PRIVACY NOTICE AND CONSENT TEMPLATE

Privacy Notice and Consent template guidance

How should I use my private notice and consent template?

This document includes a series of templates your company can use to develop your own privacy statement and consent collection notice.

Will I need to update my due diligence checklist?

Yes. Your company is obligated under GDPR to display a privacy statement. You should review this checklist at least every 3 months and amend as necessary to ensure your company is complying with GDPR.

Privacy notice template

Your privacy notice is considered one of the most complex but crucial aspects of GDPR compliance. To help you to better understand your privacy notice and obligations under GDPR, we've broken this guidance document down into two sections:

A. General guidance
B. Privacy notice template

A. General guidance

Under GDPR, your company must provide explicit privacy information to any and all data subjects. These privacy statement stipulations are more specific and contain stronger specifications than what was previously expected of UK companies under the Data Protection Act 1998.

First and foremost, it's worth noting a privacy statement absolutely must be supplied by your company to any relevant individual at the point in time that they provide to you or submit their personal data. More important still, the statement that your company provides those individuals with must be:

- Concise
- Transparent
- Easily accessible
- Written in plain language
- Free of charge to access and read

Please note that additional rules are required if your privacy statement is designed for and/or directed at children.

To help you develop your privacy statement that complies with all of your GDPR obligations, we've compiled the following guidance sections.

Name and details of Data Controller

You must identify the name and contact details of the relevant data controller within your privacy statement. Here is an example of how your company may wish to outline these details:

[NAME OF DATA CONTROLLER] is the designated data controller for [COMPANY NAME] and committed to upholding our commitments to protect the rights of individuals under legislation outlined within the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Name and details of data protection officer

You must identify the name and contact details of the relevant data protection officer within your privacy statement. Here is an example of how your company may wish to outline these details:

[COMPANY NAME] has an appointed data protection officer [DATA PROTECTION OFFICER NAME] to assist us in upholding our commitment to individual rights. Our data protection officer can be contacted both through our website [COMPANY WEBSITE URL], as well as by post [COMPANY ADDRESS].

Description of the data being collected

Your company must explicitly describe the personal data you are collecting, storing or processing.

As a reminder, GDPR defines ‘personal data’ as being any type of information that includes an individual’s:

- Name
- Location
- Any sort of identification number
- Any online identifiers
- Any physical identifiers
- Any attribute that could reveal their social identity

The aforementioned data types should also be applied to include any personal data surrounding employees, students or other stakeholders and clients.

This data includes:

- Name
- Date of birth
- Address
- Telephone number
- Email address
- Role
- Emergency contacts
- Passport or other identification

There are also special categories of personal data called sensitive personal data. This type of data generally includes information like:

- Race or ethnic origin
- Religion
- Sexual orientation
- Political affiliations
- Trade union affiliations
- Genetic or biometric data
- Health information

Sensitive data

If your company collects sensitive data, your privacy statement must explicitly outline what information you are collecting, where you are going to store it and how you are going to store it.

Here is an example of how privacy statement must address this responsibility:

"*[COMPANY NAME] must collect the following sensitive data about you so that we can deliver [INSERT REASON FOR PROCESSING]:*

- *[LIST SENSITIVE INFORMATION REQUIRED]*

[COMPANY NAME] needs your explicit consent for processing this sensitive data. We must request your signature for this consent."

If your company does not collect sensitive data, you should state this within your privacy statement instead.

The age of consent for children

GDPR defines the point at which an individual is no longer considered a child is 16 years of age. That being said, GDPR empowers all EU member states to amend this age to either 13, 14 or 15 years old at their own discretion.

Bearing this in mind, data controllers are required to be aware of the age of consent in concerned member states. They are not permitted to seek consent from any individual under the specified age of consent within that individual member state.

If your company needs to obtain consent to collect, store or process the data of a child, you are permitted only to obtain consent to collect, store or process that data from an individual who holds parental responsibility for the concerned child. Your company must subsequently make reasonable efforts to verify the individual granting consent on the behalf of a child actually does hold parental responsibilities.

Privacy statements for children

If your company is offering services directly to a child, then relevant data controllers within your company must do everything they can to ensure that your company's privacy statements are written in a comprehensive and plain fashion that a child will be able to understand.

Online services being offered to children

The vast majority of consent requests your company will likely be required to collect, will be in relation to the provision of online services. Examples of online services could include provisions such as:

- Online stores
- Streaming services
- Social networking

The aforementioned rules in relation to the age of consent and corresponding privacy statements apply to most online services being offered. One exception to this is if your company is processing data relating to preventative or counselling services being offered directly to a child. Under such a circumstance, you do not need to seek consent from a parental figure.

