Guidance for consumer Internet of Things products and services

0.0.22 | 20 June 2025

Guidance for consumer Internet of Things products and services

> 16 06 2025 - the guidance was published.
>
> We are consulting on this draft guidance - please give us your views.

Contents

About this guidance

Why have you produced this guidance?

This guidance explains how data protection law and the Privacy and Electronic Communications Regulations 2003 (as amended) (PECR) apply when you process personal information in consumer Internet of Things (IoT) products.

Read it to understand the law and our recommendations for good practice.

It is not a comprehensive guide to compliance. We link to relevant further reading about any principles we've already covered in our other guidance.

Who is it for?

This guidance is aimed at organisations who process personal information in IoT products. Such organisations are likely to include manufacturers, developers of operating systems, mobile app developers, web app developers, software developers, AI service providers, providers of biometric technologies, providers of sensors and telemetry, cloud providers, and cybersecurity and IT providers.

These organisations are likely to be responsible for processing by IoT products. In this guidance, 'processing by IoT products' refers to processing by those organisations who have relevant data protection responsibilities.

In these organisations, two main audiences will find this guidance useful.

First, those with a compliance focus, including:

- data protection officers (DPOs);
- general counsel;
- risk managers; and
- senior management.

Second, technology specialists, including:

- product and UX designers;
- cybersecurity and IT risk managers.

If you are a product or UX designer interested in practical recommendations and illustrations on how to implement data protection, see the sections on:

- data protection by design and default;
- lawfulness;
- transparency;
- individual rights; and
- children.

If you are a cybersecurity or IT specialist wanting to understand what security measures you should consider, see the sections on

- data protection by design and default; and
- security.

What is the Internet of Things?

IoT is a broad term that applies to a network of physical products incorporating sensors, software, processing ability and different types of connectivity (including the internet), which enable these products to process information. IoT products can often connect to one or more IoT products.

What does this guidance cover?

This guidance covers the processing of personal information by organisations providing IoT products on the consumer market.

Consumer IoT products include:

- home entertainment products (smart speakers, connected TVs, connected toys);
- home automation products (smart lights and lightbulbs, smart thermostats, smart home hubs);
- domestic appliances (smart fridges, smart ovens);
- wellbeing products (fitness trackers, smart watches, smart scales, sleep monitors);
- security and safety products (smart security cameras, smart doorbells, smart baby monitors);
- over-the-counter medical devices (smart fertility trackers with a device, smart blood pressure monitors, smart pulse oximeters); and
- peripheral products (smart keyboards, smart mice, smart headphones).

What doesn’t this guidance cover?

This guidance doesn’t cover:

- connected and autonomous vehicles;
- smart meters;
- smart cities; or
- the use of IoT products in enterprise and industrial settings.

Also, this guidance specifically doesn’t cover:

- mobile phones;
- tablets; and
- computers.

Where this guidance refers to principles addressed in other guidance, we provide links to the relevant further reading.

How should we use this guidance?

To help you understand the law and good practice as clearly as possible, this guidance says what organisations **must, should,** and **could** do to comply.

Legislative or legal requirements

- **Must** refers to legislative requirements.

Good practice

- **Should** does not refer to a legislative requirement, but what we expect you to do to comply effectively with the law. You should do this unless there is a good reason not to. If you choose to take a different approach, you must be able to demonstrate that this approach also complies with the law.
- **Could** refers to an option or example you could consider to help you comply effectively. There are likely to be various other ways you could comply.

What information do IoT products use?

In detail

Do IoT products process personal information?

Personal information is information that relates to an identified or identifiable person.

In most cases, IoT products process personal information. This is because they are designed for people to interact with them, and many often require a user account to operate.

Remember, if you cannot identify someone directly from the information you hold, it may still be possible to identify them indirectly.

You **must** consider the information you process through IoT products and all the means that you or anyone else are reasonably likely to use to identify someone.

The range of personal information you collect may be extensive. For example, the lifecycle of a single IoT product may involve processing personal information that you:

- obtain directly from the user, such as when they give personal information like their name, date of birth, email address, user account information;
- obtain from another source, like a third party (eg a social media company or other mobile apps for purposes such as account linking);
- observe about how the user interacts with the product and any associated services (eg an app);
- collect from the product's hardware and software, such as sensors, device identifiers, voice and video recordings, images, movements, temperature, location; and

- infer about someone, for example, by combining and analysing information you collect from the user, the product or other sources, and by making inferences about their behaviours, characteristics or preferences.

It is important to be aware that information you hold may indirectly identify a person, so it could constitute personal information. This may be the case even if you need additional information to be able to identify someone, because they may still be identifiable. You may already hold that additional information or may need to get it from another source.

Further reading – ICO guidance

What is personal information: a guide

Do IoT products process special category information?

Special category information is personal information about a person's:

- race;
- ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data (where this is used for identification purposes);
- health data;
- sex life; or
- sexual orientation.

Special category information includes anything that reveals or concerns these categories of personal information. This also covers cases where you intend to infer or guess details about someone that fall within these categories.

IoT products and services may use special category information, whether directly or by inference; for example, where:

- the core functionality of your product requires this data; or
- you intentionally infer it, for example to provide your users with a 'health score' reflecting your assessment of their physical health.

You **must** process special category information only if you can identify both a lawful basis and a valid condition under article 9.

Most of these conditions mean you **must** be able to demonstrate that using special category information:

- is necessary and proportionate; and
- complies with the data minimisation principle.

Further reading - ICO guidance

- Special category data
- Data minimisation

IoT and health data

The UK GDPR defines health data in Article 4(15) as:

> "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

Health data can be about someone's past, current or future health status.

It not only covers specific details of medical conditions, tests or treatment, but also any related information that reveals anything about the state of their health.
Some types of IoT products are designed to process health data, whether directly or by inference (or inherently involve its processing).

Example

Fitness trackers and smart watches can track a user's step count. The step count information is transmitted from the product to the IoT manufacturer's servers that process the information. Step count does not

automatically reveal the user's health status. For example, low step counts may occur for several reasons, such as:

- the user not wearing the device often;
- hardware or software errors; or
- engaging in other types of non-step based activity (eg cycling).

So, step count on its own is unlikely to be health data.

However, when a person uses a fitness tracker as part of their insurance policy and the insurance company uses step count to predict their health when calculating their insurance premium, then step count is likely to be health data.

Example

A fitness tracker asks to input a user's height and weight to calculate their body mass index (BMI). The user's height, weight and BMI is transmitted from the product over a network to the IoT manufacturer's servers that process the information. Based on whether the BMI score is low, high or normal, the fitness tracker makes recommendations for a training regime.

Height and weight are not necessarily health data on their own, but the user's BMI score is more likely to be. This is because BMI scores may reveal something about the user's health status.

Example

A woman uses a smart fertility tracker to record the dates of her periods and body temperature. This information is transmitted from the product over a network to the IoT manufacturer's servers where it is further processed. The tracker makes an inference about fertile days based on this information.

Not only is the information about the user's period and body temperature special category data, the inference about fertile days also falls into this category because it can reveal something about the woman's reproductive health.

Further reading

Health data

Relevant provisions in the DPA 2018 - see Part 7, section 205(1)

https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

IoT and biometric data

Biometric data is a type of personal information that:

- relates to someone's physical, physiological or behavioural characteristics (eg voice, fingerprints, face);
- has been processed using specific technologies (eg a voice recording is analysed to detect qualities like tone, pitch, accent or inflection); and
- can uniquely identify (recognise) the person it relates to.

Biometric data only becomes special category information when you use it for the purpose of uniquely identifying someone. We call this 'special category biometric data'.

This means that if you are using biometric data but not for the purpose of uniquely identifying someone, it is not special category biometric data.

Your purpose for processing biometric data therefore defines whether you're processing special category biometric data.

Example

A smart speaker with an embedded voice assistant allows people to create a voice ID. The voice ID is a digital representation of a user's voice, which is used to match their spoken voice and identify the particular user asking a query to the voice assistant. The accompanying app for the smart speaker records the query and the name of the user who asked it.

Voice ID is biometric special category data because it is used to uniquely identify that user.

If a user asked a voice assistant a query without having voice ID set up for their voice, their voice query is also biometric special category data. This is because the voice query is still processed by the voice assistant to match against any existing voice IDs. So it is at least partly processed for the purpose of uniquely identifying someone.

Further reading

Biometric recognition guidance

IoT and location data

Some IoT products may process information about their geographical location. Location data is not special category information. But people may consider it to have a level of sensitivity because it can reveal a lot about their lives.

This means it can be personal information, so if you process it you **must** comply with the UK GDPR. In this context, you **should** consider:

- the level of location granularity you need to deliver certain features of your IoT products and services;
- only collecting location information that is essential to provide the service your users request;
- offering different location options for individual product features;
- identifying potential risks to people from processing their location, such as measures or safety features you can implement to mitigate these risks; and
- where appropriate, providing a clear and easy-to-find setting for users to turn location data on and off.

If your IoT product includes a service likely to be accessed by children, you **should** conform to the requirements of the geolocation standard in our Children's code. This may affect your overall design choices. For example, the Children's code says any geolocation setting you provide **should** be switched off by default unless you can demonstrate a compelling reason for it to be enabled.

Other specific rules may apply depending on the type of location information that your IoT product (or its associated app) processes. This is because PECR

contains provisions about both location data and device information. See the section on PECR for more information.

Further reading – ICO guidance

- Geolocation standard in the Children's code
- Guide to PECR – location data
- Guidance on storage and access technologies

People might use IoT products in the home – does the UK GDPR still apply?

People often use IoT products as part of their daily lives, which may make unclear whether data protection law applies to the processing.

This is because the UK GDPR does not cover processing by a person in the course of a purely personal or household activity. We call this 'domestic purposes'.

But it's important to note that this doesn't make **any** processing by an IoT product exempt from the law. While many consumer IoT products are designed to be used in the home, this doesn't mean **your use** of any personal information they collect is also out of scope. As this is processing you undertake for your own purposes, you **must** comply with the law when doing so – for example, when providing an IoT service or collecting information from IoT products as part of that service.

And the UK GDPR is clear that if you provide the means by which people process personal information for domestic purposes, the law applies to you.

These are important considerations you **must** take into account when you design any IoT product or service that intends to collect personal information.

Example

A driver is using a smart dash camera in their car. The dashcam records the road and surroundings when the car is on the move. The driver can view the footage from the dashcam in the accompanying app.

Although the dashcam's recordings capture public spaces as the driver uses the car, the product is not being used to continually monitor a specific public space but is instead capturing images related to the movements of the car when used by the driver. Capturing the images is part of the driver's personal activity when using the car.

However, if the driver posts dashcam recordings online, the processing of any personal information captured by the dashcam will no longer be in the course of the driver's personal activity. This processing is within scope of the UK GDPR and the driver will need to identify an appropriate lawful basis.

The manufacturer's processing of personal information in the dashcam falls within scope of the UK GDPR because it is processing carried out by a legal entity rather than by a person. It is a commercial, rather than a personal or household, activity.

Example

A person owns a smart speaker with an embedded virtual assistant. They use it for different purposes, including to play music, use a search engine or make calendar appointments.

Other people in the household use the smart speaker, including family members and visiting friends. Processing of other people's information when they use the smart speaker is a purely personal or household activity by the person who owns the smart speaker.

However, processing the personal information by the smart speaker manufacturer falls within scope of the UK GDPR because it is processing carried out by a legal entity for its own purposes, rather than by someone in the context of a personal or household activity.

The smart speaker manufacturer should design their product in a way that provides controls for users to configure product settings to minimise the personal information it collects.

Further reading – ICO guidance

- Video surveillance (including guidance for organisations using CCTV)

- A guide to the data protection exemptions

Relevant provisions in UK GDPR - see Article 2(2)(a)

https://www.legislation.gov.uk/eur/2016/679/article/2#:~:text=Article%202%20U.K.%20Material%20scope%20[F1%201.%20This

Does PECR apply to IoT products?

What PECR rules are relevant for IoT products?

Most of the PECR rules concern things like direct marketing or security of communications providers. But a specific one applies when you use technologies that store information (or access information stored) on a user's terminal equipment.

