The right to be informed

The right to be informed

At a glance

- Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the DPA.
- You must provide individuals with information including:
  - who the data controller is; and
  - your purpose(s) for processing their personal data.

This is called “privacy information” and is usually communicated in a “privacy notice”.

- You must provide privacy information to individuals “as soon as reasonably practicable”, which generally means at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data, either directly or indirectly through a public notice, depending on the processing activity and the ability to directly notify the individuals.
- There are circumstances when you are not obliged to provide the privacy information.
- You should regularly review, and where necessary, update your privacy information. You must bring any new uses of an individual’s personal data to the attention of the individuals before you start processing their data.
- Getting the right to be informed correct can help you to comply with other aspects of the DPA and build trust with people, but getting it wrong can leave you open to fines and lead to reputational damage.

Checklist

What to provide

We provide individuals with all the following privacy information:

- The name and contact details of our organisation; and
- The purposes of the processing.

When to provide it

- We provide individuals with privacy information at the time we collect their personal data from them (or as soon as possible afterward if it is not reasonably practicable to give notice upfront).
- If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information within a reasonable of period (or make it easily accessible, e.g. on our website, if it is not reasonably practicable to directly contact the individual).

How to provide it

We provide the information in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

Changes to the information

- We regularly review and, where necessary, update our privacy information.
- If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice – drafting the information

- We undertake an information audit to find out what personal data we hold and what we do with it. The results may be recorded in a record of processing activities (RoPA).
- We put ourselves in the position of the people we're collecting information about.
- We carry out user testing to evaluate how effective our privacy information is.

Best practice – delivering the information

When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons; and
- mobile and smart device functionalities.

What is the right to be informed and why is it important?

The right to be informed covers a key transparency requirement of the DPA. It is about providing individuals with a privacy notice that contains clear and concise information about who you are and what you do with their personal data.

Using an effective approach can help you to comply with other aspects of the DPA, foster trust with individuals and obtain more useful information from them.

Getting this wrong can leave you open to complaints, investigation and fines, and may lead to reputational damage.

What privacy information should you provide to individuals?

You are required to provide:

- your own identity; and
- the purpose(s) of processing.

It is best practice (but optional under the DPA) to provide additional information, such as:

- your organisation's contact details;
- your representative's contact details (if applicable);
- the legal basis of processing (including statutory requirements if applicable);
- the legitimate interests of processing (if applicable);
- the categories of data obtained;
- the source of the data;
- the recipients or categories of recipients of the data;
- the details of any international transfers;
- the retention period of the data;
- the rights available to individuals;
- the right and contact details to make a complaint to the Ombudsman; and
- the details of any automated decision making.

What you should tell people differs slightly depending on whether you collect personal data from the individual it relates to or obtain it from another source.

Additionally, a lot of best practice information will be required information under a Subject Access Request (SAR). Consequently, you may be able to reduce the number of SARs you receive and need to respond to by having an expanded, best practice privacy notice.

When should you provide privacy information to individuals?

When you collect personal data from the individuals it relates to, you must provide them with privacy information as soon as reasonably practicable. In most cases this will mean before or at the time you obtain their data, but where it is not practicable to do so, you should provide the privacy information as soon as possible after you have collected their personal data.

When you obtain personal data from a source other than the individual it relates to, you need to provide the individual with privacy information as soon as reasonably practicable. This is not further specified in the Act, but is taken to mean within a reasonable period of time, such as within a month, whenever you first communicate with the individual, or whenever you first disclose the data to someone else.

You must actively provide privacy information to individuals. You can meet this requirement by putting the information on your website, but you must make individuals aware of it and give them an easy way to access it.

Where direct interaction with the individuals concerned is not possible or reasonably practicable, you should still take steps to make sure that your privacy information is at least readily and publicly accessible (e.g. through a privacy notice posted on your website).

What are the exemptions to the right to be informed?

When collecting personal data from individuals, you do not need to provide them with any information that they already have.

