Data protection

Privacy notices, transparency and control

A code of practice on communicating privacy information to individuals

ico.
Information Commissioner's Office

About the code

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

In many situations where organisations obtain personal data as part of a simple transaction it should be straightforward to use the key recommendations in this code of practice to develop a clear and effective privacy notice.

However, in other situations it will not be effective to use a single document to inform individuals about what you do with personal data. The code uses the term 'privacy notice' to describe all the privacy information that you make available or provide to individuals when you collect information about them. This can encompass all the information you provide using the channels referred to in this code. This is why the ICO believes that it is good practice to develop a blended approach, using a number of techniques to present privacy information to individuals. Not all of these techniques will be useful for your specific requirements but they are all ways of presenting privacy information that we consider to be good practice. You can use the techniques that are recommended in whatever combination is most effective for you in order to present the required privacy information.

These techniques can also allow you to give individuals greater choice and control over how their personal data is used. This is a further element of best practice and demonstrates that you are using personal data fairly and transparently.

It is often argued that people's expectations about personal data are changing. People are increasingly willing to share information on social media and to allow their data to be collected by mobile apps, and they are also unwilling to read lengthy privacy notices. These factors are sometimes used to support the view that they are relatively unconcerned that their data is being collected and processed. However, there is also evidence that people do have concerns about how organisations handle their data and want to retain some control over its further use. Therefore, it is still of paramount importance for organisations to be transparent about their processing and comply with the legal requirements to provide privacy information.

Moreover, many organisations embrace transparency as a means of building trust and confidence with their consumers and use it as a means of distinguishing themselves from their competitors.

Collect and use personal information fairly and transparently

The first principle of data protection is that personal data must be processed fairly and lawfully. The DPA says that in order for the processing to be fair, the data controller (the organisation in control of processing the data) has to make certain information available to the data subjects (the individuals whom the data relates to), so far as practicable:

- who the data controller is;
- the purpose or purposes for which the information will be processed; and
- any further information which is necessary in the specific circumstances to enable the processing to be fair.

This applies whether the personal data was obtained directly from the data subjects or from other

sources.

The GDPR has further requirements about what information should be available to data subjects; they are set out in our section Privacy notices under the EU General Data Protection Regulation.

Being transparent by providing a privacy notice is an important part of fair processing. You can't be fair if you are not being honest and open about who you are and what you are going to do with the personal data you collect. However, this is only one element of fairness. Providing a privacy notice does not by itself mean that your processing is necessarily fair. You also need to consider the effect of your processing on the individuals concerned.

Therefore the main elements of fairness include:

- using information in a way that people would reasonably expect. This may involve undertaking research to understand people's expectations about how their data will be used;
- thinking about the impact of your processing. Will it have unjustified adverse effects on them? and;
- being transparent and ensuring that people know how their information will be used. This means providing privacy notices or making them available, using the most appropriate mechanisms. In a digital context this can include all the online platforms used to deliver services.

To cover all these elements you will need to consider the following issues when planning a privacy notice:

- What information is being collected?
- Who is collecting it?
- How is it collected?
- Why is it being collected?
- How will it be used?
- Who will it be shared with?
- What will be the effect of this on the individuals concerned?
- Is the intended use likely to cause individuals to object or complain?

It is also important to recognise that the ways in which data is collected are changing. Traditionally, data was **collected** directly from individuals, for example when they filled in a form. Increasingly, organisations use data that has not been consciously provided by individuals in this way. It may be:

- **observed**, by tracking people online or by smart devices;
- **derived** from combining other data sets; or
- **inferred** by using algorithms to analyse a variety of data, such as social media, location data and records of purchases in order to profile people for example in terms of their credit risk, state of health or suitability for a job.

In these cases you are acquiring and processing personal data about individuals, and the requirement to be fair and transparent still arises. These new situations can make it more challenging to provide privacy information, and new approaches may be required. A good way to approach these issues is to carry out a privacy impact assessment (PIA). This is a methodology for assessing and mitigating the privacy risks in a project involving personal data.

Privacy impact assessments
For organisations
PDF (542.94K)

Give individuals appropriate control and choice

Where you need consent from an individual in order to process their information you need to explain what you are asking them to agree to and why. This will often go hand in hand with providing privacy notices. Therefore the code also includes information about obtaining consent.

It is important to make sure that where people do have a choice, they are given a genuine opportunity to exercise it. This means that it must be freely given, specific and fully informed. Consent must also be revocable (ie people must be able to withdraw their consent) and you should have procedures in place to action and record it when this happens.

You should always be honest with the public and not lead them to believe that they can exercise choice over the collection and use of their personal information when in reality they cannot.

There are some cases in which consent is not relevant, for example if individuals are required by law to provide their personal details. Giving people control and choice over how their personal data will be processed will not always be applicable in other situations, for example in an employer/employee relationship.

In all of these cases it is still important to be fair and transparent. Ensuring you have effective privacy notices can help you to achieve this.

The Code's status

This code has been issued by the Information Commissioner under section 51 of the Data Protection Act 1998. This requires her to promote good practice, including compliance with the DPA's requirements, and empowers her, after consultation, to prepare codes of practice giving guidance on good practice.

The basic legal requirement is to comply with the DPA itself. Organisations may use alternative methods to meet the DPA's requirements, but if they do nothing then they risk breaking the law. The Information Commissioner cannot take action over a failure to adopt good practice or to act on the recommendations set out in this code. However, she can pursue enforcement action where an organisation breaches the requirements of the DPA. Furthermore, when considering whether or not the DPA has been breached the Information Commissioner can have due regard to the advice provided in this document.

This code should be read in conjunction with other ICO guidance and codes of practice.

The Information Commissioner can take enforcement action if she finds an organisation in breach of the requirements in the DPA, including a failure to provide adequate fair processing information. This could include a civil monetary penalty of up to £500,000 or an enforcement notice ordering an organisation to improve its privacy notice or stop the processing if the notice is not improved. Details of recent ICO enforcement action are available in the Action we've taken section of our website.

Who should use this code?

This code is aimed at all organisations that collect information about people, whether directly or indirectly. It applies to activities such as:

- asking people to fill in their names, addresses and health information on an official form, either online or in paper form;
- collecting information about shoppers from their loyalty card transactions; or
- recording and retaining the calls customers make to a call centre.

It also applies to situations where it may be less obvious that data is being collected, such as when people are observed by smart devices or when information is inferred from how an individual behaves online. For example:

- using an individual's location data on their smart phone to inform them of events going on in their area; or
- analysing what an individual views or shares on social media and marketing them with offers on related products and services.

This code does not apply to collection of information that does not identify people, for example, anonymised or statistical information. However, if you anonymise information once you have collected it then it is best to inform people that you do so. You should also make sure that you explain that if you are anonymising personal data, then you are undertaking processing of personal data in order to anonymise it.

This code of practice is designed as a good practice document to help you collect and use personal information fairly and transparently and give individuals appropriate control and choice over their data, including in a digital context. It focuses on drafting and communicating clear privacy notices that ensure that individuals know how information about them will be used, and that they understand the impact it will have on them.

You can use this code in several different ways, depending on the sort of information you collect and how you do it, for example:

- to produce a new privacy notice;
- to develop an existing privacy notice; or
- to evaluate an existing privacy notice.

It includes examples to show how the different approaches we are recommending can work in practice.

Why should you provide effective privacy information?

Providing privacy information is a requirement of the DPA, and this code provides guidance on how to comply with this. The GDPR specifies further detail that organisations processing personal data will need to include in their privacy notices. We have summarised these in Privacy notices under the EU General Data Protection Regulation. Following the good practice recommendations in this code will assist you in meeting these obligations.