This is regulation 6, and it applies to the use of technologies like:

- cookies;
- tracking pixels;
- local storage;
- device fingerprinting;
- scripts and tags;
- application programming interfaces (APIs);
- automatic content recognition (ACR); and
- software development kits (SDKs).

Are IoT products 'terminal equipment'?

If an IoT product is connected to a public communications network (eg the internet), it is 'terminal equipment' so PECR rules apply. This is true whether the IoT product is connected directly or indirectly (eg through another device that has a network connection).

It's also true whether the information that the product processes is streamed or cached for intermittent reporting. This is because information on the IoT product is stored or accessed, or both – for example, where you send or receive data from the device.

If your IoT product connects to the network through another network-connected device, any transmission of data to that device falls outside the scope of PECR.

However, if you store or access information that the network-connected device collects from the IoT product, PECR does apply to these processing activities.

Example

A smart lightbulb does not automatically connect to a network. The lightbulb needs to connect to its accompanying app on a mobile phone via Bluetooth to transmit information over the internet to the lightbulb manufacturer. The transmission of information between the smart lightbulb and the mobile phone falls outside the scope of PECR.

When information from the accompanying app on a mobile phone attached to the smart lightbulb is stored or accessed by the manufacturer, PECR rules apply.

How do PECR rules interact with UK GDPR?

Unless an exemption applies, PECR says you **must:**

- provide "clear and comprehensive information" to your users about the purposes of any storage or access in the IoT product; and
- obtain the user's prior consent (to the UK GDPR standard).

PECR does not define 'clear and comprehensive information'. However, in practice it refers to the UK GDPR's transparency requirements, the right to be informed and the conditions for consent.

So, if you design your IoT product to use storage and access technologies, to comply with PECR you **must** provide the same information to subscribers and users as you would when you process their personal information.

If you have to obtain consent for your use of storage and access technologies, and the information is personal information, then you **should** use consent as your lawful basis under the UK GDPR for subsequent processing.

Example

A smart TV company is using automatic content recognition (ACR) technology on their smart TVs to serve their users personalised ads.

The ACR technology periodically captures content displayed on the TV and matches it against a content library to identify what the user is watching. Based on content matches, the smart TV users are served personalised ads.

The company needs to access information on each user's TV to match against the content library. Because the ACR technology is storing and accessing information on the user's TV (ie terminal equipment), the company needs to obtain valid consent under PECR to use it for advertising.

When users start setting up their smart TV, the ACR is off by default. The smart TV asks them during the TV set-up process whether they would like to switch on this feature. Users are shown a short explanation of the technology. On the TV screen, users are presented with options to accept or reject the use of the ACR technology with equal prominence. Users can revisit their choice about ACR in the settings.

Read the sections of this guidance on consent and transparency for more details about the relevant requirements.

Do we need consent for online advertising purposes?

You **must** get consent if you use storage and access technologies for online advertising purposes in your IoT products.

This applies both to the technical processes involved in ad selection and delivery, as well as any associated tracking and profiling.

This is because use of storage and access technologies for the purposes of online advertising is not strictly necessary to provide an online service via your IoT product. You might consider generating income through advertising necessary for your business but on a technical level, you can provide the service without any advertising.

Remember, you must also have an appropriate lawful basis for any processing of personal information for the purposes of profiling and targeted advertising (eg a person's viewing habits on a smart TV). If you need

consent for your use of storage and access technologies, and the information is personal data, you should use consent as your lawful basis under the UK GDPR for subsequent processing.

If your product is aimed at children or is likely to be accessed by them, you should ensure that online behavioural advertising is off by default.

Example

A company wants to serve digital advertising on the screen of their home hub product. The company integrates a software development kit (SDK) into the home hub that collects information about users' behaviour, users' interactions with the home hub and their preferences. It uses the information to enable the display of targeted ads to users when they engage with the home hub.

The company gets valid consent from their home hub users before starting this processing. It offers users options of equal prominence to make a choice about whether or not they want their advertising to be personalised. It also provides settings for users to withdraw their consent at any time after they set up their product.

Further reading – ICO guidance

Guidance on the use of storage and access technologies

Relevant provisions in PECR - see regulation 6

https://www.legislation.gov.uk/uksi/2003/2426/regulation/6

How do the PECR rules on location data apply?

PECR contains a specific definition of 'location data'. For PECR, this is information that a network or service collects about where the user's device is or was located.

The rules on location data are in regulation 14 and are strict. You can only process this data if you are a public communications provider, a provider of a value-added service, or a person acting on the authority of such a provider, and only if:

- the data is anonymous; or
- you have the user's consent to use it for a value-added service, and the processing is necessary for that purpose.

For most organisations that make IoT products, the processing of location data under regulation 14 isn't possible. This is because they are not public communications providers or value-added service providers.

How are the PECR rules on terminal equipment relevant to location data?

IoT product providers may process other information about a person's location, even if it doesn't meet PECR's definition of location data. For example, the rules on location data don't apply to GPS-based location information or data about connections with local wifi equipment.

This is because these types of data are created and collected independently of the communications provider.

However, a different part of PECR may apply to the processing of this data. If you obtain information about a person's location by storing or accessing information on their IoT product, you **must** comply with regulation 6.

Further reading – ICO guidance

- Guide to PECR – location data
- Guidance on storage and access technologies
- Geolocation standard in the Children's code

How do we ensure accountability in IoT products?

In detail

What is accountability?

Accountability is a principle of data protection law. It means you are **responsible for complying** with the data protection principles, and that you are able to demonstrate that compliance.

Getting accountability right when you start developing your IoT product or service will help you take an approach that includes data protection issues from the beginning.

You **should** think about some things at the earliest stages. These include:

- correctly allocating roles and responsibilities regarding any organisation(s) you work with;
- identifying and assessing the risks in your processing;
- considering any specific needs or requirements if your IoT products and services are likely to be accessed by children; and
- adopting a data protection by design approach.

How should we understand controller/processor relationships in IoT?

It is common for multiple organisations to be involved in the processing activities of IoT products and services. In these cases, a crucial aspect of accountability is properly allocating roles and responsibilities.

Any one organisation may be:

- a **controller** – if it has overall control over the purposes and means of the processing;
- a **joint controller** – if it jointly makes decisions about the purposes and means with other organisations; or
- a **processor** – if it acts only on another organisation's behalf under its instructions.

Which role an organisation plays depends on:

- the specific processing of personal information taking place;
- the circumstances in which this happens; and
- who has genuine, real-life influence and control over the purposes and means of the processing.

A first step to working out your role is to identify the distinct sets of processing operations and their purposes. Whoever makes the overarching decisions about the 'how' and the 'why' of the processing is a controller.

As IoT products process personal information for several purposes, you may be a controller or joint controller for some phases of the processing and a processor for others.

What types of decision do controllers take?

Controllers make decisions about:

- whether to collect personal information in the first place;
- what types of personal information to collect;
- the purpose or purposes for which the personal information is to be used;
- which people to collect the personal information about;
- how long to retain the personal information; and
- how to respond to requests from people about their rights.

Organisations that, as a matter of fact, determine the purposes and means of processing are controllers regardless of any description of their role in a contract.

When could we be a joint controller?

Joint controllers jointly decide the purposes and means of processing. Organisations are not joint controllers if they are processing the same information for different purposes.

If your processing involves multiple organisations, you **should** take the time to assess and document the status of each organisation you work with covering all your personal information processing activities.

If you and another organisation process for the same or for shared purposes, you are joint controllers.

What types of decision do processors take?

If you don't have any purpose of your own for processing the personal information and you only act on a client's instructions, you are likely to be a processor – even if you make some technical decisions about how you process the personal information.

For example, where allowed in the contract, processors can make decisions about:

- the IT systems and methods to process personal information;
- how to store the personal information;
- the security measures that will protect it; and
- how to retrieve, transfer, delete or dispose of it.

How do these roles apply to IoT?

There are likely to be multiple parties who process personal information in the IoT ecosystem contributing to the creation and functioning of IoT products. For example:

- device manufacturers;
- application developers;
- software development kit providers;
- operating system providers;
- app stores;
- IoT platform and cloud providers; and
- organisations producing or providing other IoT products and online services.

In some instances, only one organisation make decisions about the design and delivery of an IoT product or service. If so, only that organisation is the controller for the personal information the product or service processes.

However, in practice the IoT ecosystem can be complex. Most processing by IoT products and services is likely to involve more than one organisation.

So if your IoT processing involves different types of commercial and technical arrangement with different entities, you **must** establish the respective responsibilities of each, taking into account:

- the specific circumstances of the processing involved; and
- the processing activities for which each party determines the purposes and means (whether alone or in combination).

In practice, this probably requires a case-by-case assessment depending on the processing activities.

Example

Manufacturers design and develop the IoT product's hardware or software. They may play a role in determining its overall functionality. They may also collect personal information that the device generates for their own purposes. These sorts of activity may make them controllers.

Application developers build mobile apps or other software and services to allow people to interact with the IoT product. They may have made decisions about how the app works, what data it collects and how information is stored or accessed.

The manufacturer and the app developer may be the same organisation. If so, it is responsible for the overarching decisions about the processing but:

- a manufacturer might build the product, but engage a specialist app developer to design the associated mobile app;
- an app developer might outsource some of the processing to another organisation; or
- an app developer might enable data access by other organisations, eg ad networks or other third parties via an SDK.

Example

An IoT manufacturer works with an SDK provider that provides services requested by the IoT manufacturer. The SDK provider is therefore a processor in this relationship.

The SDK provider only processes personal information for the purposes defined by the IoT manufacturer. The SDK provider acts on the IoT manufacturer's behalf.

Example

An IoT manufacturer works with an SDK provider that provides services requested by the manufacturer.

The SDK provider also processes personal information about the manufacturer's IoT product for its own purposes. It produces statistics about how its SDK works with the manufacturer's IoT product to improve its own service.

The SDK provider and IoT manufacturer have a data-sharing agreement so the SDK provider can use the information for its own purposes. The SDK provider also needs to identify an appropriate lawful basis for its processing.

In this instance, the SDK provider and the IoT manufacturer need to determine whether they are separate controllers or joint controllers.

Further reading

- Controllers and processors
- Data sharing: a code of practice
- Privacy in the product design lifecycle

What do we need to do if children are likely to use our IoT products or services?

If your IoT products (and associated services) process children's information, you **should** take into account that children merit specific protection because they may be less aware of their rights and of the risks involved in the processing.

You **must** also consider whether you need to conform to the Children's code. The code applies to relevant 'information society services', which broadly cover any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

If your IoT product is likely to be accessed by a child and you are a relevant ISS, you **should** conform with our Children's code. You should read the code alongside the UK GDPR. The code supports compliance with the general data protection principles by setting out specific standards for the design of online services likely to be accessed by children.

You **should** conform to the standards in this code if you provide an IoT product or service likely to be accessed by a child.

Examples include products or services:

- specifically aimed at children such as a smart toy, a children's fitness tracker, a children's virtual reality headset or a children's smart speaker; and
- not specifically aimed at children but likely to be accessed by them, like a smart home hub, smart speaker (aimed at the general population) or a smart doorbell.

If you provide electronic toys or products that do not connect to the internet, and only store personal information within the product itself, you may not need to conform to the code – for example, if any personal information they process is only stored on the product itself. However, even in cases where you don't collect information from the devices, you must still follow a data protection by design approach when you make them.

Refer to the Children's code for the complete list of its standards and assess how they apply to your processing.

Further reading – ICO guidance

- Age appropriate design: a code of practice for online services
- Children and the UK GDPR
- The Children's code design guidance
- Children's code self-assessment risk tool
- Children's code – tools for completing a data protection impact assessment (DPIA)
- Sample data protection impact assessment: Connected toy

What risks do we need to manage?

Consumer IoT products are often designed for use in the home, where people have the biggest expectation of privacy. For example, they can be used to monitor people's activities and behaviours, as well as those of their households, friends and family. So, IoT products can reveal information about people continuously and at a large scale.

You **should** assess whether you need to process personal information to your IoT product. You **must** also decide how long it is necessary to keep people's personal information. If you decide to collect and store it, you **must** ensure you protect it with appropriate measures.

