attribute in each component of the product? You must have effective processes to ensure data is deleted or anonymised after it is no longer necessary for the purpose it was collected.					

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
	31. **Purpose limitation:** Have you ensured that personal data is not processed for purposes that are incompatible with the purposes which were originally informed to the user, unless the user has specifically consented to such new purposes?					
	32. **De-identification:** Where it is not necessary to process personal data in an identifiable format, have you applied pseudonymisation or anonymisation on the data set in any component of the product?					
Right of the end-users	33. Have you created a process through which data subjects can exercise their right to access personal data, request its deletion or modification, request portability of their data in machine readable format or to object to the use of personal data for certain purposes? The process must ensure that such are exercised only by identified and authenticated users who are authorised to exercise the rights.					
	34. For the products with a user interface, have you considered designing the product so that the data subject can access, delete, modify or port her essential personal data and manage their permissions related to their product or account directly from the product to the extent such is viable and possible to do in a secure manner (the amount of information to be shown depends on the strength of authentication of the data subject)?					
Disclosure of data to 3rd parties	35. Have you ensured that personal data to governmental authorities has not been disclosed unless required by mandatory, applicable law?					

AREA	CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
	36. Are you only choosing such processors to process personal data on your behalf who are capable of meeting the requirements defined by you and as defined in applicable laws (such as GDPR)?					
	37. Do you have a data protection agreement in place with all 3rd party data processors who process personal data on your behalf? This agreement must meet the requirements defined in applicable laws (eg GDPR)					
	38. Have you ensured that one of the below methods is used when transferring personal data that is subject to EU law outside of the EU: 1. EU Commission approved standard model clauses are effective between the parties (default position); 2. transfer is done to a country deemed to be adequate by EU Commission (exception); or 3. recipient has in place EU approved Binding Corporate Rules that apply to the processing in question (exception);					

Commentary: Use this space to describe the extent to which your device meets the range of requirements for this principle, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

CHECKLIST 3: TRANSPARENCY

The requirements for Transparency are divided into three categories:

Essential – a checklist of what we think is essential for delivering Trust by Design

Good – a more ambitious checklist for actions that by meeting or working towards meeting, show you are a company who takes trust by design seriously, based on existing best practice

Very good – an even more ambitious set of actions, showing you can think ahead about a range of things that can impact on trust, and be a leader in Trust by Design

The specific information you need to explain to customers will depend on your particular devices and services and the way in which it is sold.

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have you ensured the device or service genuinely and honestly performs the functions it appears to perform?	☐	☐	☐	☐	
Have you provided customers with clear information in relation to the different providers of their service and to what extent they are responsible for final service delivery and support for the consumer?	☐	☐	☐	☐	
Have you ensured that customers have information about the main characteristics of your device/services – including whether the device works without an internet connection and any other restrictions?	☐	☐	☐	☐	
Have you clearly told customers about any legal guarantees (eg that the goods will meet a certain standard or after-sales services and commercial guarantees)?	☐	☐	☐	☐	
Have you provided customers information about your identity, including company name, geographical address and a telephone number / email address?	☐	☐	☐	☐	
For products you are directly selling, have you clearly explained to customers the total price of the device/ service (inclusive of taxes and other unavoidable charges), the manner in which the price is calculated, as well as any delivery or ancillary charges (where appropriate) and the arrangements for payment?	☐	☐	☐	☐	

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have you clearly explained to customers how long any contract will last for (and how and when the contract can be ended, including any early termination fees or other restrictive conditions)?					
Have you ensured the customer is clearly told of their right to walk away or return the device?					
If you are making specialised claims about your device or service (eg claiming it has medical functionality) have you ensured you have a good basis for these claims and that you meet all the regulatory requirements to make those claims?					
Have you ensured customers are told about after-sales support including, how to complain, any applicable code of conduct and any redress mechanisms?					
Have you ensured that there is nothing in your information, or in how the device or service is displayed or advertised that could be misleading to customers?					
Have you used plain and simple language to make sure that FAQs and T&Cs are easy to understand and relevant to their region and the product or service your customers are using, and which are accessible in a machine readable format?					
Have you ensured that information regarding distant sales and right to walk away is given early into the purchasing process, along with delivery, return and refund costs? And that these are not hidden in T&Cs and FAQs which are not provided or linked to on the pre-payment or payment page of a website?					
Are FAQs and T&Cs accessible in a machine-readable format?					
Have you ensured that customers are properly informed of any applicable delivery arrangements (including period for delivery)?					
Have you considered whether there is anything else your customers may expect to be told when deciding whether to purchase your device or service?					