Following good practice in providing privacy notices helps you to deal with people in a clear and transparent way and empower them. This makes good sense for any organisation and is key to developing trust with customers or citizens.

If you empower individuals to manage what you do with their personal data, giving them more choice and integrating preference management tools, such as a privacy dashboard, with your privacy notice you may be able to obtain more useful information from them.

If individuals are able to exercise real choice over what is done with their personal data, you can be more confident that people have provided informed consent for their information to be used, if this is the legal basis you are relying on.

By taking this approach, you are firstly acting more openly and, in a data protection sense, more fairly, but you are also able to use data more effectively.

As digital interaction with consumers becomes the norm, privacy notices should be seen as flexible and deliverable via a number of mechanisms, often in combination. Following the good practice approach described here means that information can be provided at different times and at appropriate points during an organisation's interaction with their customer.

The value of personal data is increasing and technology is rapidly developing. Personal data can be manipulated and used in increasingly sophisticated ways and sometimes on a large scale. Also, individuals often express general concerns about how their information is used but at the same time they often find it difficult to engage with privacy notices. This leaves them uninformed about how their information is being used and sometimes feeling unfairly treated as a result.

Providing meaningful and effective information in this context is an ongoing challenge for organisations but one that they must meet to comply with data protection law. To get this right, you need to identify the means of communication and the language and tone that is most appropriate to the audience bearing in mind the way that their personal data is being used.

What should you include in your privacy notice?

The starting point of a privacy notice should be to tell people:

- who you are;
- what you are going to do with their information; and
- who it will be shared with.

These are the basics upon which all privacy notices should be built. However, they can also tell people more than this and should do so where you think that not telling people will make your processing of that information unfair. This could be the case if an individual is unlikely to know that you use their information for a particular purpose or where the personal data has been collected by observation or inference from an individual's behaviour.

Map your information processing

To help you decide what you need to include you should map out how your information flows through your organisation and how you process it, recognising that you might be doing several types of processing. You should work out:

- what information you hold that constitutes personal data;
- what you do with the personal data you process;
- what you actually need to carry out these processes - a privacy impact assessment can help you to answer this question;
- whether you are collecting the information you need;
- whether you are creating derived or inferred data about people, for example by profiling them; and
- whether you will be likely to do other things with it in the future – this can be particularly important if you are undertaking large scale analysis of data, as in big data analytics.

When explained in sufficiently broad terms a privacy notice can allow for development in the way you use personal data, whilst still providing individuals with enough detail for them to understand what you will do with their information. However, you should not draw up a long list of possible future uses if, in reality, you do not intend to process personal data for those purposes.

Gain and record consent

You need to consider how you will gain and record individuals' consent, if required. There is a fundamental difference between telling a person how you're going to use their personal information and getting their consent. Although in many cases it is enough to be transparent, and rely on a legal basis other than consent, in others a positive indication of an individual's agreement will be needed. For example, if you wish to use personal data for the purposes of medical research it is likely that you will require an individual's consent.

When relying on consent, your method of obtaining it should:

- be displayed clearly and prominently;
- ask individuals to positively opt-in, in line with good practice; and
- give them sufficient information to make a choice. If your consent mechanism consists solely of an "I agree" box with no supporting information then users are unlikely to be fully informed and the consent cannot be considered valid.

In addition if you are processing information for a range of purposes you should:

- explain the different ways you will use their information; and
- provide a clear and simple way for them to indicate they agree to different types of processing. In other words, people should not be forced to agree to several types of processing simply because your privacy notice only includes an option to agree or disagree to all. People may wish to consent to their information being used for one purpose but not another.

Good practice would be to list the different purposes with separate unticked opt-in boxes for each or Yes/No buttons of equal size and prominence. Opt-in boxes can be prominently placed in your privacy notice. Alternatively, with online products and services you may wish to use 'just-in-time' notices so that relevant information appears at an appropriate time; see the section on just-in-time notices for more detail.

You should also consider how you can obtain consent following any changes to your privacy notice, and how individuals can revoke this consent if they do not agree with these changes.

If you are asking people to consent to receive direct marketing, then, in addition to the DPA requirements, specific rules apply to this under the Privacy and Electronic Communications Regulations (PECR).

If you want individuals to consent to direct marketing, you should have a separate unticked opt-in box for this, prominently displayed. Consent may not be needed to undertake direct marketing by post or phone call (unless the individual is registered with the Telephone Preference Service) if another processing condition can be relied on, but the ICO considers gaining consent to do this to be good practice and the most advisable approach.

The box below contains standard wording that we've tested with members of the public and, which in our view constitutes good practice when seeking consent for direct marketing.

> Here at [organisation name] we take your privacy seriously and will only use your personal information to administer your account and to provide the products and services you have requested from us.
>
> However, from time to time we would like to contact you with details of other [specify products]/ [offers]/[services]/[competitions] we provide. If you consent to us contacting you for this purpose please tick to say how you would like us to contact you:
>
> **Post ☐ Email ☐ Telephone ☐**
>
> **Text message ☐ Automated call ☐**
>
> We would also like to pass your details onto other [name of company/companies who you will pass information to]/[well defined category of companies], so that they can contact you by post with details of [specify products]/ [offers]/[services]/[competitions] that they provide. If you

consent to us passing on your details for that purpose please tick to confirm:

I agree ☐

Direct marketing guidance
For organisations
PDF (507.47K)

If you share data with other data controllers

If you are sharing personal data with other data controllers then you need to consider the challenges of communicating this in a privacy notice. Even if you have a legal basis other than consent for sharing data, you still need to tell people what you are doing with their data in order for your processing to be fair, unless there is an exemption from this in data protection legislation.

In some cases, several data controllers will be involved in processing the personal data and you will each have obligations to provide privacy notices to the user. This can happen, for example, with data collected by smart devices in the internet of things (IoT) that can be connected with one another and can collect and exchange personal data.

Example

An individual uses a wearable device to monitor their exercise. The manufacturer of the device is the data controller of the information which the device collects about the individual.

A third party application developer has created an app to use with the device that does specific things with the data, such as monitoring the individual's fitness levels and providing a reward when they reach a certain point. The app developer would be a data controller of the data used for that purpose, unless the data was properly anonymised.

A social networking site allows information to be posted from the device onto its site and then uses this data to make inferences about what the individual does, for example that they like to run. If, on the basis of this data, the network then shows adverts about running shoes to that individual, it will also be a data controller.

A health insurance company provided the device to the individual so that they could reduce their premium by completing a fitness challenge. Although the insurance company did not design the device they would still be a data controller because they determined that the data would be used to incentivise its customers.

In this scenario here are potentially four data controllers. There could be fewer if, for example, the health insurance company also developed the app.

In a complex data sharing scenario such as this, individuals may not have a clear understanding of all of

the parties involved, how their information is being shared or for what purpose. Sometimes data controllers may not be immediately aware of all the other parties involved but you need to identify who you are working with to ensure that you all provide privacy notices to meet your obligations under data protection legislation.

In most of these cases each party is a separate data controller and a data sharing agreement is needed between you, which should include how you communicate privacy notices and what they include. Each data controller must ensure that they discharge their own obligations to provide information about their use of personal data. It may also be possible to supplement these individual privacy notices with a collaborative end to end resource that brings all of the privacy information together for individuals.

Go beyond legal requirements

Depending on the circumstances, you may decide it is beneficial to go beyond the basic requirements of the law, for example by telling people:

- the links between different types of data you collect and the purposes that you use each type of data for;
- the consequences of not providing information - for example, non-receipt of a benefit;
- what you are doing to ensure the security of personal information;
- information about their rights of access to their data; and
- what you will not do with their data.