This is not meant to be a comprehensive guide to all the risks to people's rights and freedoms associated with the processing of personal information by IoT products and services. However, potential risks may arise from:

- extensive and intrusive tracking and profiling, eg of people's locations and behaviours;
- lack of control and information asymmetry;
- use of IoT products by multiple users with limited controls available for all all of them;
- inadequate security and the possibility of personal data breaches; and
- unclear roles in the IoT supply chain, meaning different organisations don't assign responsibilities correctly.

Many IoT products process special category health and biometric data as well as data about users' location. They may also be designed to create personalised experiences for their users, giving them many benefits. However, if you don't follow a data protection by design and by default approach, your processing can lead to harms.

The harms can include people feeling they've lost control over their personal information. In some cases, this can lead to psychological distress (such as anxiety). Children may be especially susceptible to psychological harms from information revealing details about their preferences and personalities. People may lose trust in how their IoT products process personal information. This can lead to a chilling effect when people don' turn on the smart features.

The feeling of losing control may be accentuated when multiple users use an IoT product but they don't have the same level of control over how it processes their personal information. Users who don't have an account for the IoT product or are not the main user may find it difficult to get the

relevant privacy information about the processing of their information, or to make choices or exercise their rights. If people don't know how to exercise their rights, products may be sold on the secondary market or passed to others with the original owner's personal information.

Personal data breaches relating to IoT products can often lead to financial or even physical harms. For example, people may become victims of fraud if their IoT product is hacked, or their home may be burgled if their smart lock's security is breached.

Personal information from IoT products is shared with many third parties because of the complex supply chain that is involved in creating and running IoT products. This complexity increases the risk that people will lose control over their personal information and experience unwarranted intrusion into their lives.

Do we need to do a data protection impact assessment (DPIA)?

A DPIA is a tool you can use to identify and reduce the data protection risks of your processing activities. It can also help you design more efficient and effective processes for handling personal information.

DPIAs can determine the type of technical and organisational measures you need to ensure your processing complies with the data protection principles.

You **must** do a DPIA before you begin any type of processing that is "likely to result in a high risk". You **must** screen for factors that point to the potential for widespread or serious effects on people.

Three types of processing always require a DPIA:

- systematic and extensive profiling on which significant decisions are based;
- large-scale use of special category data; and
- large-scale monitoring of publicly accessible areas.

We have published a list of processing operations where we have assessed there is likely to be a high risk and you **must** do a DPIA. You can find the full list in the DPIA guidance.

Most processing involving IoT products is likely to result in a high risk. This is because IoT products are often part of people's private lives, processing

information of a highly personal nature – for example, about their households, location, health, physiology, daily habits and relationships. This means that in most cases you **must** do a DPIA.

Also, if you offer your IoT product or service to children, you **must** do a DPIA. Processing children's information in this context is likely to result in a high risk, so is included on our list of processing operations that require a DPIA. If children are likely to access the product or service, you **should** refer to the Children's code for information about conducting a DPIA.

Read our guidance on DPIAs for more detail on when and how you should write one.

The severity of harms that may arise may be greater than in other processing contexts. This is because of the volume and sensitivity of the personal information IoT products can process.

Further reading

- DPIAs
- Data protection audit framework
- Accountability framework
- Children's code standard on DPIAs

How do we apply a data protection by design and default approach?

You **must** adopt a data protection by design and default approach. This means you **must** consider data protection and privacy issues upfront at the design stage and throughout the lifecycle of your IoT product and any associated service.

Data protection by design means you **must** put appropriate technical and organisational measures in place to implement the data protection principles effectively and safeguard people's rights.

To do this, you should address each stage of your product's lifecycle and ask yourself the following questions.

Planning, research and design of an IoT product

- Do you need to use personal information?

- What is the minimum personal information you need for your product to function?
- Have you identified the most appropriate lawful basis for your processing?
- Do you need to use special category information? What alternatives have you considered? Can you achieve your purpose in a less intrusive way?
- Do you need to use profiling or automated decision-making?
- Have you considered if children are likely to use your product? Have you considered what is in the best interest of a child? Have you made arrangements to process only the minimum personal information about children? Are you able to comply with the Children's code?
- Are multiple users likely to use your product? How will you give them choices about their personal information?
- Have you considered what controls you may need in place if your product is sold on the secondary market or passed on?
- Will your product involve working with any partner organisations? Have you established their roles (eg controllers, joint controllers or processors)? What do you know about their own compliance and what due-diligence checks will you make?
- Are there any privacy-enhancing technologies (PETs) that could help you comply with your data protection by design obligations?
- What risks could your users face from using your IoT product? What steps will you take to prevent your product harming people?
- How will you embed data protection into your business model?
- What security measures will provide appropriate protection for the information your product processes?
- How will you enable people to exercise their rights? How can you do this for multiple users?
- Have you consulted all relevant internal stakeholders, such as your legal team, designers, cybersecurity specialists, software developers and your DPO before launching the product?

Launch of an IoT product

- Does your product offer strong privacy defaults, user-friendly options and controls, and respect user preferences?
- Do you give people tools so they have meaningful control over how you use their personal information?
- Do your communications use clear and plain language so your users can understand what you intend to do with their personal information?

- Have you planned what to do if the launch leads to the processing of personal information you didn't intend?
- Is your customer support team able to respond to customer feedback after the launch?

Post-launch of an IoT product

- Are you monitoring for any potential privacy issues? Do you have policies in place for remedial action, and sufficient resources to carry it out?
- Are you regularly updating your product with security patches to respond to new threats and vulnerabilities?
- Are you aware of people using your product after launch in ways you didn't expect? Have you planned how you'll manage any emerging privacy implications?
- Are you planning to release any updates for the product that may change how people's information is used? Have you assessed if people's expectations for privacy would change because of the update before doing so? Do you need to reconsider your lawful basis?

Our guidance on privacy in the product design lifecycle includes more detail on considerations for each phase of a product lifecycle.

If your product is aimed at children or likely to be accessed by them, your IoT product's settings **must** be set to 'high privacy' by default. You **should** collect and retain only the minimum personal information you need to provide the elements of your IoT product. You **should** refer to the Children's code for a full list of what to consider.

Further reading – ICO guidance

Data protection by design and default

How do we ensure our IoT products process information lawfully?

In detail

How do we choose the right lawful basis?

To process personal information, you must have a valid lawful basis. There are six available lawful bases for processing:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task; and
- legitimate interests.

No single basis is 'better' or more important than the others. The most appropriate basis for your processing will depend on your purpose and relationship with the person.

With most IoT products and associated services, the most relevant lawful bases are consent, contract, legal obligation and legitimate interests. If you use storage and access technologies, you must use consent unless a PECR exemption applies.

Most lawful bases require that processing is 'necessary' for your specific purpose(s). You **must** determine your lawful basis before you begin processing. You **should** document it – and remember, you **must** tell people what lawful basis you are using in the privacy information you give them.

Read our guidance on storage and access technologies for more information about the interplay between PECR rules and choosing your lawful basis.

Special category conditions

You **must** have a valid condition for processing special category information.

Article 9 of the UK GDPR contains 10 conditions for processing special category information. Schedule 1 of the DPA 2018 provides further requirements for meeting some of these conditions. Read our guidance on special category information for more details about the conditions.

Further reading – ICO guidance

- A guide to lawful basis
- Lawful basis interactive guidance tool
- Special category data
- How do the PECR rules relate to the UK GDPR?

How do we ask for consent in IoT products?

You **must** ensure that consent is:

- freely given;
- specific;
- informed;
- unambiguous; and
- given by a clear affirmative act.

You **must** ensure that it represents a person's active choice and be as easy to withdraw as it is to give.

If you make consent a precondition of the service but the processing is not necessary for that service, the consents you obtain are invalid.

How do we inform people?

Being informed means people know what information you want to process and why, and also the consequences of giving their consent.

IoT products can have different interfaces, including a small or large screen, voice and sound interface, mobile app or web app. You **should** consider what is the best method for your relevant interface when you ask for consent and when you give people the information they need to make decisions.

For IoT products with no screens or small screens, you **should** make your requests for consent available somewhere else (eg on an accompanying mobile app). This is because a product without a screen doesn't provide a

way to show a consent request. And it may be difficult for you to provide the required information on a small screen.

Example

A graphic shows:

- a smart watch (ie a product with a small screen); and
- a smart speaker (ie a product with no screen)

handing over to the product's accompanying mobile app to allow users to make choices about the processing of their personal information.

How you present choices in an interface can help people make better decisions, but it can also affect their actions and, if done badly, invalidate their consent.

If your IoT product is aimed at children or likely to be used by them, the UK GDPR and DPA 2018 specify that if you rely on consent for any aspects of your processing, you must get parental authorisation for children under 13. You should refer to the Children's code for more detail on how to approach your requests for consent from a child.

What does 'freely given' mean?

You **must** give people genuine choice and control over how you use their personal information. If people don't have a real choice, their consent is not freely given and is invalid.

People must be able to refuse consent without detriment as well as to withdraw it easily at any time.

You **must** ensure that the consent you obtain is unambiguous. So your consent interfaces must involve a clear affirmative action (an opt-in). Pre-ticked opt-in boxes are specifically non-compliant under UK GDPR.

If you offer multiple choices in a consent interface, you must not make one more appealing or prominent than another. This is likely to invalidate the user's consent.

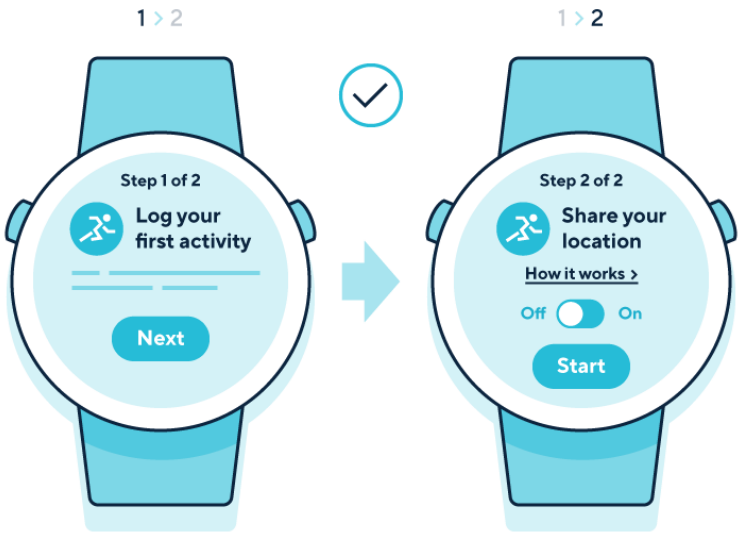
You **must not** ask for consent in quick succession or repeatedly.

You **could** introduce positive friction into the consent mechanisms to help people consider their choices. Positive friction might require a user to slow down as they interact with consent mechanisms and consider their choices.

You may want to avoid disrupting the user's experience, but this does not override your need to ensure that consent requests are valid – so some level of disruption may be necessary. However, you should be careful to avoid making consent requests unnecessarily disruptive.

Example

A graphic shows a smartwatch being set up by a user. The user has gone through 12 of the 20 steps of the set-up where they have been asked to make choices about the processing of their personal information. This set-up shows requests for consent in quick succession. The user is unlikely to be able to consider all the requests to provide freely given consent.



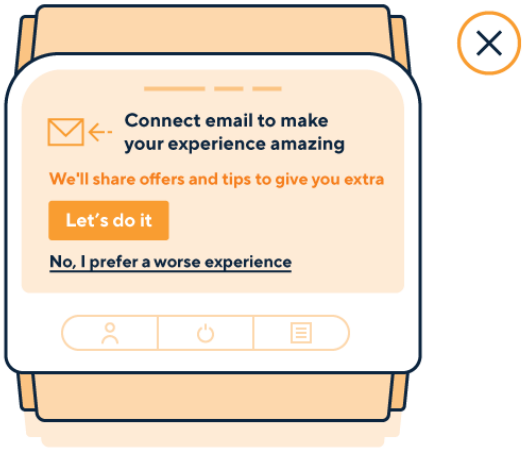
Example

A graphic shows a smartwatch being set up by a user. The user has gone through 12 of the 20 steps of the set-up where they have been asked to make choices about the processing of their personal information. This set-up shows requests for consent in quick succession. The user is unlikely to be able to consider all the requests to provide freely given consent.