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have you ensured that customers are informed about the interoperability of digital content with hardware and software, and any compatibility constraints – including how to port data and whether it is possible for the customer to switch communications provider?	☐	☐	☐	☐	
Additional requirements for off-premises or distance sales (where these are permitted)					
Have you complied with any laws for providing detailed information i.e. ensured that where a contract is concluded by telephone, the seller's identity and purpose of the call is clearly disclosed up-front?	☐	☐	☐	☐	
Have you provided the customer with a copy of the signed contract, or confirmation of the contract, on paper (or another medium if agreed)?	☐	☐	☐	☐	
If the device/service is under a subscription model or a contract of indefinite duration, have you provided information about the total cost per billing period / total monthly costs (if possible) and the way in which the costs are calculated, and any deposits or guarantees the customer has to provide?	☐	☐	☐	☐	
Have you provided information about the cost of using distance communications to conclude the contract if it not a basic rate (eg it is a premium rate services)?	☐	☐	☐	☐	
Have you ensured the customer is provided with detailed information about the minimum duration of a customer's obligations and the terms/conditions for terminating the contract?	☐	☐	☐	☐	
Have you provided the key information above in writing (or another durable medium if agreed) in a legible, plain and intelligible way to the customer?	☐	☐	☐	☐	
Have you provided detailed information about out-of-court complaints and redress mechanisms and how they can be accessed?	☐	☐	☐	☐	

Commentary: Use this space to describe the extent to which your device meets the range of requirements for this principle, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

CHECKLIST 4: SUPPORTING VULNERABLE CUSTOMERS

The requirements for Supporting vulnerable customers are divided into three categories:

Essential – a checklist of what we think is essential for delivering Trust by Design

Good – a more ambitious checklist for actions that by meeting or working towards meeting, show you are a company who takes trust by design seriously, based on existing best practice

Very good – an even more ambitious set of actions, showing you can think ahead about a range of things that can impact on trust, and be a leader in Trust by Design

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
If the device is for a minor, are age restrictions clearly identifiable?	☐	☐	☐	☐	
Have all compliance obligations regarding vulnerable consumers been met?	☐	☐	☐	☐	
Are limitations on use clearly explained?	☐	☐	☐	☐	
Are there additional security provisions in place to address the needs of vulnerable customers and help mitigate risk?	☐	☐	☐	☐	
Are sales staff aware of and able to explain how the device works and how it can or can't be adapted for particular needs?	☐	☐	☐	☐	
Are support staff trained to support and help vulnerable customers after product release, and provide assistance as needed?	☐	☐	☐	☐	
Are vulnerable customers' needs considered during the project design phase?	☐	☐	☐	☐	
Are there policies in place setting out how staff should engage with vulnerable consumers?	☐	☐	☐	☐	
Can the device be adapted for use by a wide range of customers?	☐	☐	☐	☐	
Can the device be adapted for use by all groups of customers?	☐	☐	☐	☐	

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Are there safeguards in place on the device that can stop it being used to control or coerce another person?	☐	☐	☐	☐	

Commentary: Use this space to describe the extent to which your device meets the range of requirements for this principle, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

CHECKLIST 5: CUSTOMER SERVICE AND COMPLAINTS HANDLING

The requirements for Customer service and complaints handling are divided into three categories:

Essential – a checklist of what we think is essential for delivering Trust by Design

Good – a more ambitious checklist for actions that by meeting or working towards meeting, show you are a company who takes trust by design seriously, based on existing best practice

Very good – an even more ambitious set of actions, showing you can think ahead about a range of things that can impact on trust, and be a leader in Trust by Design

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Is it made clear to the customer, in your contract/ communications, who to contact and who is responsible for the different elements of a service?	☐	☐	☐	☐	
Have you clearly explained to all customers how they can complain in your pre-sales information?	☐	☐	☐	☐	
Have you provided clear instructions to customers explaining how to use the product or service and contact details for customer support, including FAQs, email and calling details at a minimum?	☐	☐	☐	☐	
Do you retain records of complaints after the complaint is resolved?	☐	☐	☐	☐	
Do you explain to customers who have complained how you will manage their complaint?	☐	☐	☐	☐	
Have you given customers the right to escalate complaints to an alternative dispute resolution ("ADR") scheme or other independent redress service if you cannot resolve it? This should be clearly sign-posted to consumers including at which point they should get in touch in the complaints process	☐	☐	☐	☐	
Do you have a clear internal process for dealing with complaints – including when they should be escalated and to whom, and how long each step in the process should take?	☐	☐	☐	☐	