Example

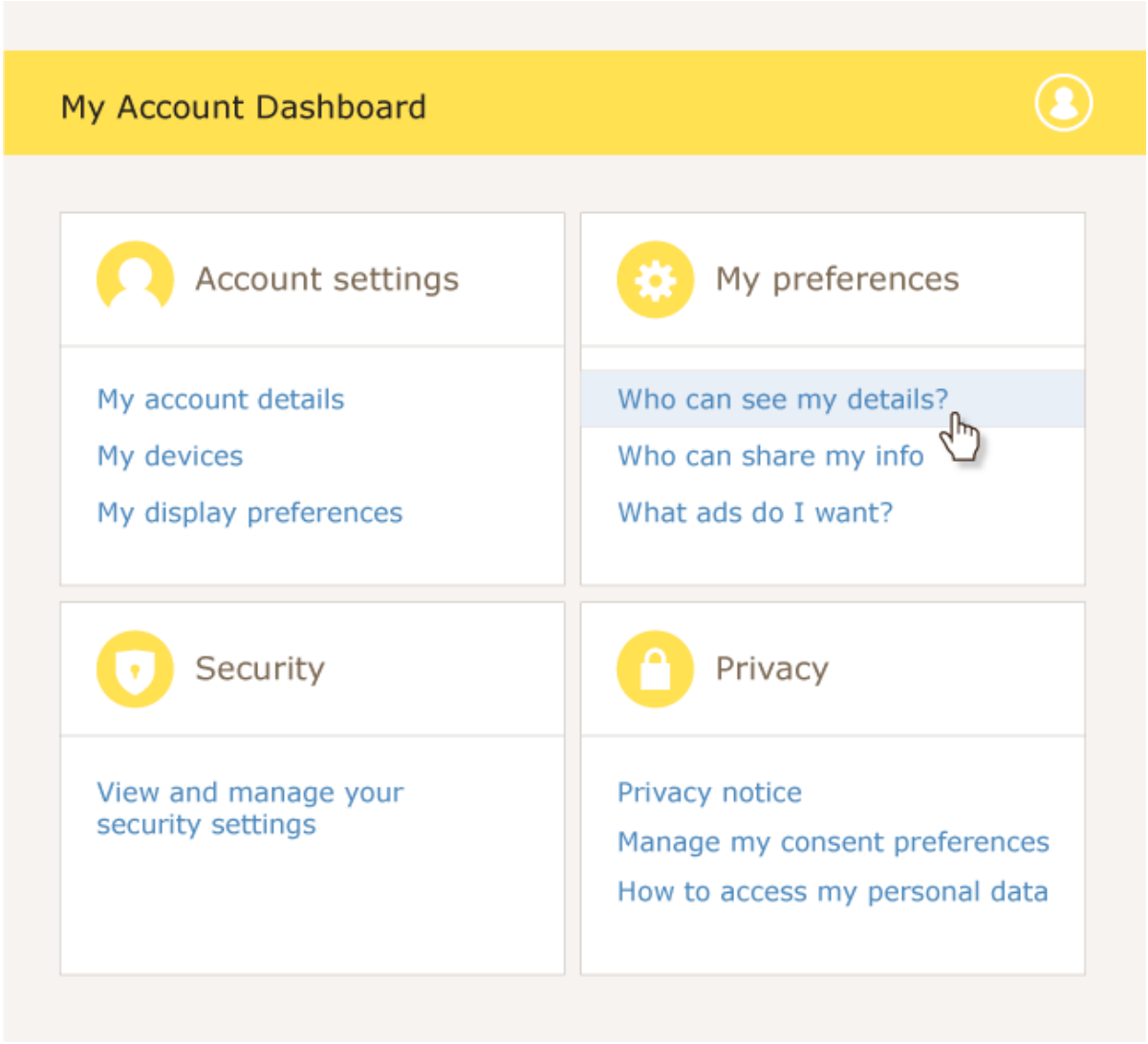
If you have no intention of sharing data with third-parties for marketing purposes you can state this explicitly in your privacy information but you must be absolutely certain before making the statement and amend it if the position changes.

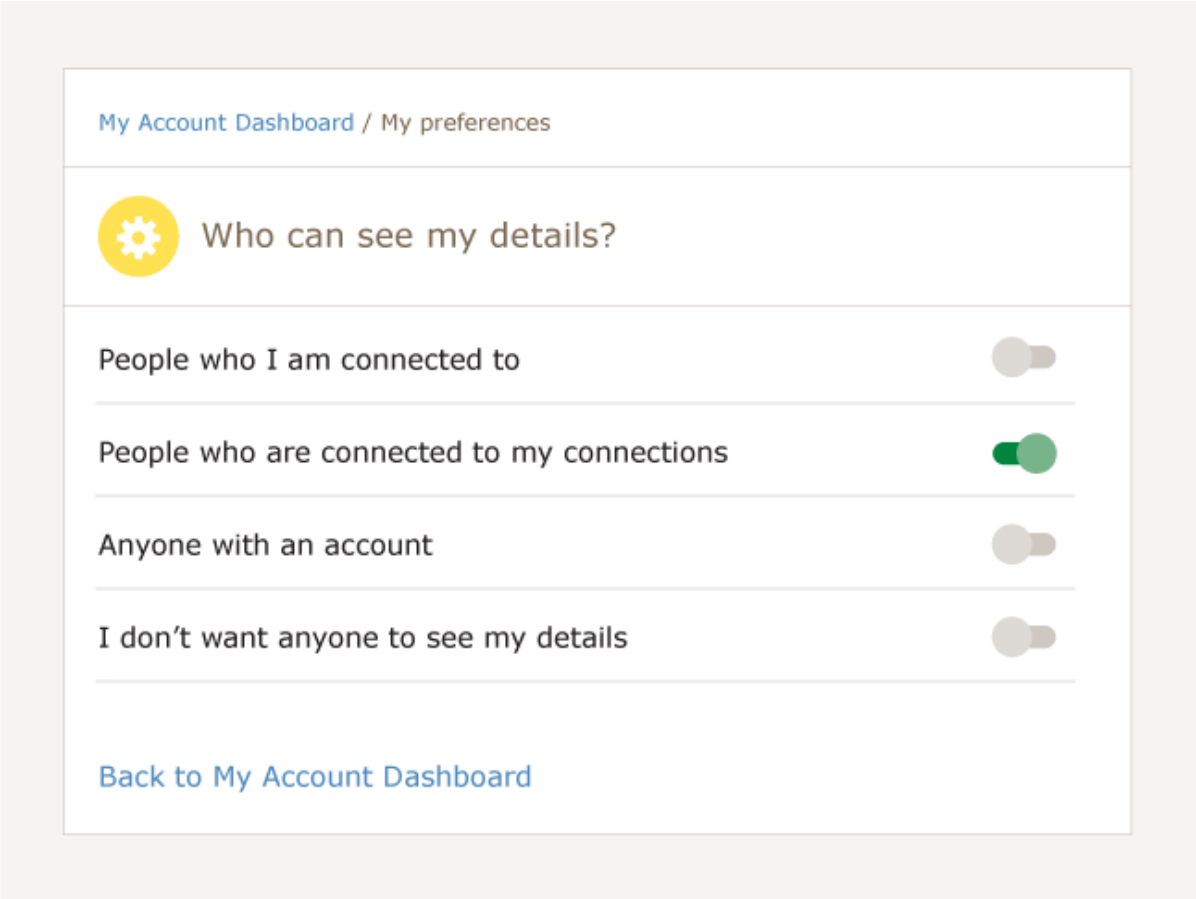
Use preference management tools

It is good practice to embed links to tools like dashboards within your privacy notice to allow individuals to manage their preferences and to prevent their data being shared where they have a choice.