Similarly, you **must not** use option labels that invite guilt or another negative emotion. Sometimes known as 'confirmshaming', this can bias people's choices and invalidate their consent.

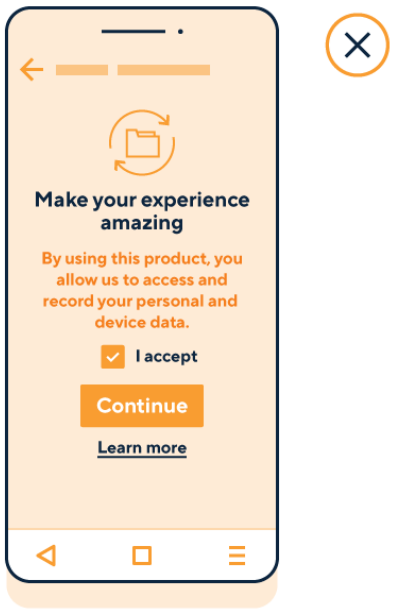
You **must** not use 'biased framing' to emphasise the supposed benefits of one particular option to make it more appealing or the supposed risks of another to discourage people from selecting it.

You must give people the option to refuse and withdraw consent without being penalised.



Example

A graphic shows a smart blood pressure monitor with a digital screen on the product displaying a request to connect user's email using nudging techniques. The blood pressure monitor uses 'confirmshaming' by saying 'Connect email to make your experience amazing' and the option to opt out is labelled as "No, I prefer a worse experience'. The options to opt in and out are displayed using biased framing, making the opt-in option more visible and brighter. The option to opt out is less prominent.



Example

A graphic shows a mobile app making a consent request for the processing of personal information. The consent request uses biased framing, where the option to opt in is more prominent, using brighter colours, and a pre-ticked box saying 'I accept'. The user is presented with a button to continue. It is not clear from the design that they could opt out. There is a link to 'learn more' about the processing of information.

What do you mean by 'specific and informed'?

For consent to be specific and informed, you must tell people about:

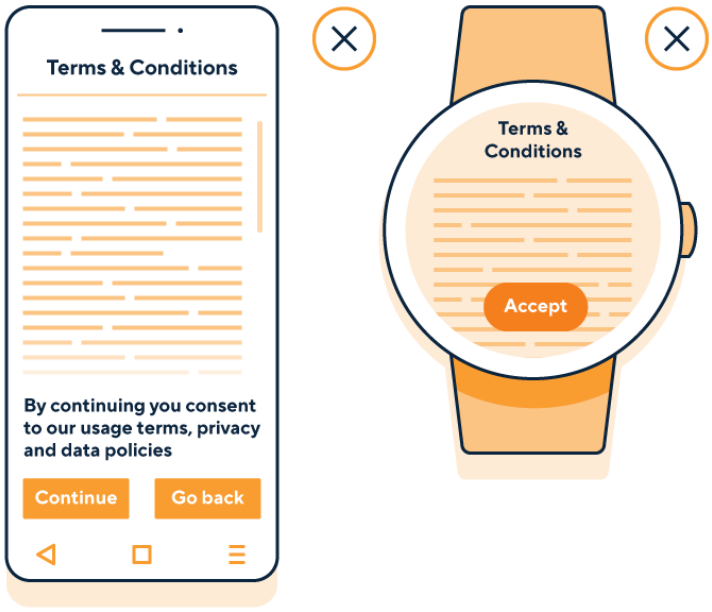
- who you are;
- why you want their personal information;
- what you're going to do with it;
- who you'll share it with; and
- how they can withdraw their consent at any time.

These requirements are separate from your obligations to provide privacy information under the right to be informed.

You must give granular options to consent separately to different purposes.

You must separate consent from terms and conditions. The rules about consent requests are separate from your transparency obligations under the right to be informed, which apply whether or not you are relying on consent.

You should think carefully about when to use consent interfaces. Use too few and you may not comply with UK GDPR requirements. However, overusing unnecessary consent pop-ups will cause decision fatigue, training people to accept information sharing or other uses of their information blindly in every product they encounter.



Example

A graphic shows an outline of a mobile app displaying the bundling of terms and conditions, privacy policy and consent. The graphic includes an indication of a block of text that the user needs to scroll through. The block of indicated text is overlayed with a message saying, 'By continuing you consent to our usage terms, privacy and data policies'. The user is presented with two buttons, one for 'continue' and the other to 'go back'.

Another graphic shows a smartwatch displaying the bundling of terms and conditions and privacy terms on a small screen. There is a single button to 'accept' the conditions without the possibility to decline them.

You must tell the person the controller's identity. This means you need to identify yourself, and also name any third-party controllers who will be relying on the consent.

You must offer people a way to reopen consent interfaces later on. It must be as easy to withdraw consent as it is to give it.

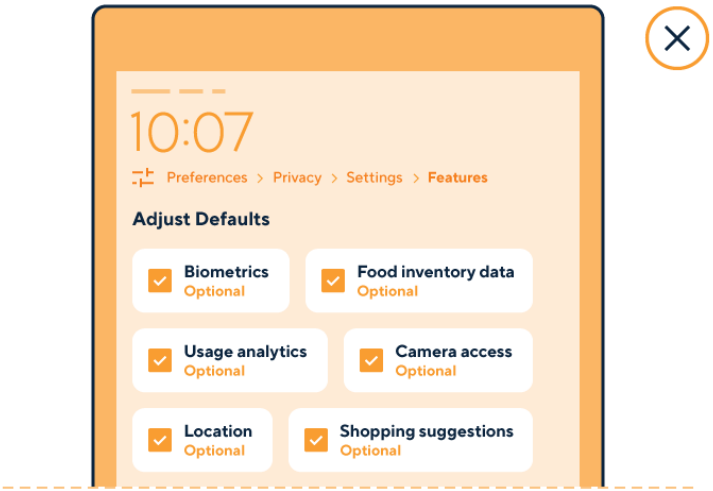
You could provide 'privacy settings' in the product settings where your users could access consent interfaces for different types of processing.

What do you mean by unambiguous indication?

You must ensure that it is obvious that the person has consented, and what they have consented to.

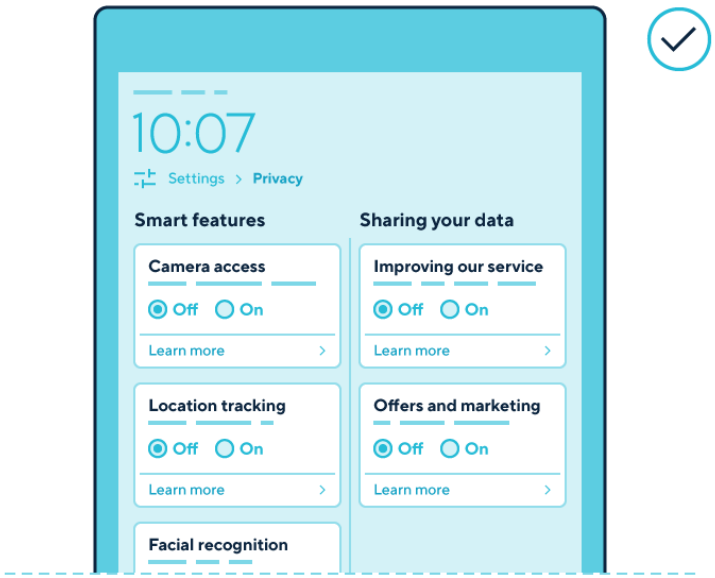
The key point is that you must make all consent opt-in consent (ie a positive action or indication – there is no such thing as 'opt-out consent'). Failure to opt out is not consent as it does not involve a clear affirmative act.

Relying on silence, inactivity, default settings, pre-ticked boxes or your general terms and conditions does not lead to valid consent. Neither does taking advantage of inertia, inattention or default bias in any other way.



Example

A graphic of a screen on a smart fridge shows 'preferences' settings. The privacy settings are hidden on the fourth layer of the settings and aren't named intuitively for users to find them easily. The graphic shows types of personal information the fridge is processing, including biometrics, location, food inventory data, camera access, usage analytics and shopping suggestions. Each data type has been marked as 'optional'. The categories of personal information have been pre-ticked by default to indicate that all this information will be processed.



Example

A graphic of a screen on a smart fridge shows settings for privacy on the second layer of the settings. Privacy settings are logically divided into 'smart features' controls, including camera access, location tracking and facial recognition, and controls for 'sharing your data', including controls for 'improving our service' and 'offers and marketing'. Each control is set to 'off' by default and there is an option to click on 'learn more' for information about what each setting does with personal information.

Relevant provisions in the UK GDPR - see Recital 32

https://www.legislation.gov.uk/eur/2016/679/contents

What is 'explicit consent'?

The UK GDPR does not define explicit consent. In practice, it is not very different from the usual high standard of consent. This is because all consent must involve a specific, informed, freely given and unambiguous indication of the person's wishes.

The key difference is that 'explicit' consent requires a clear statement (whether oral or written).

You must ask users of IoT products for their explicit consent if you are processing their special category data and explicit consent is your chosen condition for processing.

Refer to our guidance on consent for more information about how to phrase explicit consent requests.

Example

A graphic of a smartwatch shows a screen prompting users to finish setting up their data-processing choices in the mobile app. A graphic of a mobile app next to the smartwatch shows a screen where users are asked to provide explicit consent to processing special category health data, including heart rate, for the smartwatch's fitness-tracking function.

When should we ask for consent?

If you are relying on consent as your lawful basis for processing people's information, you must ask for consent when you start your processing. You may choose not to start all your processing at the same time.

If you start processing different types of personal information at different times, you should consider finding the right moments to ask people for consent.

In practice this means you should think about asking for consent at appropriate points in the user journey.

While the set-up of a product is a logical point in the user journey, it is not necessarily the only time to ask for consent. There may be other moments when it will be appropriate to do so. This also means you aren't overloading your users with consent requests all at once and you can make them more specific.

Some of the moments you should consider include:

- during product set-up;
- when the IoT product collects personal information about a new person or when a new account is added;
- when a user enables a new product feature after initial set-up, and the feature requires consent for additional types of information for a new purpose (eg location data, health information);
- if a product update changes how personal information is processed; and
- if a young person becomes old enough to give consent for themselves.

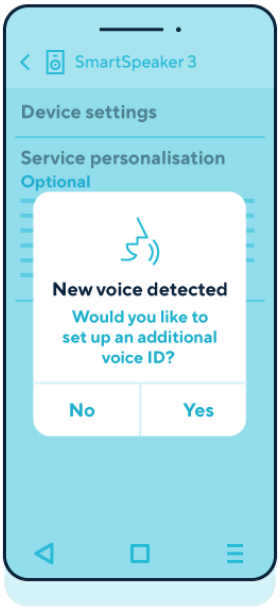
What methods can we use to obtain consent?

Whatever method you use, consent must be an unambiguous indication by clear affirmative action. This means you must ask people to actively opt in. Examples of active opt-in mechanisms include:

- ticking an opt-in box;
- clicking an opt-in button or link online;
- selecting from equally prominent yes or no options;
- choosing technical settings or preference dashboard settings;
- responding to an email requesting consent;
- answering yes to a clear oral consent request; and
- responding to just-in-time notices.

Example

A graphic of a smart speaker shows the speaker using an oral consent request to allow the user to make choices about whether their personal information is processed, offering yes or no answers to the question ‘Can I process your voice data to create a more personalised experience?’



Example

A graphic shows an accompanying mobile app displaying a just-in-time notice saying that a smart speaker has detected a new voice. The app is asking ‘Would you like to set up an additional voice ID?’, offering yes and no answers of equal prominence.

Further reading – ICO guidance

- Consent
- Privacy in the product design lifecycle

How do we ensure people can withdraw consent?

Your users **must** be able to withdraw consent at any time. This means you **must** design your consent mechanism with technical capability for users to withdraw consent as easily as they gave it.

You **must** also tell people how they can withdraw consent in your consent mechanism.