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have you provided options to complain by telephone and online? Different ways of getting in touch should be available, taking into account both vulnerable consumers and those with accessibility requirements	☐	☐	☐	☐	
Have you trained your staff to understand and deal with complaints?	☐	☐	☐	☐	
Do you keep records of each complaint so you can track complaints and how you are managing them?	☐	☐	☐	☐	
Have you thought about the different types of customer who may need to complain, and taken their needs into account?	☐	☐	☐	☐	
How are you ensuring that all complaints are resolved within a reasonable time frame? And that non-urgent complaints are dealt with within four weeks?	☐	☐	☐	☐	

Commentary: Use this space to describe the extent to which your device meets the range of requirements for this principle, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

CHECKLIST 6: ENVIRONMENT

The requirements for Environment are divided into three categories:

Essential – a checklist of what we think is essential for delivering Trust by Design

Good – a more ambitious checklist for actions that by meeting or working towards meeting, show you are a company who takes trust by design seriously, based on existing best practice

Very good – an even more ambitious set of actions, showing you can think ahead about a range of things that can impact on trust, and be a leader in Trust by Design

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Have measures been taken to ensure that the disposal of any heavy metals and other dangerous substances contained in the connected device or service is not harmful to the environment and human health?	☐	☐	☐	☐	
Have devices and services been designed so that the time sensitive software responds to latent or low use periods in order to save energy? Low energy devices and services are to be welcomed, such as easy to access 'low power use' settings.	☐	☐	☐	☐	
Do you have an environmental policy that makes it a business priority to reduce your impact on the environment and makes environmental impacts a key consideration in how you run your business?	☐	☐	☐	☐	
Have software updates been made available to customers regardless of location, wherever technically feasible and, as a minimum, for the whole expected lifetime of the product?	☐	☐	☐	☐	
Are your devices easily upgradeable to reduce the potential for the device or service to be rendered obsolete? [Lower alternative may be to re-use faulty units/returned units]	☐	☐	☐	☐	
Are devices, adaptors and other connection points compatible with each other to reduce the potential for new incompatible interfaces to render devices obsolete?	☐	☐	☐	☐	

CHECKLIST	Yes	No	Working towards	Does not apply	Commentary
Are devices designed and built with resource efficiency in mind – from using sustainably produced and/or recycled materials and construction methods; to providing clear guidance to customers on the most efficient use, re-use/repair and disposal of the device and its component?	☐	☐	☐	☐	
Have customers been provided with clear, comparable and credible information concerning expected lifetime and reparability of device or service?	☐	☐	☐	☐	

Commentary: Use this space to describe the extent to which your device meets the range of requirements for this principle, and any future plans to improve design, manufacture and after care to reach a higher level in the future.

6. ADDITIONS TO PRIVACY CHECKLIST

KEY TERMS RELATED TO PRIVACY CHECKLIST

Below are highlights of the most relevant definitions for the purposes of this document.

Anonymisation refers to irreversible de-identification of personal data. This is a very high standard. Often data is not anonymous even if related identifiers have been hashed with randomly generated identifiers, as the data can be re-identified by cross-correlating it with other data sets, thereby making it identifiable again.

Communication means any information exchanged or conveyed between a finite number of parties by means of an electronic communication network or electronic communication service. As communication related data often includes personal data, it has to be processed with the same care and subject to these requirements. Note, however, that processing of communication related data is subject to more stringent requirements, under many applicable laws, than personal data is.

Confidential communications related information means information such as network traffic data, call, messaging and other communications logs and content of the communications, for example SMS, MMS, voicemail.

Consent is the freely given, revocable (where relevant), informed, conspicuous, unambiguous, comprehensive indication of wishes which signify the data subject's (consumer, employee or other) agreement to their personal data being processed. Consent must be understandable so that an average person without technical knowledge would understand the privacy implications of the activity in question.