A privacy dashboard can help to achieve this. This offers people one place from which to manage what is happening to their information. This is helpful if you process personal data across a number of applications or services.

For individuals it allows them to alter settings, so that (where consent is relevant) they are able to clearly indicate that they agree to the particular processing or data sharing. It also allows for consent to be provided and revoked over time, as processing develops or individuals change their minds. It should be as easy to revoke consent as it was to provide it.


My Account Dashboard
Account settings
My account details
My devices
My display preferences
My preferences
Who can see my details?
Who can share my info
What ads do I want?
Security
View and manage your security settings
Privacy
Privacy notice
Manage my consent preferences
How to access my personal data



You can then use this platform to relay details of any changes to your data processing and feel reassured that customers will take the time to understand and action them. Ultimately this should help to build trust and confidence with the customer.

Building individuals' awareness and confidence in tools like dashboards is likely to make them more informed and better placed to engage with messages about what is happening to their information and how to manage it. Well designed and readily accessible dashboards also provide an opportunity for individuals to access copies of their personal data, ideally in a re-usable and machine readable format. Providing information in this manner will not remove the right to make a subject access request (SAR) but in some cases individuals will be able to access the information they require via this route rather than by submitting a SAR.

Where should you deliver privacy information to individuals?

You should not necessarily restrict your privacy notice to a single document or page on your website. The term ‘privacy notice’ is often used as a shorthand term, but rather than seeing the task as delivering a single notice it is better to think of it as providing privacy information in a range of ways. All of the information you are giving people about how you are processing their data, taken together, constitutes the privacy information.

Communicating privacy information

You can provide privacy notices through a variety of media:

- Orally - face to face or when you speak to someone on the telephone (it’s a good idea to document this).
- In writing - printed media; printed adverts; forms, such as financial applications or job application forms.
- Through signage - for example an information poster in a public area.
- Electronically - in text messages; on websites; in emails; in mobile apps.

It is good practice to use the same medium you use to collect personal information to deliver privacy notices. So, if you are collecting information through an online form you should provide a just-in-time notice as the individual fills out the form. It would not be good practice to collect information through the form and then email the individual with a separate link to a privacy notice.

Example

A message at the point you enter your email address explaining that it will be used for customer service purposes will be more effective and accessible than just a link to a separate notice elsewhere.

In some contexts it can be very difficult to communicate a privacy notice. For example, in an emergency situation obtaining personal details quickly can be critical to protecting an individual. In cases like these, you should explain how you use the information at an appropriate point later on, or if you can’t provide privacy information, it is particularly important to make sure you only use the information you collect in a way that members of the public are likely to anticipate and agree to.

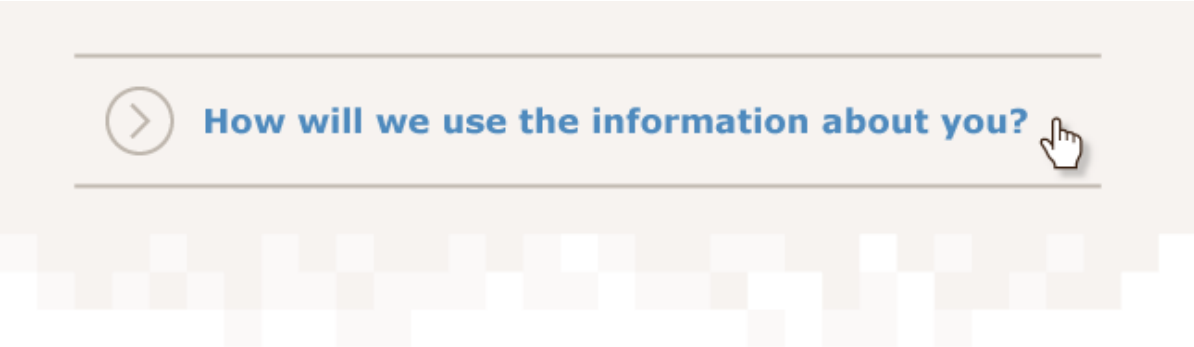
Take advantage of all of the technologies available when providing privacy notices. It may be valuable to consider these solutions after you have completed a privacy impact assessment. Examples of technological solutions include just-in-time, video, the functionality of devices and privacy dashboards. These can be seen as privacy-enhancing technologies, because they help to protect privacy and safeguard personal data. A blended approach, incorporating a variety of these techniques is likely to be most effective. Keep the individual as the focus when making decisions about the way to deliver privacy

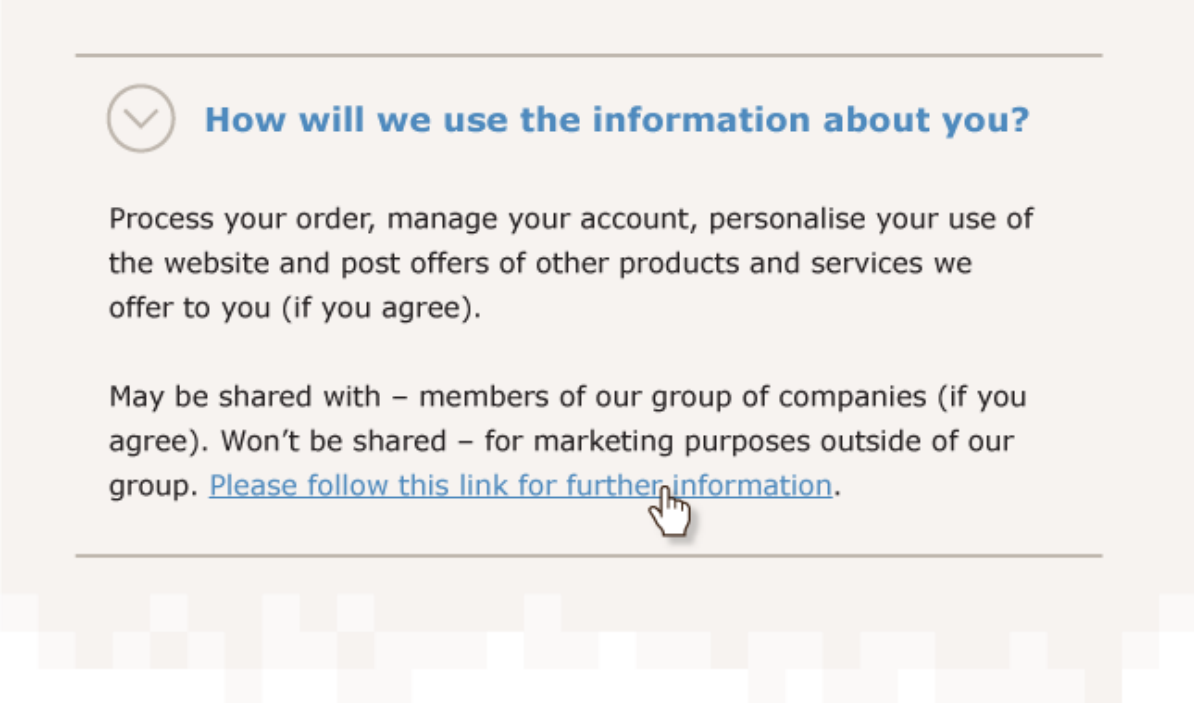
notices.