You **should** make any effects of withdrawing consent clear – for example, if people can no longer use certain features of your IoT product if they withdraw consent.

How do we ask for consent from multiple users?

If your IoT product can be used by multiple users, you **must** consider ways to gather consent for processing personal information from them if you've chosen it as your lawful basis.

Gathering consent from multiple users where not everyone has an account for your IoT product may be difficult. You **should** consider giving people the option to create multiple accounts for the same product if this is likely to improve their ability to exercise more control over their personal information.

You **should** consider in which instances you may be able to ask different users for their consent to processing in a meaningful way. This may depend on how you design the hierarchy of multiple users in your product.

If your hierarchy set-up for multiple users relies on a main account holder and an additional account holder – where you expect the main account holder to make most decisions about processing by the IoT product – you **should** make sure you clearly explain to the additional account holder what each account holder can control.

If your set-up for multiple users is designed with a more equal approach to account holders, you **should** make sure you clearly explain what each

account holder can control about processing by the IoT product. You **should** include notifications for all users when you change how their personal information is processed.

When is consent not appropriate?

If for any reason you cannot offer people a genuine choice over how your IoT product processes their personal information, consent is not the appropriate basis for your processing – for example, if you would still process their personal information on a different lawful basis if they refused or withdrew consent.

Consent is also unlikely to be the appropriate lawful basis if you ask for it as a precondition of using your IoT product and its associated app.

Example

A parent buys a children's GPS tracker for their eight-year-old child. The location is core to the service of the tracker, meaning the children's tracker wouldn't be able to function without it.

Asking for consent to process the information about the child's location is not the most appropriate lawful basis because providing this information is a condition of the service. It is more appropriate to use performance of a contract as a lawful basis to process GPS data.

How do we ensure our IoT products process personal information fairly?

Fairness in a data protection context is about how you do the processing as well as its outcome (ie its effect on people).

For processing to be fair, you **must** use information in ways that:

- people would reasonably expect; and
- do not have unjustified adverse effects on them.

Fairness is closely linked to transparency – part of ensuring your processing is fair is explaining to users how you use their information. But it's not just about this. For example, you are unlikely to be treating people fairly if your IoT product collects personal information that's not necessary for its functions.

You **should** regularly review how you use personal information in your IoT products. This can minimise the risk of unfair outcomes for users.

For example, you **could** set up collaborative ways of working between your design, technical, legal and policy teams to ensure there is alignment between the product's features and the personal information you need to collect for it to function properly.

You **could** provide guidance and training to your staff on how to ensure data minimisation in product design and development.

Fairness is also closely linked to necessity, proportionality and purpose limitation.

How does the fairness principle apply when an IoT product uses AI?

It is particularly relevant to consider fairness if your IoT product uses AI – for example, to help you analyse information about people's interactions with the product and any associated service like an app.

This is because AI technologies can be susceptible to bias, which can result in discriminatory outcomes.

You **must** ensure your IoT products perform accurately and produce unbiased, consistent outcomes.

Example

A fitness tracker manufacturer develops an AI system that calculates users' health and fitness levels. It will use the AI system to suggest personalised exercise and nutrition plans to the users.

The manufacturer trains the AI system on a large dataset that includes height, weight, activity levels, body mass index and fat composition.

In testing, the manufacturer finds that the AI system gives women lower fitness scores because of their naturally higher healthy body fat composition than men.

In this case, the AI system puts a certain group (women) at a disadvantage, which seems discriminatory.

There are many reasons why the system might give women a lower score. In this case, the probable reason is imbalanced training data with more men than women.

You **must** ensure that any AI technologies you involve in your IoT products are sufficiently statistically accurate and avoid discrimination. You **should** conduct regular checks of your systems for accuracy and bias.

For more resources on how to identify risks to fairness in AI and how to mitigate them, see our guidance on fairness in AI.

Further reading – ICO guidance

- Principle (a): Lawfulness, fairness and transparency
- How do we ensure fairness in AI?
- Annex A: Fairness in the AI lifecycle

How should we tell people what we're doing?

In detail

You **must** inform people that you intend to process their personal information.

Being transparent about your use of people's personal information is closely linked to fairness. Your processing is unlikely to be fair if you do not give people information about it.

Regardless of the type of IoT product you use in your processing, you **must** tell users:

- why you are using their personal information;
- what lawful basis you are using for processing;
- what types of personal information you are using;
- what decisions you are making with the information and how it affects their use of your service;
- whether you keep personal information used or generated by your systems and for how long;
- whether and in what circumstances you share their personal information with other organisations; and
- how they can exercise their data protection rights.

You **must** provide privacy information to people at the time you collect their personal information from them. You **could** also give people privacy information ahead of time when you start your processing.

If your IoT product is aimed at children or likely to be accessed by them, you **must** ensure that the privacy information you give them – and other published terms, policies and community standards – is concise, prominent

and in clear language suited to their age. You **should** provide additional specific 'bite-sized' explanations about how you use personal information at the point that use is activated.

How do we ensure our processing by IoT products is transparent?

When deciding how to comply with the transparency principle, you should consider:

- the most appropriate formats to deliver privacy information;
- the accessibility of your language;
- appropriate moments in a person's user journey;
- different interfaces where people could receive privacy information; and
- who are the product users (eg a single user vs multiple users, adults or children).

You **must** separate privacy information from terms and conditions, as well as any requests for consent to process personal information. You **must not** include a tick box to indicate consent with your privacy information.

You **should** make sure that privacy information is specific and relevant to an IoT product and the processing it does. You **must** provide privacy information for all its processing.

Example

A digital company manufactures and sells IoT products as well as operating an online video streaming service and email service.

The transparency information it provides for its IoT products is different to that of its two other services because the personal information it processes is different. Its IoT products process information from the product sensors that includes, for example, health and biometric information. Therefore, the company has three different sets of transparency information for its users, specific to each service.

You **should** make it easy for people to find privacy information again once they have set up the device.

For example, you **could** provide access to privacy information in the product's settings or in a privacy dashboard – a dedicated section where people can manage what's happening to their personal information.

How do we decide the right methods for providing our privacy information?

When deciding how to provide privacy information, you **should** consider how people will interact with your IoT product and the wider context of its use. This will help you work out the most effective way of informing them.

Privacy notices are a useful way to communicate privacy information but may not be the most appropriate for all instances in the context of IoT. Where appropriate, you **should** consider other techniques alongside a notice. This will help you demonstrate you've taken steps to communicate privacy information in ways that people are likely to notice and use.

You **should** use various techniques such as 'just-in-time' (JIT) notices or a layered approach, where appropriate.

You **could** provide a dedicated privacy and security hub where people can find privacy information.

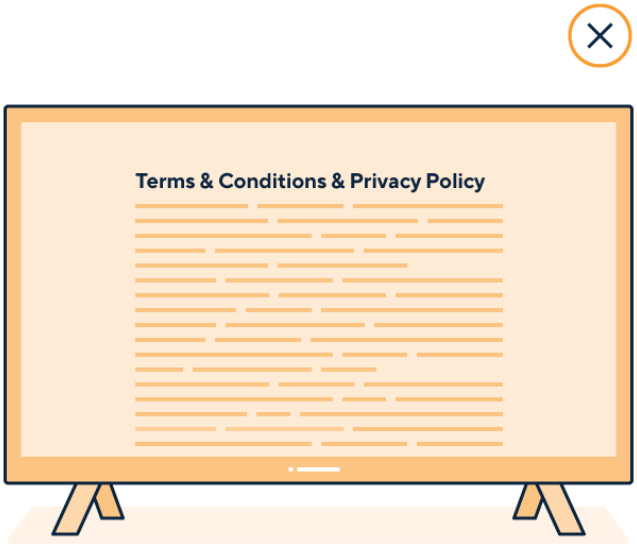
But you **should** be careful not to overload them with information. You **should** consider if people are likely to read what you provide and the circumstances in which they do so. You **could** have a concise transparency information resource, for example as part of the JIT notice, and refer users to the privacy hub if they want more information.

How do we make our privacy information easy to follow?

You **should** design your privacy information in a way that enables people to understand what happens to their personal information. This helps you demonstrate your compliance with the UK GDPR's transparency principle and people's right to be informed.

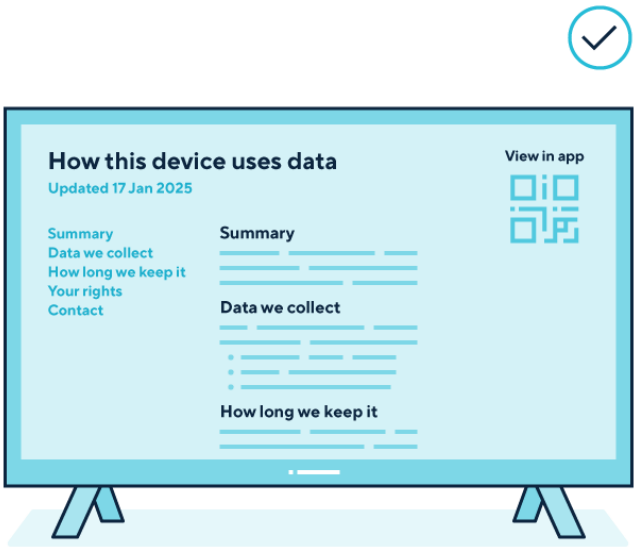
Privacy information should be easy to read and understand. You **must** make it concise, transparent, intelligible and easily accessible, using clear and plain language.

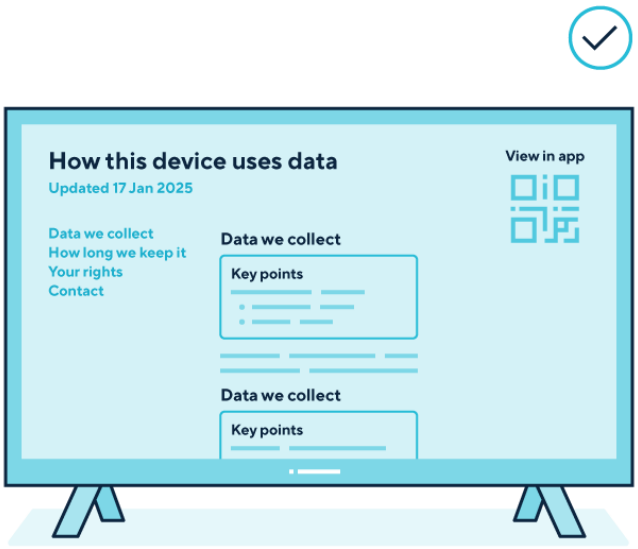
Where appropriate, you **should** use navigation panels, collapsible lists, bullet points, large text, pictures, diagrams and videos to deliver your privacy information.



Example

A graphic shows a smart TV displaying a privacy policy and terms and conditions. It bundles them in a large block of text without headings or navigational aids.





Example

Two examples of smart TVs show on-screen privacy information. The first shows privacy information with a navigation panel for different sections of the document and a clear heading for each section. It provides a short summary at the top.

The second shows privacy information with a navigation panel for different sections of the document and a clear heading for each section. Each section contains a text box with key points for users to take away.

Both examples contain a QR code so users can scan and view the privacy information on their mobile if preferred.

What are the right moments for us to provide privacy information?

Timing is important. You **should** identify the moments when people might expect to make decisions about their personal information, and when they might be ready to make reasonable, informed choices.

Consider when in the user journey you should discuss privacy. You **must** provide privacy information at the time of collecting personal information from the person it relates to, but you **should** consider other moments too.

You **could** consider providing privacy information at the different moments in the user journey. For example, when a user:

- visits a product website;
- downloads an accompanying app from an app store;
- sets up a product for the first time;
- creates or adds user accounts;
- receives a security update that changes how you process their personal information;
- receives a product update that changes how you process their personal information (eg launching a new feature);
- enables a product feature themselves; and
- has their personal information collected by the product.

Often, your IoT product may start processing people's personal information:

- during set-up (eg if the user gives you personal information as part of this process); or
- once set-up is complete and the product starts working.

You **should** provide privacy information at least at these moments in the user journey.

However, in some instances, users will not turn on all the features of the product at this time or you add new features that are not covered by the transparency information they've already interacted with. This means you might only start certain types of processing later.