Explicit consent is a specific act of consent, for example ticking a box or changing a consent setting. Consent is sought separately from mere service terms or privacy policy approval, for example, by way of opt-in. Consent also exists when the user makes an active informed choice, for example:

- The user's request or use of a feature clearly indicates permission to use location data or user information (e.g. "find nearest gas station");
- When at the time of enabling a setting or feature, the setting or a feature itself clearly informs the user that location data or user information will be shared with defined parties; or
- The user inserts information into a text field or chooses information through a drop-down menu and the use of the information is indicated to the user; and
- The other conditions for consent as defined above are met.

Location data means any information that indicates or can be linked to the geographical location of the device, typically established through triangulation (for example, GPS, cell-tower or Wi-Fi based location data). Examples of data that is not location data include:

- User "manages his presence" e.g. makes a statement that he is "currently at home"
- IP address-based location (can easily be faked and only provides a high-level approximation of the location at best).

Network based location data refers to location which is established from the mobile network without accessing information on the user's device. NOTE: the rules related to network based location data only apply to markets where the distinction is made. In the absence of a specific rule, the generic rules for location in this document apply.

Personal data means any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity. It is thus a very broad concept which includes, without limitation, information such as:

- Directly identifiable information such as name, email address; and/or
- Indirectly identifiable information such as mobile phone number (MSISDN), user or screen name (e.g. jsmith999), IP address, unique identifiers such IMSI, IMEI (where these can be linked to other information which links such identifiers to an individual) and any other form of unique identifier which enables an individual to be identified as an individual; and/or
- Information associated with directly or indirectly identifiable information such as account related information i.e. address, payment details, CDRs and information extracted from CDRs such as billing or

usage information; and/or
- The private content generated by individuals such as cloud storage of contacts, photos, music, communications etc.

Processing refers to the full lifecycle of personal data and includes any and all operations performed with such data, for example collection, recording, organisation, storage, adaptation or alteration, analytics, reporting, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, blocking, erasure, anonymization or destruction of personal data.

Pseudonymisation refers to reversible de-identification of personal data, for example by maintaining a key which can be used to re-identify hashed identifiers.

Traffic data means data processed for the purpose of conveying a communication in an electronic communications network or billing of that communication. As traffic data often includes personal data, it has to be processed with the same care and subject to these requirements. Note, however, that processing of traffic data is subject to more stringent requirements, under many applicable laws, than personal data is.

Traffic Data includes data relating to the routing, duration and time of the communication such as IP-address, Electronic Serial Numbers (ESN), International Mobile Equipment Identity (IMEI) codes, International Mobile Subscriber Identity (IMSI) codes, mobile IDs, MSISDN codes, telephone numbers, parties to a communication and other such information.

GUIDANCE NOTE ON MINIMUM CONTENT OF PRIVACY NOTICE

The Privacy notice referred to in checklist 2 must provide information about at least the following items:

1. The identity and the contact details of the controller and, where applicable, of the controller's representative;
2. The contact details of the data protection officer, where applicable;
3. The categories of personal data being processed, including also traffic data and content of communications, if applicable;
4. The purposes of the processing for which the personal data is intended as well as the legal basis for the processing;
5. Where the processing is based on legitimate interests of a third party (instead of consent or processing that is necessary to perform the contract with the data subject), the legitimate interests pursued by the third party;
6. The recipients or categories of recipients of the personal data, if any;
7. Where applicable, the fact that that the Mobile Service Provider transfers personal data to a third country or international organisation, including reference to the appropriate or suitable safeguards that provider has put in place, and where applicable, the means by which data subject can obtain a copy of or where they have been made available;
8. The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
9. Whether or not any tracking technologies are used and what data they collect and for which purposes;
10. The existence of the right to request, from the controller, access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
11. Where the processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
12. The right to lodge a complaint with a supervisory authority;
13. Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data, and of the possible consequences of failure to provide such data;
14. Whether or not automated decision-making, including profiling, takes place and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.


BUDGET
Today
£0.60
£0.58
next
usage
menu
£ 0.05
£ 0.06
£
kW

CONSUMERS INTERNATIONAL

COMING TOGETHER FOR CHANGE

Consumers International brings together over 200 member organisations in more than 100 countries to empower and champion the rights of consumers everywhere. We are their voice in international policy-making forums and the global marketplace to ensure they are treated safely, fairly and honestly.

consumersinternational.org

@consumers_int

/consumersinternational