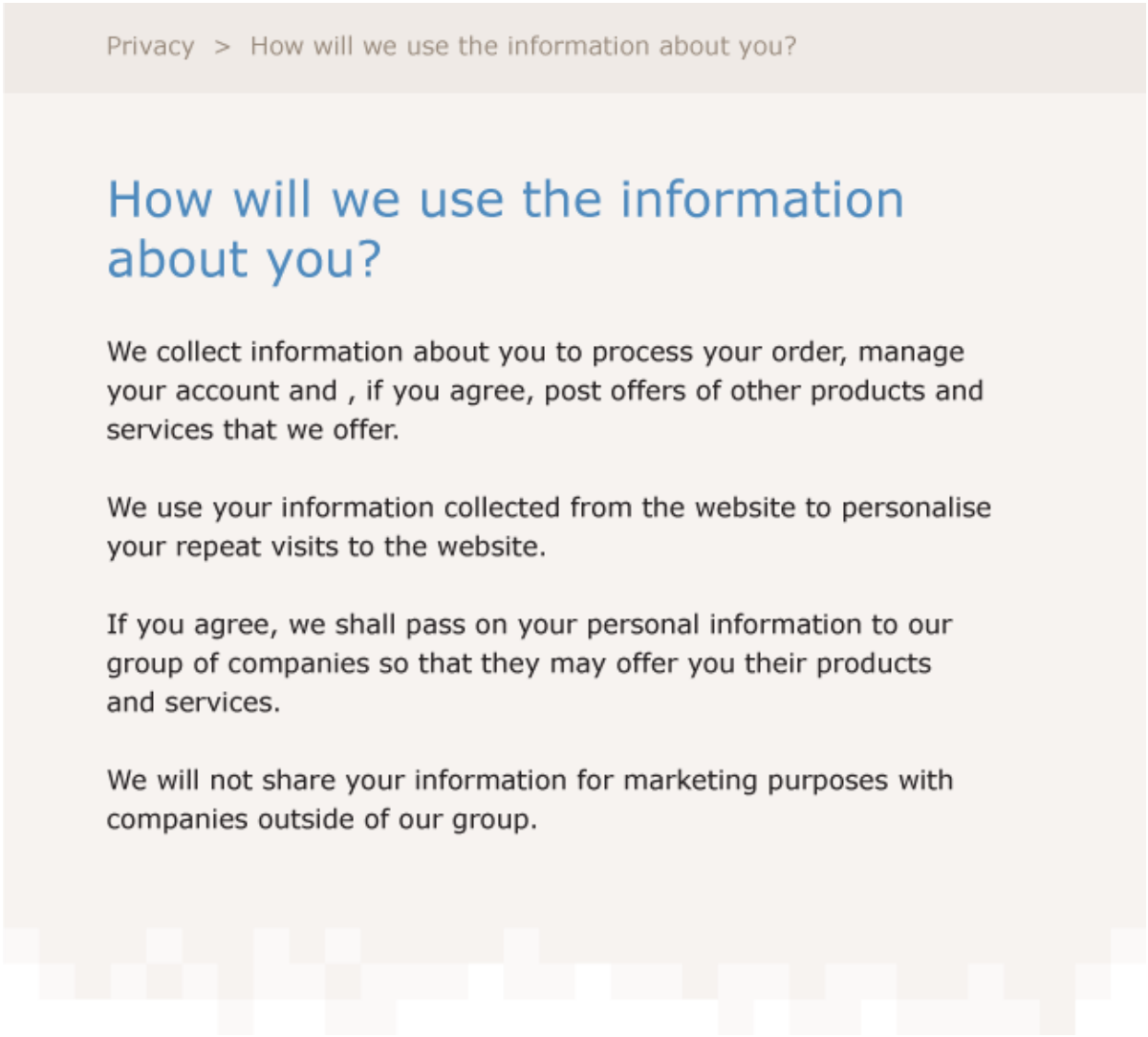
Layered approach

A layered approach can be useful as it allows you to provide the key privacy information immediately and have more detailed information available elsewhere for those that want it. This is used where there is not enough space to provide more detail or if you need to explain a particularly complicated information system to people.

It usually consists of a short notice containing the key information, such as the identity of the organisation and the way you will use the personal information. It may contain links that expand each section to its full version, or a single link to a second, longer notice which provides more detailed information. This can, in turn, contain links to further material that explains specific issues, such as the circumstances in which information may be disclosed to the police.







There will always be pieces of information that are likely to need to go into the top layer of a notice, such as who you are, what information you are collecting and why you need it What else goes into which layer will depend on the type of processing that you undertake. The ICO considers that data controllers have a degree of discretion as to what information they consider needs to go within which layer, based on the data controller's own knowledge of their processing. A combination of your own knowledge of how you process personal data and an understanding (that will be informed by this code) of what you need to do to make processing fair or fairer, will allow you to decide on what information should go into which layer of a notice. However, all layers should be accessible.

It works very well in an online context, where it is easy to provide a front page link. The front page should also give people prominent, early warning of any use of their information that is likely to be unexpected or objectionable. As demonstrated by the example in the Test, roll out and review section, when using this approach you need to ensure that people don't miss information if they arrive at a particular area of your website by a search. You also need to ensure that searches including 'privacy notice' or associated terms return links to full privacy notices.

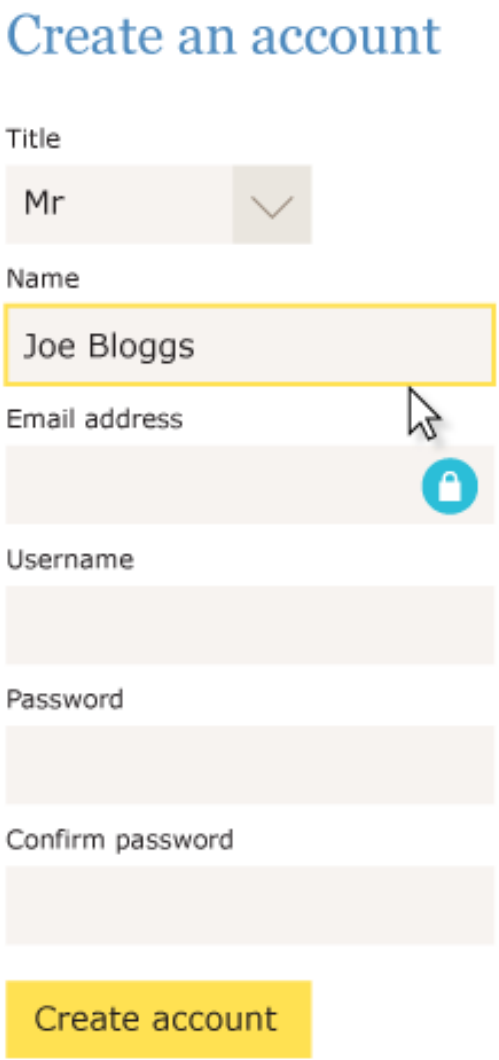
This technique is also useful if you are a data controller who has further sectoral requirements that mean you need to present other information in addition to the privacy information. For example, information regarding fraud in the financial sector. As this increases the amount of information you have to provide, it is even more important that you present it in an engaging manner and the tools and techniques recommended in this code will help you.

Just in time notices

Just-in-time notices are a tool you can use to provide relevant and focused privacy information in such situations. This is another type of layered approach to provide information at certain points of data collection.

Often, and particularly when on an organisation's website, people will provide personal data at different points of a purchase or interaction. When filling out a form people may not think about the impact that providing the information will have at a later date.

Just-in-time notices work by appearing on the individual's screen at the point where they input personal data, providing a brief message explaining how the information they are about to provide will be used.



The individual can either choose to carry on with the basic information or click on the link to find out more information. This can direct them to a more specific page explaining in detail what will be done with the personal information they have provided.