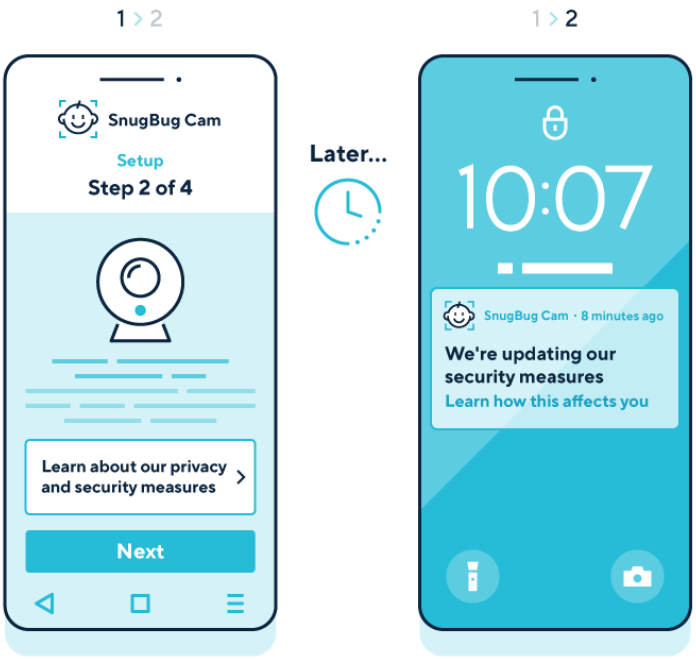
You **should** consider how to provide transparency information then. For example, you could use a just-in-time notice or refer people to your privacy policy.

Example

A design team at a smart security camera manufacturer must ensure they explain what happens to people's information. They are considering at what moments during the user journey they start processing users' information. They identify that the smart security camera can start processing different personal information at different times.

For example, the smart camera processes some information as soon as the product is set up, but it would only start processing biometric information from facial recognition if the user turned it on. Users can turn on this feature any time, not just at the product set-up.

The design team decide to provide transparency information in the step-by-step instructions during initial account sign-up, and to deploy 'just in time' notice when users turn on additional features, including facial recognition.



Example

A graphic shows the set-up of a smart baby monitor. The users were shown a link to more information about the product's privacy and security measures, which they could choose to interact with. A few weeks later, the baby monitor is due a security update that will change how some of the users' personal information is processed. The users receive a notification on their mobile phone about the security update. They can navigate to a page that explains the changes.

The right moments may vary for different people with different needs.

Whatever moments you choose, you **should** ensure people have enough time and knowledge to consider the information fully.

How do we provide privacy information on different product interfaces?

When you think about how to provide privacy information, you **should** consider how your users interact with your IoT product.

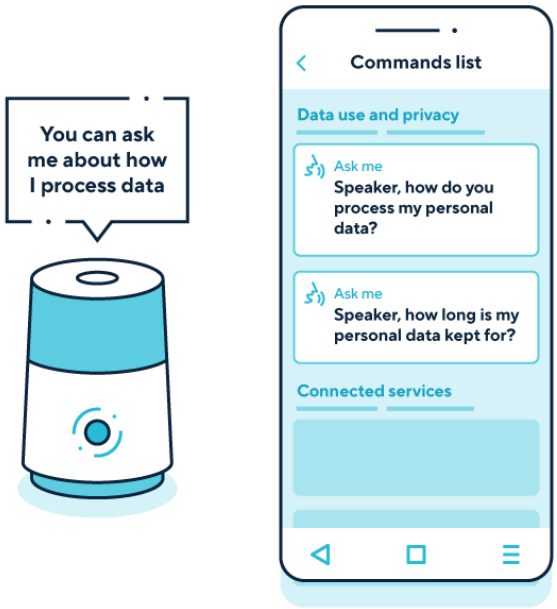
This is particularly relevant for IoT products that have different types of interface. For example:

- Will your users interact with your product through a display?
- Does your product involve the use of an associated mobile app?

IoT products can have different types of interface. They include small and large screens, voice and sound interface, light controls, mobile or app interface, or a web browser interface.

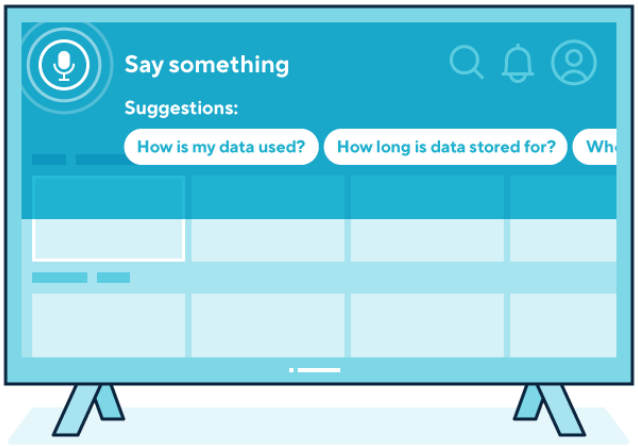
You **should** plan for what privacy information you can make directly available on the IoT product and what information you will make available on a mobile app (if there is one) or through an account accessed through a web browser.

Some devices have a prominent voice interface and a far less prominent display interface. You **could** consider making privacy information available through the voice interface.



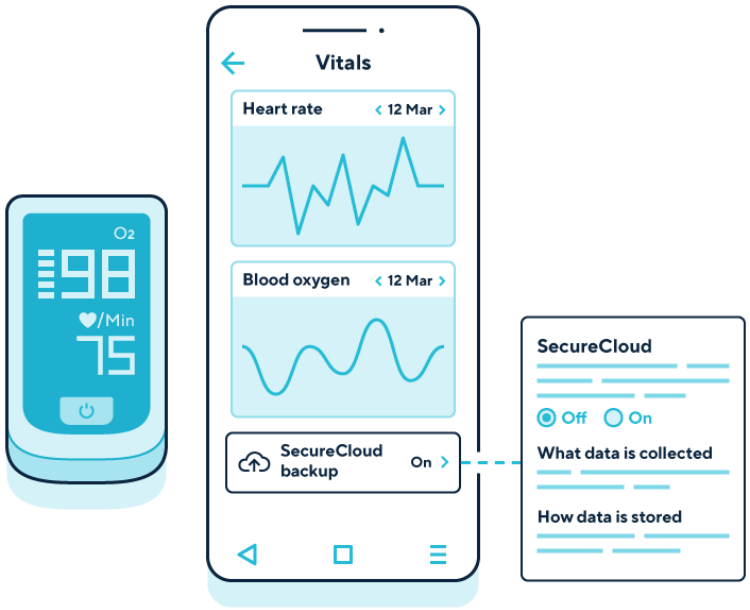
Example

A graphic shows a smart speaker answering users' questions about how their personal information is processed via its voice interface.



Example

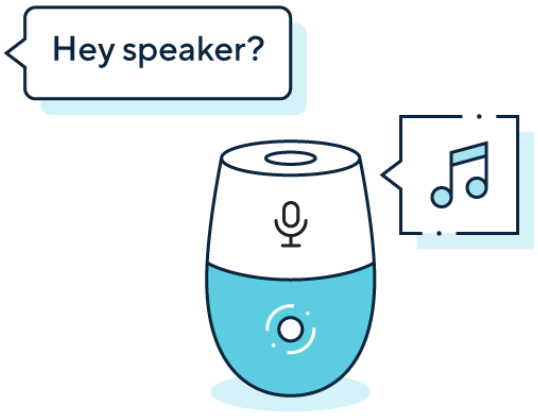
Two graphics show smart TVs using a smart assistant's voice interface to provide privacy information about how users' personal information is processed.



Example

A graphic shows a smart oximeter and its accompanying app displaying privacy information about the cloud back-up setting being on. After users click on the cloud setting, they are presented with more information about what data is collected and stored on the cloud. The oximeter doesn't have an on-device screen that would allow it to show information in this way.

Some IoT products have prominent light controls and sound interfaces. You **could** use these methods to signal to your users when IoT products are on and processing personal information.



Example

A graphic shows a smart speaker making a sound when it starts ‘listening’ after being prompted by a user.

Example

A graphic shows a smart security camera indicating a camera light being on when recording video footage.

How do we provide privacy information if there are multiple users?

An IoT product can often be used by multiple people. Whether you intentionally design your product for use by multiple users or not, you **must** ensure all potential users whose information you will process are given privacy information.

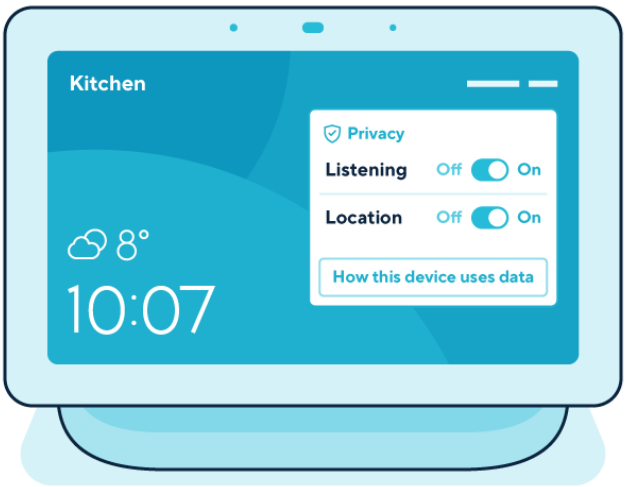
This may be difficult if users don't have their own account. You **should** consider giving people the option of having multiple accounts for a product if this is likely to improve their experience and access to transparency information.

If you are giving users multiple accounts, you **should** make sure transparency information is easy to find for everyone that has an account, not just the primary account holder.

In situations where users don't have their own account or don't want to create one, you **should** find other ways of giving them transparency information.

This **could** include providing privacy information:

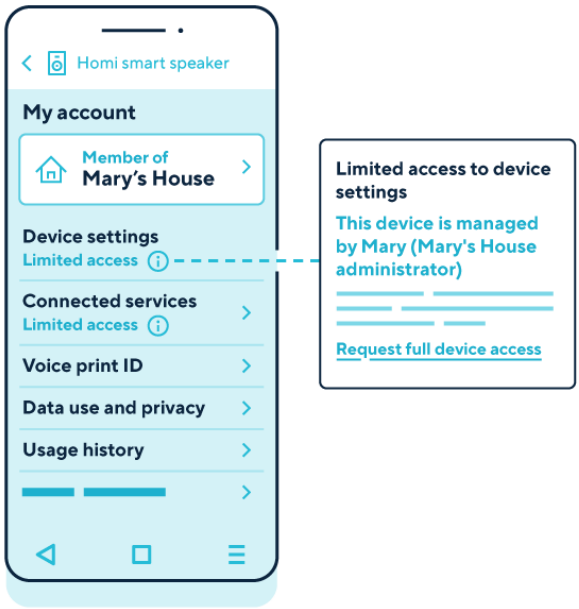
- on the accompanying app's app store page;
- directly through the product's interface, such as screen or a speaker; or
- on any product listing, prominently next to the product description.



Example

A graphic of a smart home hub shows a dashboard with privacy settings allowing any user, registered or unregistered, to manage controls for

sharing certain personal information, including location and whether the home hub's voice assistant is listening. Any user can access transparency information about how the home hub uses personal information.



Example

A graphic shows a smart speaker's accompanying app indicating what product controls are available to an additional user. The additional user is made aware they have limited access to change device settings or to make decisions about what connected services they can control. They can manage their voice ID and view their usage history. They can also view information about how the smart speakers use personal information and privacy.

Further reading

- Principle (a): Lawfulness, fairness and transparency

- Accountability framework – transparency
- Children’s code – see standard 4 for how to provide information in an accessible and easy-to-understand way
- Right to be informed

How do we ensure accuracy in IoT?

The accuracy principle in data protection law means you **must:**

- take all reasonable steps to ensure the personal information you process through your IoT product is not incorrect or misleading about any matter of fact;
- keep the personal information up-to-date, if necessary; and
- consider how you will respond to any challenges from users about the accuracy of the information you've gathered through your IoT product.

