PRIVACY NOTICES QUICK GUIDE

The right to be informed

Contents

Publication date: May 2023

DATA PROTECTION NETWORK

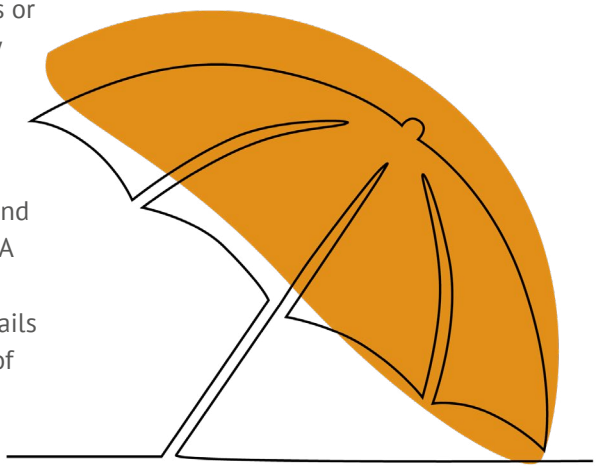
Why a privacy notice is needed

All businesses need an external facing privacy notice if they're collecting and handling people's personal information. And despite a common misconception, this doesn't just relate to data gathered via a website. Some may also have separate privacy notices for different groups of people, for example an employee privacy notice, one for job applicants and so on.

A core theme running through data protection law, be it UK or EU GPDR, is being upfront and open about how personal information is collected and what it's used for.

People have a fundamental right to be informed and one of the main ways organisations can meet this is by publishing a privacy notice.

Other methods can be used to provide people with information at the time you collect their data, for example just-in time notices, drop-down boxes or pop ups. These can specifically inform people why you need certain information, like a telephone number for instance.



A privacy notice is often referred to as a Privacy Policy. However, essentially it isn't a policy at all, and people shouldn't have to confirm they agree to it. A privacy notice is a notification about the different ways in which you'll handle people's personal details (your processing of 'personal data'). It's a method of providing necessary and legally required information.

Key considerations

Easy-to-understand

Data protection law (UK/EU GDPR) tells us privacy information must be 'concise, transparent, intelligible and easily accessible form, using clear and plain language'.

Avoid jargon

Try not to use overly technical terms or legal jargon which people might find difficult to understand.

Data protection terminology like profiling, controller, processor, personal data and so on, may not be easily understood. We need to explain things in plain, clear language.

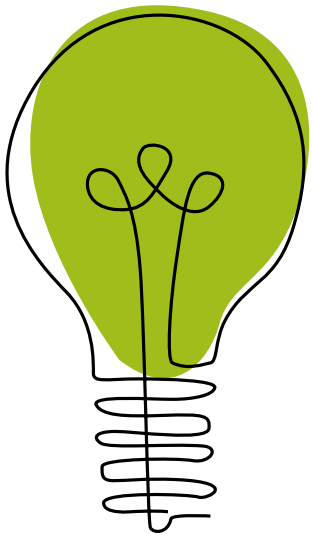
This can be easier said than done, so getting a good copywriter on board can really pay off.

Mandatory requirements

There's specific information which we're legally required to cover. These requirements are set out in UK/EU GDPR Articles 13 and 14 and a summary is provided below.

Complexity

The more complex your business activities are, the more detailed your notice(s) will need to be.



Layering / dashboards

For detailed notices using dashboards and/or a layered approach, where people can click to find out more detail, can make it easier for people to digest and navigate to the information they're seeking. Some businesses have gone a step further using icons, illustrations and short video explainers.

Your privacy notice may be the least visited page on your website, but you can be sure someone who wants to complain will study the detail. As will a Regulator if you fall under their spotlight. Prospective clients and partners may also scrutinise your privacy notice as part of their due diligence.

When done well, a Privacy Notice shows people you care about data protection.

Core legal requirements

There are seven key points which must always be covered in a privacy notice. The following is based on Article 13 of UK/EU GDPRs and guidance from the UK's Information Commissioner's Office.

The 7 essential elements

1. **Name and contact details of your organisation**
2. **Purposes of processing**

   What does this mean?

   Set out all the different ways in which people's personal information is used. This could be for marketing, research, providing goods or services, delivery, customer feedback, research and so on.

   The UK's Information Commissioner's Office (ICO) guidance says we should explain the types of personal data we collect and handle, such as contact details, financial information, health data or website statistics. And that we should also include how we collect personal data, be this directly or indirectly.

3. **Lawful basis for processing**

   What does this mean?

   For the different purposes you use personal information, you need a lawful basis – be it contract, legitimate interests, consent, public interest, legal obligation or vital interests. People should be informed as the lawful bases you rely on.
   See our Lawful Basis Guide.