You can achieve a similar result using the hover over feature when completing fields in an online form.

Icons and symbols

You can use icons and symbols as part of a layered approach. This can indicate that a particular type of data processing is occurring.

- For example, a symbol that designates that information will be used for marketing could appear when you input your email address.
- For those who would like to know more, they can click on the symbol and be directed to a more detailed explanation of what will be done with this piece of their personal data.
- Alternatively, you can use the 'hover over' function so that when you place the cursor over the symbol it states 'marketing' and if the user wishes to know more they can click through for more detail.

Icons and symbols can also act as useful reminders that data processing is taking place, especially if that processing is intermittent, in the same way as a red light which comes on when audio or video is being recorded.

Icons and symbols can be useful in relation to IoT devices, where it is difficult to provide detailed privacy information on the device itself and in other situations where data is being captured by observation rather than being provided by individuals.

The design of any symbols is important as you need to make the messages they convey as clear as possible. It is also important to limit the number of symbols used, as people are unlikely to take the time to learn what a large number of different symbols mean. Use symbols consistently and make sufficient information available so that people understand what they mean; you should produce a key to the symbols that can be accessed easily by users.

If you are a large organisation then a set of symbols that can be used across your operations would be an effective and consistent means of providing privacy information.

- The use of symbols can be done with your brand in mind so that they fit with the look of your websites.
- The same approach could work within sectors, where an agreed set of symbols could be used to ensure consistency across organisations.

If you are going to use symbols to present privacy information then it is important that you undertake user testing to ensure that what you produce is effective.

If the icons are made available electronically you should also consider making them available in a machine readable form. This would allow a device to 'read' the information the icon conveys.

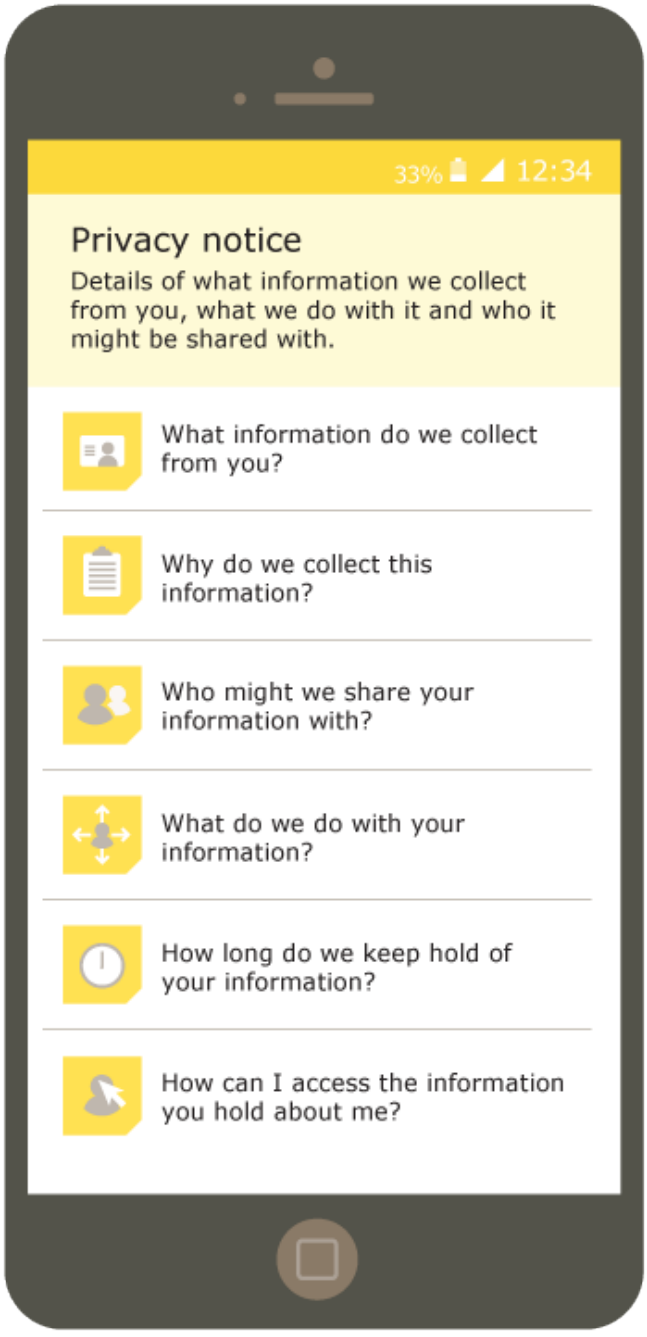
Privacy notices on mobile devices and smaller screens

You must also consider how people will view privacy notices on portable devices (smart phones, tablets).

You must ensure that privacy notices are as clear and readable on these devices as the information you would see on a computer screen. The text should be large enough to read and people should not have

to zoom in to see it. Information should fit on the screen as normal. A useful tool is responsive web design, which allows you to create a website that can change the information on the screen to the optimal setting for viewing that information, depending on the type of device you are viewing it on.

As the devices are likely to have less space to display your privacy information, a layered approach is likely to be the best method to communicate privacy notices effectively.



The use of video or just-in-time notices to convey privacy information is particularly suitable for smaller devices as the size and length of text will not be an issue. You are unlikely to be able to convey all the necessary detail in a video but following a layered approach, individuals can be directed to more detailed information as appropriate. Keeping the video short and to the point will also avoid any issues individuals may have with data usage if Wi-Fi isn't available.

00:00 / 01:07

View this video on the GoAnimate website at ico.org.uk/PNvideo

You can use the functionality of a device, for example using voice alerts on a smart phone (or on-screen notifications once the phone is set to silent), to provide information essentially like a just-in-time notice. However, you must consider how you can prevent the phone or mobile app giving someone constant alerts regarding their information. This is where a link to a dashboard or information management tool may be helpful, or a prompt to review your settings on your smartphone.

Privacy in mobile apps: Guidance for app developers
For organisations
PDF (731.19K)

When should you actively communicate privacy information?

It is good practice to try to put yourself in the position of the people you're collecting information about. You need to understand the level of knowledge your intended audience has about how their data is collected and what is done with it. This will help you decide when to give them privacy information. If an individual would not reasonably expect what you will do with their information you need to actively provide privacy information, rather than simply making it available for them to look for themselves, for example on your website.

If it is reasonable for someone to expect that you will use their information for an intended purpose, you are less likely to need to actively explain it to them and can instead make privacy information available if they look for it.

Example

A person might purchase a book from an online store. Their personal information is only used to despatch the goods, to take payment and for the company's own record keeping. In this case, the collection and use of the information would not be unfair even if the individual has not been explicitly told about it. This is because any reasonable person requesting the service would understand that they cannot receive the goods they want unless some processing of their personal information takes place.

However, there are situations when someone would not reasonably expect you to use their information in the way that you intend to. The need to actively provide privacy information is strongest where:

- you are collecting sensitive information;
- the intended use of the information is likely to be unexpected or objectionable;
- providing personal information, or failing to do so, will have a significant effect on the individual; or
- the information will be shared with another organisation in a way that individuals would not expect.

If you have explicitly assured individuals that you will not share their information with third parties but now wish to do so, you should inform them and actively seek their consent. You should also update your privacy notice accordingly.

If you are unsure whether someone would reasonably expect what you will do with their information, there are a number of other things you can do to get a more informed picture about your customers:

- Undertake some research with customers and the wider public, explaining what you would like to do and from that gauge whether or not they would reasonably expect you to do what you're planning. Focus groups or online questionnaires could be used.
- If you are planning on doing something similar to what you have done in the past, review whether you had any issues when implementing new processing or if you received a lot of complaints about it.
- Look at the experience of others in your sector or industry to see if there has been an approach that

has been welcomed by customers or worked particularly well.