In practice this means you **must** take reasonable steps to design your IoT product so that the information it processes is accurate. If the technology – such as sensors – that your IoT product relies on to process personal information is inaccurate, such as sensors, you will probably not be able to meet the requirements of the accuracy principle.

The accuracy principle is also linked to the security principle. The accuracy of the personal information is important for the integrity of your systems and processes.

The accuracy principle applies to the processing of all personal information, including biometric data and information processed by AI systems.

Some IoT products use biometric recognition systems, for example:

- to authenticate users through their fingerprint;
- to identify people through a security or a doorbell camera; or
- to match a query on a voice assistant to a household member.

They can also use AI systems, for example to draw inferences about people based on their health and wellbeing information from fitness trackers or other wellness devices.

Biometric recognition and AI systems may involve the processing of personal information, so the accuracy principle applies. But they don't need to be 100% statistically accurate to comply with it.

The outcomes of your biometric recognition or AI system are statistically informed guesses about someone's identity or something that might be true about a person now or in the future.

To avoid these outcomes being misinterpreted as factual, you **should** ensure your records indicate they are statistically informed guesses rather than facts.

At the same time, you **must** ensure your system is sufficiently statistically accurate for your purposes. This doesn't mean every single outcome has to be correct, but you **must** factor in the possibility of errors and their possible effect on your decision-making and the people it applies to. If you don't do this, your processing may not comply with the fairness principle.

Further reading – ICO guidance

- Principle (d): Accuracy
- What do we need to know about accuracy and statistical accuracy?
- How does the accuracy principle apply to biometric data?

How long should we keep personal information for?

You **must not** keep personal information obtained from processing on your IoT product for longer than you need it. There are no set time limits in data protection law because it depends on your situation and your purposes for processing the information.

You **must not** hold personal information indefinitely, 'just in case' it might be useful in the future.

Example

A company manufactures and sells smart speakers. It needs to process user queries to the voice assistant embedded in the speaker. User queries are personal information. The company uses the queries to train its AI systems to improve its technology. It previously identified the right lawful basis to do this.

It doesn't keep user queries indefinitely. Once users close their account, it deletes their relevant information. It also provides an option for users to delete their recordings periodically – weekly, monthly or yearly.

If your IoT product or service involves data sharing with other organisations, you **should** agree among you what happens when you no longer need to share the data.

You **should** review your retention periods regularly, and erase or anonymise personal information when you no longer need it for the purpose for which it was obtained and processed.

You may also have to follow other laws that say how long you need to keep certain information.

Further reading

- Principle (b): Purpose limitation
- Principle (e): Storage limitation

How do we ensure security of personal information in IoT?

In detail

You **must** process personal information in a way that ensures appropriate security and protection against unauthorised or unlawful processing (among other things).

This means you **must** apply appropriate security measures to your IoT products and services when you process personal information. This includes both technical measures for your product and ensuring you have appropriate organisational measures in place.

You **should** determine what these measures are by carrying out a risk analysis that considers:

- the circumstances of your processing and the likely security threats you may face;
- the harm that may arise if the personal information is compromised; and
- what forms of attack your product and its associated services may be vulnerable to.

What's 'appropriate' is likely to differ depending on the type of IoT product, its functions, and the nature of the personal information you process.

For example, different measures may be needed for things like:

- special category information (eg biometric and health data);
- information of a highly personal nature to your users (eg home automation products that could build up a detailed picture of their private lives); and
- personal information about children.

The security risk profile of your IoT product may be affected by whether the processing happens on the device or elsewhere, for example on external

servers. Processing on the IoT product may need different security measures in place than when the processing occurs in the cloud.

You should also consider situations where your users' safety may depend on the security of your IoT product. For instance, a smart lock with compromised security could be a threat to your users' physical safety.

What measures do we need to consider?

Your risk assessment will indicate what measures may be appropriate. Beyond this, industry standards for IoT may help you define appropriate security measures for your IoT product.

Your IoT product may be subject to other legal requirements specified in separate legislation. One example is the Product and Telecommunications Infrastructure Regulations 2024 (PSTI Regulations). These apply to manufacturers of connectable products like IoT devices, and have specific obligations about:

- passwords;
- vulnerability disclosures; and
- minimum security update periods.

In such instances, these requirements are additional and separate to the data protection requirements specified in the UK GDPR. While they don't automatically equate to compliance with the security principle, they nevertheless may comprise appropriate measures that we would expect in the security context. Where the PSTI Regulations do apply, we may take their requirements into account if there is a security incident.

You may consider the following measures, depending on your circumstances.

Passwords

While passwords are a common security measure, you should consider whether they are appropriate for your particular circumstances.

Passwords carry well-known risks. More complex passwords are known to be more secure – but only if they are unique. However, there is a risk that if you require over-complex passwords, people will bypass the security measure and write them down or repeatedly request to reset their password.

If you choose to use passwords for your IoT products, you must ensure you have a policy in place to govern how you set them up. You should also enforce an appropriate level of complexity and prevent the use of common, easily guessed passwords. This will help you avoid allowing your users to set weak or already compromised passwords.

If the PSTI Regulations apply to you, your passwords have to be:

- unique per product; or
- defined by the user.

You **could** consider alternative ways of authenticating, such as passkeys and biometric verification. These may provide a more seamless experience for users while still providing security.

Multifactor authentication

You may need to authenticate users of your IoT product to ensure it is protected against unauthorised access. You **should** implement multifactor authentication wherever it is possible to do so.

Multifactor authentication provides another layer of security for your IoT products. Using a password only, even a strong one, may not provide sufficient security against more sophisticated attacks. Many IoT products lack interfaces that would allow users to login to them directly and may need other types of evidence to authenticate the user.

Security updates

You **must** provide regular security updates for your IoT products. Where possible, you **should** enable your IoT product to operate during a security update. You **should** make clear how security updates can be installed – whether this is automatically over-the-air or manually.

If an IoT product can’t be automatically updated, you **must** give users the option to update it manually. If it’s not possible to update the product automatically or manually, you **should** inform users that they should remove the IoT product from the network.

Remember, you **must** ensure that the measure you take provide the ongoing security of your IoT product and any associated systems and services throughout its envisaged lifecycle.

You **should** tell your users how long you will provide security updates. Remember, if the PSTI Regulations apply to you, you have to provide this information.

Vulnerability disclosure policy

You **should** have a vulnerability disclosure policy and make it publicly available. You **should** include contact information in the policy so your users can report issues. You **could** also include basic information about any timelines for initial acknowledgement of any reports and how you will provide status updates until you resolve the reported issue.

Again, if you have to comply with the PSTI Regulations, having a vulnerability disclosure policy is a legal requirement for you.

Software integrity

You **should** verify the IoT product's software using secure boot mechanisms. This is so that if an unauthorised change is detected to the software, the device alerts the user and does not connect to wider networks except those needed to perform the alerting function.

Monitoring

You **could** also monitor your IoT products and services for any security anomalies or flaws – for example, telemetry information that can allow you to identify unusual circumstances early and deal with them. This minimises security risk and allows you to resolve problems quickly.

If you collect information for this purpose, you **must** do so fairly, lawfully and transparently. You **must** also pay particular attention to the principles of purpose limitation and data minimisation. For example, only collect the minimum information you need and only use it for security purposes.

To maintain security of personal information throughout the whole IoT product lifecycle, you **should** have tools and processes in place to enable the deletion of personal information.

Encryption

The UK GDPR includes encryption as an example of an appropriate technical measure. It is a well-established and widely deployed technology that you can implement relatively easily.

So, you **should** assess the points in your IoT product's lifecycle where encryption may mitigate any risks your processing poses.

It's likely that your product will both store and transfer personal information, and you **should** implement encryption in both cases.

When evaluating whether encryption can mitigate any risks you identify, you **should** consider:

- the sensitivity of the information you are processing – if your IoT product processes special category information or things like location data, your risk profile may be higher;
- the harms that may arise if personal information is subject to unlawful or unauthorised access;
- the data flows in your IoT product's overall ecosystem; and
- where this personal information will be stored (eg on the IoT product or in the cloud).

You **should** ensure that your IoT product supports secure firmware updates to patch vulnerabilities and update encryption algorithms as needed.

For products that you no longer provide updates for, you **should** ensure that the product's intended lifetime does not exceed the recommended usage lifetime of the cryptographic algorithms it uses.

Examples of personal information in IoT products that may benefit from encryption include:

- authentication information (eg passwords, encryption keys);
- device identifiers;
- names, addresses, timestamped location data, phone numbers, and email addresses;
- payment details where present;
- biometric data (eg voice recordings, facial recognition data, and fingerprints);
- data collected from smart health devices like smart scales or fitness trackers;
- recordings and video streams (eg from smart security cameras or voice assistants); and
- content of any communications data.

You **should** also be aware of any industry or sector-specific guidance or advice that includes content about encryption. While following these may not

specifically guarantee UK GDPR compliance, we may take them into account in the event of any incident.

Example

ETSI standard TS 303-645 on consumer IoT devices contains a number of security-related provisions that reference encryption. These include the use of:

- best-practice cryptography to communicate securely;
- reviewed or evaluated security functionalities;
- updateable cryptographic algorithms;
- device authentication requirements; and
- in-transit encryption.

Read our guidance on encryption for more detail.

Further reading

- Principle (f): Integrity and confidentiality (security)
- A guide to data security
- Data protection by design and by default
- Encryption
- Passwords in online services
- Security outcomes

Other resources

- Product Security and Telecommunications Infrastructure Act
- ETSI Standard EN 303 645 on cybersecurity baseline requirements for consumer IoT
- NCSC guidance on protecting data at rest and in transit
- Introduction to ISO 27400:2022 family of standards on IoT security and privacy
- ISO 31700-1:2023 - Consumer protection — Privacy by design for consumer goods and services — Part 1: High-level requirements

- ISO/TR 31700-2:2023 – Consumer protection — Privacy by design for consumer goods and services — Part 2: Use cases
- NIST IoT device cybersecurity capability core baseline

Can PETs help us with our data protection compliance?

Yes. You **should** consider using privacy-enhancing technologies (PETS) in your IoT product, as these can help you demonstrate compliance with the security principle.

But you **must** still:

- have appropriate organisational measures in place to keep information secure, such as regular testing; and
- review your security measures to ensure they remain effective.

PETs can help you meet other data protection obligations too, like the requirements around data protection by design and by default. For example, PETs that limit the amount of personal information you process can help you demonstrate compliance with the data minimisation principle.

The table below provides a list of PETs, along with the risks they may mitigate for IoT applications. It also shows suitable and unsuitable use cases for IoT.

PET	Description	Suitable IoT processing activities	Unsuitable IoT processing activities
Differential privacy	A statistical technique that ensures the privacy of people in a dataset by adding noise to the data. Useful for allowing databases to be queried without releasing information about people and to comply with the purpose limitation principle.	Statistical data analysis, data sharing. Suitable for applications where aggregate data is used.	Real-time decision-making processes. Use on IoT products with limited processing power, memory, battery life, weak wireless range or similar. Noise addition can reduce the accuracy for real-time decision-

			making.
Secure multiparty computation	A cryptographic method allowing parties to jointly compute a function over their inputs while keeping those inputs private. Useful for compliance with data minimisation requirements and the security principle.	Collaborative data analysis, cross-organisational computation. Ideal for scenarios requiring collaboration without exposing individual data.	Applications requiring fast processing speeds. Use on IoT products with limited processing power, memory, battery life, weak wireless range or similar. Not suitable for time-sensitive processes due to computational intensity.
Zero knowledge proofs	A cryptographic method by which one party can prove to another that a statement is true, without conveying any additional information apart from the fact that it's true. Useful for compliance with data minimisation requirements and the security principle.	Identity verification, access control. Best for scenarios where verification without data exposure is critical.	High-volume or low-latency data exchanges. Use on IoT products with limited processing power, memory, battery life, weak wireless range or similar. Not efficient for high-volume data due to computational intensity.
Federated learning	A machine-learning approach where a model is trained across multiple decentralised devices holding local data samples, without exchanging them. Useful for compliance	Predictive modelling, privacy-preserving analytics. Suitable for decentralised data	Scenarios requiring immediate data centralisation. Use on IoT products with limited processing power, memory, battery life, weak

	with data minimisation requirements and the security principle (when combined with other PETs).	environments.	wireless range or similar. Not ideal where real-time, centralised data analysis is needed.
Synthetic data	Artificially generated data that mimics the statistical properties of real datasets. Useful for compliance with data minimisation requirements and the purpose limitation principle.	Testing and development, training AI models. Useful for situations where real data is sensitive or not available.	Applications requiring precise, real-world data accuracy. Not suitable where high fidelity to actual data is critical.
Homomorphic encryption	A form of encryption allowing computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of operations performed on the plain text. Useful for compliance with the principles of accuracy and security.	Secure data processing, encrypted data analysis. Ideal for secure data processing.	Scenarios requiring low computational overhead. Use on IoT products with limited processing power, memory, battery life, weak wireless range or similar. Not practical for use cases with limited computational resources due to its high processing demand.
Trusted execution environment	A secure area of a main processor. It guarantees code and data loaded inside to be protected for confidentiality and integrity. Useful for compliance	Secure data processing, IoT device security. Excellent for securing sensitive operations on IoT devices.	General-purpose computing environments. Adds considerable cost to lightweight IoT devices. Not suitable for applications not

	with the accountability and security principle.		requiring hardware-based security measures.

