Sample privacy notice document

The following provides a simple format for a data privacy notice. It is intended for business use and as a starting point only.

To comply with the requirements of the **General Data Protection Regulation (GDPR)**, you should customise this document to your specific requirements and business practices around privacy and data processing.

Disclaimer: This sample privacy notice does not constitute legal advice. The content is for general information purposes only. It is provided without any representations or warranties, express or implied. If necessary, seek appropriate legal counsel in relation to GDPR or your specific circumstances.

For definitive legal advice on providing privacy information under the GDPR, see the Information Commissioner's Office guide on privacy notices.

Privacy notice - format

Introduction

Begin with a brief general statement on:

- why privacy matters to you
- the information contained within the privacy notice (ie clear and concise summary)
- what services the notice applies to (eg website, software, purchases, subscription, etc)

You may include an encouragement for the user to read the policy carefully and contact you with any questions or concerns about your privacy practices.

Who we are?

Provide name and contact details of the data controller. This will typically be your business or you, if you are a sole trader. Where applicable, you should include the identity and contact details of the controller's representative and/or the data protection officer.

What information do we collect?

Specify the types of personal information you collect, eg names, addresses, user names, etc. You should include specific details on:

- how you collect data (eg when a user registers, purchases or uses your services, completes a contact form, signs up to a newsletter, etc)
- what specific data you collect through each of the data collection method
- if you collect data from third parties, you must specify categories of data and source
- if you process sensitive personal data or financial information, and how you handle this

You may want to provide the user with relevant definitions in relation to personal data and sensitive personal data.

How do we use personal information?

Describe in detail all the service- and business-related purposes for which you will process data. For example, this may include things like:

- personalisation of content, business information or user experience
- account set up and administration
- delivering marketing and events communication
- carrying out polls and surveys
- internal research and development purposes
- providing goods and services
- legal obligations (eg prevention of fraud)
- meeting internal audit requirements

Please note this list is not exhaustive. You will need to record all purposes for which you process personal data.

What legal basis do we have for processing your personal data?
Describe the relevant processing conditions contained within the GDPR. There are six possible legal grounds:

- consent
- contract
- legitimate interests
- vital interests
- public task
- legal obligation

Provide detailed information on all grounds that apply to your processing, and why. If you rely on consent, explain how individuals can withdraw and manage their consent. If you rely on legitimate interests, explain clearly what these are.

If you're processing special category personal data, you will have to satisfy at least one of the six processing conditions, as well as additional requirements for processing under the GDPR. Provide information on all additional grounds that apply.

When do we share personal data?
Explain that you will treat personal data confidentially and describe the circumstances when you might disclose or share it. Eg, when necessary to provide your services or conduct your business operations, as outlined in your purposes for processing. You should provide information on:

- how you will share the data
- what safeguards you will have in place
- what parties you may share the data with and why

Where do we store and process personal data?
If applicable, explain if you intend to store and process data outside of the data subject's home country. Outline the steps you will take to ensure the data is processed according to your privacy policy and the applicable law of the country where data is located.

If you transfer data outside the European Economic Area, outline the measures you will put in place to provide an appropriate level of data privacy protection. Eg contractual clauses, data transfer agreements, etc.

How do we secure personal data?
Describe your approach to data security and the technologies and procedures you use to protect personal information. For example, these may be measures:

- to protect data against accidental loss
- to prevent unauthorised access, use, destruction or disclosure
- to ensure business continuity and disaster recovery
- to restrict access to personal information
- to conduct privacy impact assessments in accordance with the law and your business policies
- to train staff and contractors on data security
- to manage third party risks, through use of contracts and security reviews

Please note this list is not exhaustive. You should record all mechanisms you rely on to protect personal data. You should also state if your organisation adheres to certain accepted standards or regulatory requirements.

How long do we keep your personal data for?
Provide specific information on the length of time you will keep the information for in relation to each processing purpose. The GDPR requires you to retain data for no longer than reasonably

necessary. Include details of your data or records retention schedules, or link to additional resources where these are published.

If you cannot state a specific period, you need to set out the criteria you will apply to determine how long to keep the data for (eg local laws, contractual obligations, etc)

You should also outline how you securely dispose of data after you no longer need it.

Your rights in relation to personal data
Under the GDPR, you must respect the right of data subjects to access and control their personal data. In your privacy notice, you must outline their rights in respect of:

- access to personal information
- correction and deletion
- withdrawal of consent (if processing data on condition of consent)
- data portability
- restriction of processing and objection
- lodging a complaint with the Information Commissioner's Office

You should explain how individuals can exercise their rights, and how you plan to respond to subject data requests. State if any relevant exemptions may apply and set out any identity verifications procedures you may rely on.

Include details of the circumstances where data subject rights may be limited, eg if fulfilling the data subject request may expose personal data about another person, or if you're asked to delete data which you are required to keep by law.

Use of automated decision-making and profiling
Where you use profiling or other automated decision-making, you must disclose this in your privacy policy. In such cases, you must provide details on existence of any automated decision-making, together with information about the logic involved, and the likely significance and consequences of the processing of the individual.

How to contact us?
Explain how data subject can get in touch if they have questions or concerns about your privacy practices, their personal information, or if they wish to file a complaint. Describe all ways in which they can contact you – eg online, by email or postal mail.

If applicable, you may also include information on:

Use of cookies and other technologies
You may include a link to further information, or describe within the policy if you intend to set and use cookies, tracking and similar technologies to store and manage user preferences on your website, advertise, enable content or otherwise analyse user and usage data. Provide information on what types of cookies and technologies you use, why you use them and how an individual can control and manage them.

Linking to other websites / third party content
If you link to external sites and resources from your website, be specific on whether this constitutes endorsement, and if you take any responsibility for the content (or information contained within) any linked website.

You may wish to consider adding other optional clauses to your privacy policy, depending on your business' circumstances.