- Consider using a privacy impact assessment. Further guidance can be found in our Conducting privacy impact assessments code of practice. This explains how to consult and understand the perspective of individuals in chapter 3.

If you decide that you will need to actively communicate privacy information, you can do this by:

- contacting them directly by letter or email;
- reading out a script during a phone call;
- providing interactive information in an online form, to explain why you need particular information; or
- delivering text-based notifications that appear briefly when an individual hovers over a particular field.

How should you write a privacy notice?

One of the biggest challenges is to encourage people to read privacy information. People are often unwilling to engage with detailed explanations, particularly where they are embedded in lengthy terms and conditions. This does not mean that privacy notices are merely a formality; it means that they have to be written and presented effectively.

You should:

- use clear, straightforward language;
- adopt a simple style that your audience will find easy to understand;
- not assume that everybody has the same level of understanding as you;
- avoid confusing terminology or legalistic language;
- draw on research about features of effective privacy notices when developing your own;
- align to your house style. Using expertise, for example in-house copywriters can help it fit with the style and approach your customers expect;
- align with your organisation’s values and principles. Doing so means that people will be more inclined to read privacy notices, understand them and trust your handling of their information;
- be truthful. Don’t offer people choices that are counter-intuitive or misleading;
- follow any specific sectoral rules as well as complying with data protection law, for example in advertising or financial services sectors; and
- ensure your privacy notices are consistent across multiple platforms and enable rapid updates to them all when needed. Privacy notices can be managed using content management systems (CMS).

Privacy notices for a wide range of individuals

If you are dealing with a wide range of individuals you need to think about the relationships you have with the various groups and whether they will all understand the information. For example, a local authority might use information about eligible people to administer free access to local leisure facilities and information about business proprietors to collect business taxes.

Consider breaking your customers down into different categories and providing separate notices for each. This is likely to make information clearer and easier to understand rather than having a single, catch-all privacy notice.

Privacy notices for vulnerable individuals

If you collect information from vulnerable individuals, such as children, you must make sure those individuals are treated fairly. This involves drafting privacy notices appropriate to the level of understanding of your intended audience and, in some cases, putting stronger safeguards in place. You should not exploit any lack of understanding or experience, for example, by asking children to provide personal details of their friends.

Again, you should try to look at your collection of information from the individual's point of view. You should use your knowledge of the individuals you deal with to decide your approach. In particular, you

should try to work out whether the individuals you are collecting information about would understand the consequences of this. If in doubt, you should be cautious and should instead ask the individual's parent, guardian or carer to provide the information. Alternatively, you could develop mechanisms to prevent vulnerable individuals from going too far if you have already identified concerns, for example on a mobile app or website.

When dealing with vulnerable individuals there may be times when using a combination of the techniques described in this code may not be effective, as it may cause confusion or provide less clarity. If this is likely to be the case, the key point is to focus on providing a clear and understandable privacy notice that has taken into consideration the target audience. The Privacy notices in practice section contains real life examples of privacy notices demonstrating good and bad practice that we have retained from the previous version of this code of practice.

More guidance about consent and children under the GDPR will be made available separately to this code.

Privacy notices for people whose first language is not English

Sometimes you may want to collect information from people whose first language is not English. In some cases you may be obliged by law to provide forms and privacy notices in another language, for example, Welsh. Although you may not be required by law to offer translations, it is good practice to provide your privacy notice in the language that your intended audience is most likely to understand.

Personal information online code of practice
For organisations
PDF (624.01K)

Test, roll out and review

Before roll out

Carrying out user testing will provide useful feedback on a draft privacy notice. This is where you select a sample of your customers and ask them to use your privacy notice to obtain their feedback on:

- how they used it;
- if they found it easy to understand;
- whether anything was difficult, unclear or they did not like it; or
- if they identified any errors.

Asking your customers to do this will help you improve the effectiveness of your privacy notice. You are likely to come up with a far more useful and engaging product if you consider feedback from the people it is aimed at.

Example

You may produce a privacy notice that is based on assumptions you have made about a user's journey around your website. However, during your user testing you identify that people are often directed to a specific page straight from a third party search engine and therefore miss some of the privacy information that you have supplied on your homepage. Having identified this, you can ensure that your privacy information is correctly connected together so that individuals do not miss anything important. For example, you can provide a link to your full privacy notice in all your just-in-time notices so that an individual can see the important message at that point in the journey but can also refer back to the full document to see if they have missed anything.

Having made any changes to your privacy information as a result of user testing, you are then ready to roll it out using the tools and approaches you have selected.

After roll out

It is good practice to regularly review your privacy notice.

You should:

- ensure that it remains accurate and up to date;
- analyse complaints from the public about how you use their information and in particular any complaints about how you explain your use of their information;
- check that your privacy notice actually explains what you do with individuals' personal data; and
- update your privacy notice to reflect any new or amended processing.

As well as regular reviews, you should review your privacy information whenever you change or update

a process. This follows the concept of privacy by design and you should incorporate this approach into your processes. You should check whether or not your changes impact upon what privacy information you provide and if they do, amend your privacy information appropriately. If you are relying on consent for your processing, you may also need to ask data subjects for their consent as well.

Your privacy notice checklist

What

Decide what to include by working out:

- what personal information you hold;
- what you do with it and what you are planning to do with it;
- what you actually need;
- whether you are collecting the information you need;
- whether you are creating new personal information; and
- whether there are multiple data controllers.

If you are relying on consent, you should:

- display it clearly and prominently;
- ask individuals to positively opt-in;
- give them sufficient information to make a choice;
- explain the different ways you will use their information, if you have more than one purpose;
- provide a clear and simple way for them to indicate they agree to different types of processing; and
- include a separate unticked opt-in box for direct marketing.

Also consider including:

- the links between different types of data you collect and the purposes that you use each type of data for;
- the consequences of not providing information;
- what you are doing to ensure the security of personal information;
- information about people’s right of access to their data; and
- what you will not do with their data.

Where

Give privacy information:

- orally;
- in writing;
- through signage; and
- electronically.

Consider a layered approach:

- just-in-time notices;
- video;
- icons and symbols; and
- privacy dashboards.

When

Actively give privacy information if:

- you are collecting sensitive information;
- the intended use of the information is likely to be unexpected or objectionable;
- providing personal information, or failing to do so, will have a significant effect on the individual; or
- the information will be shared with another organisation in a way that individuals would not expect.

How

Write and present it effectively:

- use clear, straightforward language;
- adopt a style that your audience will understand;
- don’t assume that everybody has the same level of understanding as you;
- avoid confusing terminology or legalistic language;

- draw on research about features of effective privacy notices;
- align to your house style;
- align with your organisation’s values and principles;
- be truthful. Don’t offer people choices that are counter-intuitive or misleading;
- follow any specific sectoral rules;
- ensure all your notices are consistent and can be updated rapidly; and
- provide separate notices for different audiences.

Test and review

Before roll out:

- test your draft privacy notice with users;
- amend it if necessary.

After roll out:

- keep your privacy notice under review;
- take account of any complaints about information handling;
- update it as necessary to reflect any changes in your collection and use of personal data.

Your privacy notice checklist
For organisations
PDF (102.26K)

Privacy notices in practice

In practice, you may need to do more to engage individuals and build confidence in what you are doing with their personal information in the following scenarios about sharing, selling and Big data.

We have also included examples of good and bad practice to help you produce effective privacy information.