Further reading

Privacy-enhancing technologies (PETs)

How do we help people exercise their rights?

In detail

The UK GDPR gives people various rights about their personal information. You **must** help people exercise these rights. This includes people who are registered or unregistered users of your IoT products and services and whose personal information you process.

You **should** consider how you can do this in the easiest and most appropriate way for them – for example, directly through your IoT product, through its accompanying mobile app, or through any online account they use.

You **should** pay particular attention to this if your IoT product is aimed at children or likely to be accessed by them. You **should** provide prominent and accessible tools to help children exercise their data protection rights and report concerns.

Further reading

Individual rights

Our guidance on privacy in the product design lifecycle contains more information on empowering people to exercise their rights through interfaces.

What is the right of access?

The right of access allows people to see what information you collect and share about them. It allows people to submit a subject access request (SAR) and receive a copy of the personal information you process.

You **should** consider how to give people access to their information where they might expect it. This could be directly on the IoT product, in its accompanying mobile app or in the user's online account.

You **should:**

- avoid making this process unnecessarily cumbersome; and
- consider where your users are most likely to look for tools allowing them to access their personal information.

Example

An IoT product is designed to be used with an accompanying mobile app. Users can also create an online account by using their browser, eg on a desktop PC or on their mobile device.

In these cases, a user may find it logical to look for ways to make a subject access request (SAR) in the mobile app's settings as this is where they will usually interact with the product's features.

The organisation also enables users to make a SAR by logging into the online account via their browser.

A different organisation makes a similar product with the same sort of online functionality. However, it enables users to make a SAR only through the online account and not the mobile app. This is not good practice because it artificially limits how people can exercise their rights, and doesn't take account of how they normally use the product.

Personal information obtained through an IoT product can relate to more than one person. Therefore, responding to a user's request to access information may involve providing information that relates to both the requester and another person.

You **should** consider whether it is possible to comply with the request without revealing information that relates to and identifies another person.

You may delete from your response parts of the information that would identify the other person.

If you cannot delete the information about the other person, then to comply with the request you **could** try to ask the person for their consent if they are known to you. Alternatively, in some situations it may be reasonable to disclose the information about them anyway. You **should** refer to our guidance on right of access for when this might be the case.

Example

When there are multiple accounts for the same IoT product and you respond to a subject access request, some of the information you could give will probably relate to other people who have accounts for the product as well as the requester.

Since they have their accounts with your product, and are probably known to each other, you should have the means to contact them and ask for consent.

Further reading

Right of access

What is the right to rectification?

People have the right to ask you to rectify any inaccurate personal information you hold about them. They may also be able to have incomplete personal information completed, although this depends on the purposes of the processing.

Rectification requests may result from a subject access request.

If you receive a rectification request, you **must** satisfy yourself about whether the information you hold is accurate and consider what steps you have taken to assure yourself of this. If the information is not accurate, you **should** take steps to rectify it within one month of receiving the request.

You **should** consider how you may be able to give people tools to amend or update their personal information themselves through their IoT product.

Further reading

Right to rectification

What is the right to erasure?

People have the right to have personal information erased. This is also known as the 'right to be forgotten'.

This right is not absolute. You **should** refer to our guidance for details about when the right to erasure does not apply.

If you have disclosed the personal information to others, you **must** contact each recipient and inform them of the erasure request, unless this proves impossible or involves disproportionate effort.

You **should** provide settings for erasure of personal information in the most appropriate and logical way to the user – for example, in the same way you collected their information in the first place, if appropriate.

You **could** offer settings directly in your IoT product, its accompanying mobile app or web account where people can ask you to delete their personal information.

You **must** be absolutely clear with people as to what will happen to their personal information when you fulfil their erasure request, including in respect of back-up systems. You **must** also communicate their erasure request to any organisation you have shared personal information with.

If you use the 'settings' function within the IoT product to allow people to make an erasure request, you **must** clearly explain that their request will delete their account or delete all their personal information (including from your back-ups), or both.

You **should** remind people that simply deleting your IoT product's mobile app will not necessarily delete their information.

You **could** implement more granular options to allow people to delete certain types of personal information.

Read our guidance on the right to erasure for more information about when it applies and what it requires.

Further reading

- Right to erasure
- Principle (c): Data minimisation

What is the right to data portability?

The right to data portability applies to any personal information someone gives you where:

- your lawful basis for processing is either consent or contract; and
- you are carrying out the processing by automated means.

People using IoT products may wish to move their personal information from one IoT product (or an online service) to another IoT product. They have the right to receive this personal information.

In practice, people can ask you to transmit their personal information to another IoT product manufactured by you or to a different organisation.

You **must** transmit the personal information if it is technically feasible.

The right doesn't apply to personal information that you create based on what someone has given you.

Further reading

Right to data portability

What is the right to object?

People have the right to object to the processing of their personal information at any time. This allows them to stop (or prevent) you processing their personal information.

The right only applies in certain circumstances. Whether it applies depends on your purposes for processing and your lawful basis for processing. For example, it will apply where the lawful basis is legitimate interests, but it won't apply if you rely on consent.

But people have the absolute right to object to the processing of their personal data if it is for direct marketing purposes. This includes online advertising that involves personal data processing. In this context, there are no exemptions or grounds for you to refuse.

In practice, this means you **must** inform people about how to object to targeted online advertising. You **could** implement a setting on your product or its mobile app where your users can express their objection.

Read our guidance for information about what an objection request might look like and when you are obliged to fulfil the request.

Further reading

Right to object

What is automated decision-making and profiling?

What is profiling?

Profiling analyses aspects of a person's personality, behaviour, interests and habits to make predictions or decisions about them. Profiling may use algorithms.

Organisations use profiling to:

- find out something about people's preferences;
- predict their behaviour; and
- make decisions about them.

Your IoT product is likely to involve profiling if it uses personal information for purposes such as personalising the user experience. For example:

- a fitness tracker may process users' weight, height and physical activity levels to make predictions about how long it may take them to lose a certain amount of weight;
- IoT products with sleep-tracking functionality process information about people's sleep patterns and possible sleep deprivation;
- a smart TV may use information about users' viewing habits to enable targeted advertising

- a virtual assistant on a smart speaker may tailor its responses to users' queries based on their location;
- smart doorbells may track visitor patterns to record and analyse the frequency and timing of visitors to identify regular visitors and unusual activity;
- a home hub may learn daily routines to automate home settings, such as adjusting the thermostat when users wake up or go to bed; and
- smart domestic appliances such as washing machines or refrigerators may keep track of their usage patterns and use this information to suggest maintenance schedules and energy-saving tips.

Automated decision-making

Automated decision-making is the process of making decisions by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Automated decision-making often involves profiling but does not have to.

Relevant provisions in the UK GDPR - see Articles 4(4), 22(1), (2) and Recital 71

https://www.legislation.gov.uk/eur/2016/679/contents

What are the rules for profiling and automated decision-making?

The UK GDPR gives people the right not to be subject to **solely** automated decisions, including profiling, which have a **legal or similarly significant effect** on them.

'Solely' means a decision-making process that is totally automated and excludes any human influence on the outcome. A process isn't solely automated if someone weighs up and interprets the result of an automated decision before applying it to a person.

If you are unsure whether a decision has a similarly significant effect on someone, you should consider the extent to which it might impact their rights and freedoms or affect, for example, their:

- financial circumstances;
- health;
- reputation;
- employment opportunities;
- behaviour; or

- choices.

While many IoT products may involve automated decision-making, their decisions do not necessarily have a legal or similarly significant effect. A DPIA can help you decide whether or not the intended processing is going to be subject to Article 22.

Example

A smartwatch records people's physical activity, including the types of activity and their health metrics. It uses this personal information to make recommendations for exercising programmes to improve their fitness.

The decision about what exercising programmes to show the user is unlikely to significantly affect them. All it does is show them programmes based on their past activity metrics.

However, decisions may have significant effects if your IoT product performs them for other purposes.

Example

A smartwatch records people's physical activity. An insurance provider provides fitness trackers as part of its insurance products and uses the personal information to determine people's health insurance premiums. Users who have higher levels of activity receive lower premiums than those who don't.

This type of decision is more likely to significantly affect particular users, as it may impact their financial circumstances, health, behaviour or choices.

If you want to use automated decision-making, including profiling, you **must** ensure your processing is covered by one of the exceptions in Article 22(2):

- the decision is necessary for a contract;
- the decision is authorised by law; or

- the decision is based on the person's explicit consent.

Remember, people can also object to any profiling you do. As part of compliance with the right to object, you **must** bring this to people's attention and present it separately from other information.

If your product is aimed at children or likely to be used by children, you **should** switch processing options that use profiling to **off by default**. 'Off by default' does not mean profiling is impossible or banned. By following the safeguards and steps in the code's standard, your profiling using children's data can take place safely and fairly.

Relevant provisions in the UK GDPR – Article 7, Article 9(2)(a) and (g), Article 22(2), Article 22(4), Recital 71

https://www.legislation.gov.uk/eur/2016/679/article/2

Further reading – ICO guidance

- Automated decision-making and profiling
- Children's code: Profiling

Glossary

Application programming interface (API): A computing interface that defines interactions between multiple software intermediaries.

Application (app) developer: A provider specialising in creating and/or maintaining software applications for mobile devices or IoT products, external to the IoT manufacturer.

App store: A distribution platform making available mobile apps, including accompanying apps for IoT products.

App store provider: Organisations responsible for operating the app store with the capability to add and remove apps and make decisions about entry requirements for the app store.

Automatic content recognition (ACR): A type of storage and access technology that periodically captures content that a device displays (eg a smart TV) and matches it against a content library. ACR can be used for different purposes, from identifying the content the user selects to collecting information about their viewing habits (eg for advertising).

Consumer IoT: Products incorporating sensors and different types of connectivity, including the internet, which enable the products to process information, available to people through retail purchase on the consumer market.

Cloud provider: Providers of cloud computing resources (including storage, processing and software) on demand, via a network.

Infrastructure as a service (IaaS): A cloud service model offering access to the raw computing resources of a cloud service.

IoT manufacturer: An organisation with the overall responsibility for the creation and functioning of the IoT product, which may include hardware and/or software creation, then bringing the IoT product to market.

IoT platform: Infrastructure that enables the deployment, management and operation of IoT products through the provision of cloud computing services.

IoT operating system provider: A provider of a software platform designed to manage and coordinate the functions of IoT products, enabling

products to connect to the internet, communicate with each other and process data.

Software development kit (SDK): A set of tools used for developing applications provided by hardware and software providers. They usually include application programming interfaces (APIs), sample code and documentation.

SDK provider: An external organisation to the IoT manufacturer, which provides an SDK.

Telemetry: In IoT, telemetry can refer to the processing of information from IoT products for purposes like analysis and remote monitoring.

User: A user (data subject) of an IoT product whose personal information is processed by an IoT manufacturer or other third parties. The user may be, but doesn’t have to be, the owner of the IoT product.