   If you rely on legitimate interests as your lawful basis for certain purposes, you should explain what these are.

There should be no surprises about how we're using people's personal data. If we conduct wealth-screening, research, marketing segmentation and so on, we must tell people.

A Record of Processing Activities, can really help to inform what you put in your privacy notice. A RoPA is mandatory for all organisations with more than 250 employees or smaller businesses which handle large volumes particularly sensitive data.

It can be helpful to list your purposes for processing and your lawful basis together in a table within your privacy notice. At DPN our privacy notice is fairly straight-forward and you can see how we've used a table: Privacy Statement

4. **Data retention**

   Tell people how long you'll keep personal information for. If you can't be specific, explain how you decide retention periods.

   Data protection law tells us we shouldn't keep personal data longer than we need it, so we need to assess how long we need to keep it and clean out data we long longer have a justifiable use for. Data Retention Guide

5. **People's privacy rights**

   Tell people what their privacy rights are and how they can exercise them. For example the right of access, the right of erasure, objection and so on.

6. **Right to withdraw consent**

   When relying on consent as the lawful basis, people must be told they can withdraw their consent at any time.

   For example, if you rely on consent for email marketing, you should tell people how to stop receiving marketing communications in future. (In fact, the right to object to direct marketing by any means, is a fundamental right, so it's best to make sure its easy and clear how to say 'no more thanks').

7. **Right to lodge a complaint**

   Tell people they have the right to complain to the relevant Supervisory Authority (regulator), for example, the Information Commissioner's Office (ICO) in the UK.

6 points to include, when relevant

1. **Data Protection Officer**

   Provide contact details for your DPO (if you've appointed one). Remember not all businesses need one – DPO Myth Buster

2. **Data Protection Representative**

   If you're based outside the EU, but you offer services or monitor the behaviour of people based in the EU you should have a Data Protection Representative and provide contact details for them.

3. **Data sharing**

   Provide details of other organisations you share people's personal data with. This includes suppliers acting as processors, handling data on your behalf.

   ICO guidance states you can provide specific names, or at least should list the categories of organisation they fall within. Controller or Processor?

4. **International data transfers**

   Tell people if their personal data will be transferred to countries outside the UK (or if based in the EU, outside the EU). Explain whether transfers are based on an adequacy decision. If not provide a description of other safeguards in place, such as the UK's International Data Transfer Agreement or the EU's Standard Contractual Clauses (SCCs).

   This would apply for example, if you're a UK based company and use a supplier based overseas, which handles your data on your behalf to provide a service to you. International Data Transfers Guide

5. **Automated decision-making, including profiling**

   Tell people if you make solely automated decisions, including profiling which may have a legal or similar significant effect on individuals. Meaningful information should be provided about the logic involved, the significance and envisaged consequences.

6. **Statutory/contractual obligations**

   Let people know if you're required to collect their data by law or under contract, and the consequences should they not provide necessary information.

   There are some other best practices, such as indicating when the privacy notice was last updated and offering assurances around security.

Other factors to bear in mind

- **Data sourced indirectly:** The law tells us if we collect personal information from another source, i.e. not directly from the individual themselves, we need to make sure we tell them we're handling their personal data and provide privacy information.
- **Updates:** A privacy notice should be a living breathing document, not something which just gets written, published and forgotten about.
- **New activities:** Doing something new with data? Is the new purpose compatible with why you originally collected the data? Is it covered by what you say in your privacy notice?
- **Notify changes:** You'll need to take steps to try and notify people if you make significant changes to your privacy notice.
- **Records:** You may be required to demonstrate what privacy information was provided at the time someone gave you their details. It's therefore advisable to keep a record of previous versions and when they were live.
- **Rest of the world:** If you have customers in other territories, you may need to consider other privacy information requirements in other regions, for example under the Californian Privacy Act.

DATA PROTECTION NETWORK

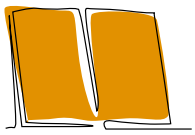
About DPN

Founded in 2014 we regularly publish news, insight and guides. Our experienced team work across a range of sectors providing tailored data protection training, data protection gap analysis reviews and helpdesk support.

Get in touch

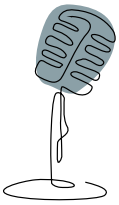
Consultancy

No-nonsense, practical data protection cunsultancy from our experienced team



Articles

News, insight and how-to-guides to support your day-to-day protection work



Events

Expert speakers share knowledge and tips on a range of privacy topics

Training

Down-to-earth data protection training workshops focused on developing your team's skills

Simon Blanchard
simon@dpnetwork.org.uk

Philippa Donn
phil@dpnetwork.org.uk

Sign up for DPN email updates
https://dpnetwork.org.uk/newsletter-sign-up/

www.dpnetwork.org.uk