The DPA recognizes the following exemptions from the right to be informed:

- Section 19: the data is processed for crime prevention, detection or investigation, the apprehension or prosecution of any person suspected of having committed an offence, or the assessment or collection of any fees or duty;
- Section 21: the data is processed for monitoring, inspection or a regulatory function, to the extent that applying it would be likely to prejudice the discharge of the function;
- Section 23: the data is processed for statistical purposes or for the purposes of historical or scientific research;
- Section 24: the data consists of information you are obliged by the Act to make available to the public;
- Section 27: the data is processed for purposes of conferring any honor or dignity by the Crown or the Premier;
- Section 28: the data is processed for purposes of corporate finance and the application of the provision could affect the price of a financial instrument, or for the purpose of safeguarding an important economic or financial interest of the Cayman Islands;
- Section 29: the data consists of intentions in regard to any negotiations with the individual which would be prejudiced by the processing;
- Section 30: the processed data consists of information in respect of which legal professional privilege

applies and in respect of trusts and wills;
- Regulation 7: the notification could reasonably cause mental or physical harm to any person;
- Regulation 9: to the extent that the notification would be likely to prejudice the carrying out of social work because of serious harm to the physical or mental health or condition of any person.

For more details on these and other exemptions, see here.

How should you draft your privacy information?

An information audit or data mapping exercise can help you find out what personal data you hold and what you do with it.

You should think about the intended audience for your privacy information and put yourself in their position.

If you collect or obtain children's personal data, you must take particular care to ensure that the information you provide them with is appropriately written, using clear and plain language.

For all audiences, you must provide information to them in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

How should you provide privacy information to individuals?

There are a number of techniques you can use to provide people with privacy information. You can use:

- **A layered approach** – typically, short notices containing key privacy information that have additional layers of more detailed information.
- **Dashboards** – preference management tools that inform people how you use their data and allow them to manage what happens with it.
- **Just-in-time notices** – relevant and focused privacy information delivered at the time you collect individual pieces of information about people.
- **Icons** – small, meaningful, symbols that indicate the existence of a particular type of data processing.
- **Mobile and smart device functionalities** – including pop-ups, voice alerts and mobile device gestures.

Consider the context in which you are collecting personal data. It is good practice to use the same medium you use to collect personal data to deliver privacy information.

Taking a blended approach, using more than one of these techniques, is often the most effective way to

provide privacy information.

Should you test, review and update your privacy information?

It is good practice to carry out user testing on your draft privacy information to get feedback on how easy it is to access and understand.

After it is finalized, undertake regular reviews to check it remains accurate and up to date.

If you plan to use personal data for any new purposes, you must update your privacy information and proactively bring any changes to people's attention.

The right to be informed in practice

If you **sell** personal data to (or **share** it with) other organisations:

- As part of the privacy information you provide, you must tell people that you plan to sell or share the information, and also who you are giving their information to, unless you are relying on an exception or an exemption.
- You can tell people the names of the organisations or the categories that they fall within; choose the option that is most meaningful.
- It is good practice to use a dashboard to let people manage who their data is sold to, or shared with, where they have a choice.

If you **buy** personal data from other organisations:

- You must provide people with your own privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, it is best practice to carry out a privacy impact assessment to find ways to mitigate the risks of the processing.
- If your purpose for using the personal data is different to that for which it was originally obtained, you must tell people about this. It is best practice to also tell them what your legal basis is for the processing.
- Provide people as soon as practicable with your privacy information after buying the data.

If you obtain personal data from **publicly accessible sources**:

- You still have to provide people with privacy information, unless you are relying on an exception or an exemption.
- If you think that it is impossible to provide privacy information to individuals, it is best practice to carry out a privacy impact assessment to find ways to mitigate the risks of the processing.
- Be very clear with individuals about any unexpected or intrusive uses of personal data, such as combining information about them from a number of different sources. Remember that you still need a legal basis for the intended processing.

- Provide people with privacy information as soon as practicable after obtaining the data.

If you apply **Artificial Intelligence (AI)** to personal data:

- Be upfront about it and explain your purposes for using AI.
- If the purposes for processing are unclear at the outset, give people an indication of what you are going to do with their data. As your processing purposes become clearer, update your privacy information and actively communicate this to people.
- Inform people about any new uses of personal data before you actually start the processing.
- If you use AI to make solely automated decisions about people with legal or similarly significant effects, tell them what information you use, why it is relevant and what the likely impact is going to be.
- Consider using just-in-time notices and dashboards which can help to keep people informed and let them control further uses of their personal data.

Relevant provisions

Data Protection Act (2021 Revision)

Schedule 1, part 2, paragraph 2: Specified information at relevant time

Section 19(2): Exemption relating to crime, government fees and duties

Section 23(2): Exemption relating to research, history or statistics

Data Protection Regulations, 2018:

Regulation 7(1): Exemption relating to health

Regulation 9(1): Exemption relating to social work

Further guidance

Article 29 Working Party: Guidelines on Transparency under Regulation 2016/679

ICO: Guidance on the right to be informed

ICO: Guidance on Data Protection Impact Assessments