Why data is processed

Your company must outline all of the reasons for processing data. Examples of processing reasons might include:

A. Financial administration
B. The provision of support services
C. The provision of information services
D. Account management
E. Equal opportunities monitoring
F. Research and analysis
G. The provision of operational information
H. Marketing
I. Safeguarding
J. Security
K. Crime prevention
L. To protect legitimate interests

You must state in your privacy policy any situations in which automatic decisions or actions are made within your company in relation to data.

Your company should also include a broad description of the ways in which you plan to use personal data, and the legal grounds supporting your ability to do so.

Furthermore, your privacy statement should also include a line similar to the following:

"[COMPANY NAME] only uses personal data for the reasons in which we have collected. We will only ever use your personal data for another reason if we reasonably consider another purpose in which to use that data which is compatible with the original reason in which the data was collected.

If we are required to make such a decision, we will always notify you. We may also at times be required by law to process your personal data without your knowledge.

To find out more about the reasoning behind any decision [COMPANY NAME] has made to process your data for a new purpose, get in touch."

If your company plans on using personal data for marketing purposes, you must explicitly say so. An example of how you may wish to convey this within your privacy statement could include:

"You may receive marketing communications from [COMPANY NAME] if you have:

- *Requested information from us*
- *Purchased goods or services from us*
- *Provided us with explicit consent for us to send you marketing communications*
- *Not opted out of receiving marketing communications*

We will always ask for your consent before we share your personal data with any third-parties. You can ask us or any relevant third-parties to cease sending you marketing communications at any time, by emailing us. You should send relevant requests to [DATA PROTECTION OFFICER EMAIL ADDRESS].

Please note that if you opt out of receiving marketing communications from [COMPANY NAME], your personal data may still be retained as it relates to the provision or purchase of a product and/or service, warranty registration or other transactions."

Legal basis for processing personal data

To comply with your legal responsibilities under GDPR, your company must identify the lawful basis upon which you are processing an individual's personal data.

You must satisfy at least one condition under Article 6 of GDPR if you are processing personal data. If you are processing special category data, you must satisfy at least one condition under both Article 6 and Article 9.

Relevant conditions of these articles are outlined below:

Article 6: Personal Data	Article 9: Special Categories
Individual has given consent	Individual given explicit consent
Processing is required for delivery of contract	Processing is required to carry out obligations of controller or employment
Processing is required for legal compliance	Processing is required to protect vital interests of individual unable to provide consent

Processing is required to protect vital interests of the individual	Processing is required for legitimate activities by a foundation, association or any other non-profit with a political, philosophical, religious or trade union aim
Processing is required for a task that is in the public interest	Processing relates to personal data that has already been made publicly available by the individual
Processing is required for legitimate interests by controller or third party	Processing required to establish, exercise or defend against legal claims
	Processing is required for reasons of substantial public interest
	Processing is required for occupational medicine, the assessment of the working capacity of the employee, medical diagnosis, the provision of treatment or the management of health or social care systems
	Processing is required for reasons of public interest in public health
	Processing is required for achieving aims that are in the public interest or for scientific, historical or statistical purposes

If your company would like to utilise the legitimate interests basis, you must satisfy the following requirements:

- Your company must process data for the purposes of your legitimate interests or for those of a third-party to whom you disclose it
- Once the latter requirement has been met, the interests listed must be balanced against the rights of the concerned individual

Your company cannot rely on the legitimate interests basis in situations where the processing is unwarranted or has a prejudicial effect on an individual's rights or freedoms, as well as the legitimate interests of the individual. If your company's legitimate interests clash with those of the data subject, it is the legitimate interests of the data subject that will ordinarily be given precedence.

For every type of personal data you process, you should provide a description of the ways you intend to use this data, and the legal grounds for doing so. You should also explain the legitimate interests you have to process this data, where relevant. An example of holding this information is as follows:

Action	**Data/Information type**	**Legal grounds for processing**
Processing the delivery of products or services ordered, and actively managing the payments and debt recovery processes	(1) Personal identifiable information (2) Contact information (3) Financial information	(1) To complete the contractual agreement (2) Required for our legitimate interest of recovering any funds owed to us after the delivery of products or provision of services
Updating customers on any amendments to our terms and conditions or privacy policy	(1) Personal identifiable information (2) Contact information	(1) To complete the contractual agreement (2) Required to satisfy legal requirements
Registering a new customer	(1) Personal identifiable information (2) Contact information	(1) To complete the contractual agreement
Protecting our business and websites by performing website tests, applying security updates, assessing any cybersecurity threats and analysing our databases	1) Personal identifiable information (2) Contact information (3) Website and Technical information	(1) Required to satisfy legal requirements (2) Required for our legitimate interest of protecting our websites and business from malicious usage, to prevent cybercrime, complete technical website audits and increase our network security
Emailing customers to request feedback or participation in a prize draw	(1) Personal identifiable information (2) Contact information (3) Product usage information (4) Marketing information	(1) To complete the contractual agreement (2) Required to satisfy legal requirements (3) Required for our legitimate interest of studying how customers interact with our products and services offered, and how these can be further enhanced

The Data Recipients

Your company needs to explicitly state all of the recipients of data, as well as all of the recipients of categories of data. For the purposes of your company's privacy statement, a recipient can be actively defined as a natural or legal individual, public authority, agency or any other organisation to which personal data is submitted. This includes organisations that are third-parties, as well as subservient organisations within your company.

An example of the type of messaging you may wish to include in your privacy statement could run along the following lines:

"[COMPANY NAME] may be required to share your personal data with carefully selected third-parties for the identified processing purposes. These third parties may include:

A. *IT or system administration services providers*
B. *Professionals providing banking, legal, accounting, consultancy and/or insurance services.*
C. *Government regulators based in the United Kingdom and other relevant jurisdictions*
D. *HM Revenue & Customs*
E. ***[INSERT ANY THIRD PARTY YOUR MAY SHARE DATA OR DATA CATEGORIES WITH]***
F. *Any existing or future third parties to which [COMPANY NAME] may sell, transfer or merge aspects of our business or assets*

All third parties to which we transfer data are required to respect your personal data, keep it secure and process it only for the specified purposes for which it has been collected. Third parties will only ever receive or process your data with our explicit permission."

Data transfers to countries outside the EU

If your company plans to transfer personal data to outside the EU, you must specify why that transfer is necessary, where the data will be transferred and to whom it will be transferred.

Data Retention Periods

Your company must state a specific retention period for which personal data will be stored. If it is not possible to share an explicit retention period, you must share the criteria that will be used to determine any retention period.

Automated decision-making processes

If your company will use data as part of an automated decision-making process, you must state the existence of those processes, the logic involved, and any consequences associated with those processes as they relate to personal data.

Where/how data is collected

In instances in which your company has not obtained personal data from the data subject directly, you must cite who this data was obtained from.

Individual rights

Your company has an obligation to inform individuals about their rights under GDPR. This includes their right to access and port data, their right to rectify incorrect data, restrict use, object to processing or withdraw consent.

An example of how your company may wish to explain this within your own privacy statement could run as follows:

"[COMPANY NAME] respects your rights. We fully observe your right to access your personal data, to object to the processing of personal data, or to erase, restrict, rectify or port your personal data. Relevant requests can be made to [DATA CONTROLLER] at [COMPANY ADDRESS]."

Visit us online at [COMPANY WEBSITE URL] for further details relating to your individual rights."

Information security

If you collect, store or process personal data, you must explain the security measures your company has in place to protect that data.

An example of how your company may wish to explain this within your own privacy statement could run as follows:

"[COMPANY NAME] has implemented a series of security measures to make sure that your personal data is protected from accidental loss, unauthorised access, alteration or disclosure. [COMPANY NAME] limits access to your data only to those employees, agents, contractors or other third parties with a legitimate reason to access that information. Those individuals or organisations will only ever process or access your personal data upon our explicit instructions. They are subject to a duty of confidentiality."

Complaints

You must provide individuals with a complaints procedure if they are not content with the way in which their personal data has been collected, stored or processed.

An example of how your company may wish to explain this within your own privacy statement could run as follows:

“If you are not happy with how your personal data has been processed, you should contact [DATA CONTROLLER NAME] in the first instance by using the contact details listed above. If [DATA CONTROLLER NAME] is unable to satisfy your concerns, you have the right to apply to the Information Commissioner’s Office for a resolution.

You can contact the Information Commissioner’s Office at the following address:

Information Commissioner’s Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
www.ico.org.uk ”

B. Privacy notice template

Please note the following privacy notice is a template only. Particular sections of this template may or may not apply to your business, and you may be required to add new sections, statements or information based upon your own unique company needs or data requirements.