Sharing information

If you are sharing personal data with other organisations you should consider whether you need to actively inform the data subjects about this. Data can be shared in many different scenarios, including businesses selling data on a commercial basis or public authorities sharing data to improve the delivery of services.

In order to treat people fairly prior to sharing information, you must carefully consider what any recipient organisation is going to do with it and what the effect on people is likely to be. It is good practice to obtain an assurance about this, for example in the form of a contract or a written data sharing agreement.

Combining information from different sources can create a very detailed picture of an individual's affairs, for example by combining information from several different social media sites, including images, video and location history. Organisations that intend to combine information acquired from third party sources should explain this, and its likely consequences. This is a clear example of where it is appropriate to actively communicate a privacy notice using a combination of techniques as an individual may not expect this to happen and may find it overly intrusive.

It is good practice to embed links to tools like dashboards within your privacy notice to allow individuals to manage their preferences and to prevent their data being shared where they have a choice. Data sharing is one area in which the use of an icon or symbol within a privacy notice may be helpful. Read more information in the section on icons and symbols and our Data Sharing code of practice.

Selling information

Some organisations set out to collect personal information with the intention of selling or renting it to third parties. If you intend to do this, you should give people a clear idea of the types of organisations you are supplying their information to, what purposes it will be supplied for and if these are marketing purposes, gain their consent where necessary. You should tell them this when you ask them to provide their details and give them a simple opportunity to revoke this consent in the future. See the section on Gain and record consent above for more information about a standard approach to seeking and recording consent. There is more guidance on sharing information for marketing in our Direct Marketing guidance.

Privacy notices are very useful when information is being bought, sold or rented. They can help the recipient organisation to check what people were told when they originally provided their information. Depending on what they were told, the recipient organisation may then need to communicate its own privacy notice to the individuals concerned. If there is a difference between what people were told originally and what the recipient organisation intends to do with the information, then individuals must be

advised of this within a reasonable period of time. If there is a difference, individuals should be asked whether they agree to their information being used for the new purpose (this is true in all situations, not just when selling information) unless a data controller intends to rely on a different condition for processing the information. Failing to check what 'permissions' apply to the data could lead to a breach.

Normally, personal information can only be sold if the individuals concerned have already been told that their information may be passed on to other organisations.

When a business is insolvent, bankrupt, being closed down or sold, its database can be sold on (or, if rented, it should be returned to its owner). However, the seller must make sure that the information will only be used for the same or a similar purpose. If the buyer wants to use the personal information for a new purpose, it will have to get consent for this from the individuals concerned.

Big data

Large scale analytics, also known as big data, can raise particular issues in relation to data protection and transparency, where it uses personal data. It typically involves processing large volumes of information, taken from a range of sources, and using algorithms to detect trends and correlations. It can be used to make decisions about an individual. In some cases this type of processing can have a relatively limited impact on individuals but in others it can result in extremely intrusive profiling.

People often have limited awareness that information about them is being gathered and processed in this way. Often they don't understand how the information is used to make decisions that affect them. In the absence of clear, well-structured and easily accessible privacy notices, it is unlikely that this type of processing would be within their reasonable expectations.

When undertaking large scale analytics you should consider whether you need to use data that identifies individuals, or whether you can work with anonymised data. Anonymisation can be an important tool in big data analytics. See our Anonymisation code of practice for further information.

You should assess the impact of your processing on individuals, and ways to mitigate this, by carrying out a privacy impact assessment. You need to decide how you will comply with the first data protection principle to process personal data fairly and lawfully. This will involve balancing the benefits you expect from the processing against the impact on individuals.

There may be particular issues with privacy notices in a big data context, in that it may be more difficult to foresee at the outset how you will use the data. Nevertheless, you still need to give people a general indication of what you are doing with their data and add detail to the privacy notice as you go on, if necessary.

You must decide whether you need to obtain consent from individuals to this type of processing or if you can rely on one of the other conditions in the law, such as legitimate interests. This will frequently depend on the likely effect on the individual; the greater the impact, the more likely you are to need consent. If you are relying on the legitimate interests condition, you should to be able to demonstrate how you have taken account of the impact on individuals' privacy rights.

Where consent is required you need to contact individuals to obtain it, either using contact information you already hold or using alternative techniques such as just-in-time notices when they log on to use your services. Where consent is not required you still need to make sufficient information available so that people understand how their information is being used.

This type of analytics often involves finding new uses for data. If you obtained information for one

purpose but you now intend to use it for another you should make this clear and explain the impact of the new processing. Where you have identified a number of potential uses for the information you should include an explanation of them in the information you provide.

Big data analytics can deliver a wide range of benefits, but it is often opaque to the individuals whose data is being processed, and may produce unexpected consequences for them. If you are using data in this way it is important to build a relationship of trust with people. Being transparent about the processing, and finding effective ways to deliver privacy information are both key to that relationship.

Good and bad examples of privacy notices

The practical examples linked here are based on real privacy notices that we have seen. They illustrate good practices to adopt, such as giving people appropriate choices that are easy to exercise, and bad practice to avoid, such as using confusing language. They are illustrative extracts only and are not intended to be used as templates. They cannot cover every type of information you collect but they should help you to produce your privacy notice, whether printed or online. Please note that the formats shown may not meet accessibility requirements.

Good and bad examples of privacy notices
For organisations
PDF (208.99K)

Privacy notices under the EU General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are more detailed and specific than in the DPA and place an emphasis on making privacy notices understandable and accessible. Data controllers are expected to take 'appropriate measures'.

Data controllers may need to include more information in their privacy notices, but we believe that if you follow the good practice recommendations in this code you will be well placed to comply with the GDPR regime. There is still discretion for data controllers to consider where the information required by GDPR should be displayed in different layers of a notice.

The GDPR says that the information you provide to people about how you process their personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

These requirements are about ensuring that privacy information is clear and understandable for data subjects. They also make explicit what has always been set out as good practice. Following the advice in this code about the use of language, about adopting innovative technical means for delivering privacy information such as layered and just in time notices, and about user testing will help you to comply with the new provisions of the GDPR, as well as the current requirements of the DPA. The explicit emphasis on adapting privacy notices for children goes beyond what is currently required by the DPA. Data controllers processing children's data will need to take account of the level of comprehension of the age groups involved and tailor their notices accordingly. The code seeks to address this in relation to making privacy notices accessible.

The GDPR includes a longer and more detailed list of information that must be provided in a privacy notice than the DPA does. There are also some differences in what you are required to provide, depending on whether you are collecting the information directly from data subjects or from a third party.

Following the advice in the code about planning privacy notices and mapping your information flows will give you much of the detail you need to meet these requirements.

The following table summarises the privacy information you have to provide. It is taken from our Overview of the GDPR document.

	Data obtained directly from data subject	**Data not obtained directly from data subject**
What information must be supplied?	Not required when the data subject has the information.	Not required when the data subject has the information

		Not required when derogations in article 14(5)(b) to (d) apply. For example it would pose a disproportionate effort for archiving in the public interest.
Identity and contact details of the controller and where applicable, the controller's representative) and the data protection officer		
Purpose of the processing and the legal basis for the processing		
The legitimate interests of the controller or third party, where applicable		
Categories of personal data		
Any recipient or categories of recipients of the personal data		
Details of transfers to third country and safeguards		
Retention period or criteria used to determine the retention period		
The existence of each of data subject's rights		
The right to withdraw consent at any time, where relevant		
The right to lodge a complaint with a supervisory authority		
The source the personal data originates from and whether it came from publicly accessible sources		

Whether the provision of personal data part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data		
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.		
When should information be provided?	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

We will consider producing further guidance as appropriate on the specific categories of information listed here.