Frequently asked questions

Who is using my data?	[COMPANY NAME]
What is my data being used for?	[COMPANY NAME] stores and processes data to help us maintain your account, process and store transaction details, offer customer support, send system updates and send offer details.
What will happen to my data?	[COMPANY NAME] may use your data to send you information, updates and offers we think you'll be interested in.
What data will be kept and stored?	[COMPANY NAME] stores registration details, transaction details, usage information and any information about your web preferences on our website.
What data will be shared with others?	We only share your data with regulators or government bodies if requested.
How long will my data be kept for?	[COMPANY NAME] will store your data for a period of [RETENTION PERIOD] after your last attempted login. After this period, your account will be deleted. You can request your account to be delete at any time.
Who will be able to access my data?	[COMPANY NAME] will never sell or share your data to any third-party, unless you grant us your explicit permission to do so.
How will my data be kept and made secure?	[COMPANY NAME] stores your data on secure servers that are based in the UK. Data is processed in the UK, and we use standard industry security protocols.

Privacy **Notice**

Date: [DATE OF COMPLETION]

[COMPANY NAME] takes your privacy seriously. That is why we will only use your personal information to provide you with the products and services you have requested, as well as to administer your account. We will not sell or share your information with third-parties you grant us explicit permission to do so, and we will never use your personal data for any reason other than the reasons described within this policy.

About our privacy policy

Our privacy policy outlines your relationship with our company and explains in detail how we use the information that you provide us with.

About [COMPANY NAME]

[COMPANY NAME] is the trading name of [COMPANY NAME], which is registered in [COUNTRY OF INCORPORATION] and registered with the UK's Information Commissioner's Office under the Data Protection Act 2018. Our data controller is [NAME OF DATA CONTROLLER], and we encourage you to get in touch with any questions you may have about [COMPANY NAME].

You can reach us by:

- Post: [ADDRESS]
- Telephone: [PHONE]
- Email: [EMAIL]
- Website: [URL OF COMPANY WEBSITE]

Changing your preferences

If you'd like to change your web, contact or marketing preferences, you can do so at any time. Simply contact us at [EMAIL ADDRESS] to request the necessary amendments.

How we do business

[COMPANY NAME] is committed to upholding and maintaining your personal rights. We operate our business in-line with the European Union's General Data Protection Regulation and observe your rights to change or withdraw your opt-in options at any time. As part of our ongoing commitment to uphold your rights, [COMPANY NAME] will also extend advice on how you can issue formal complaints to relevant authorities, such as the Information Commissioner's Office.

Sensitive data

[COMPANY NAME] does not collect any sensitive data about you. Sensitive data refers to (but is not limited to) information about your race or ethnic background, religious or political affiliations, trade union affiliations, sexual orientation, criminal background or health background.

Who our privacy policy applies to

This privacy policy has been developed to inform users of [COMPANY NAME] how we use their data. [COMPANY NAME] is a [DESCRIPTION OF BUSINESS], and we need to process the data of individuals to offer our products and/or services. Bearing that in mind, our privacy policy applies to any and all individuals registered with us as a user, customer, administrator or in any other capacity.

What information this policy applies to

There is a lawful basis for processing your data, and this section of our privacy policy outlines how this applies to the personal information you provide us with or allow us to collect.

The information this policy applies to includes information that you:

- Provide as part of any registration process
- Provide as part of any campaign creation activity
- Provide in the form of numerical data, metadata or communications
- Give us as part of our ongoing relationship

This policy also applies to information that we:

- Collect relating to how you interact with our website
- Must process to complete purchases and other transactions

Consent

Please note that when you submit personal data on our website, you are giving [COMPANY NAME] your explicit consent that we can use that data in line with our privacy policy.

Opting-out

After giving [COMPANY NAME] your consent, you are free to amend your consent or withdraw your consent at any time. You have the right to object to the processing of your data. To opt-out, change your preferences or revoke your consent, simply contact us by emailing [DATA PROTECTION OFFICER EMAIL ADDRESS].

Data processing and storage

[COMPANY NAME] collects and stores data in the UK. We will store your data for a period of [RETENTION PERIOD] after your last recorded login attempt unless otherwise noted and explicitly stated.

[COMPANY NAME] stores data relating to transactions, payments and orders for a period of up to seven years. This period may be extended under certain circumstances as part of our ongoing commitment to comply with UK and international law.

We use carefully selected and recognised third-parties to help us take payments, provide commerce services and manage company accounts. Some of these third-parties may operate outside the European Union.

[COMPANY NAME] may process your data based on more than one legal ground.

Circumstances under which we may be required to process your data under more than one legal ground may include:

Reason	Data type	Legal basis
Customer registration	Identity and contact information	To carry out a contract we've made with you
Processing and/or delivering your order	Identity, contact information, financial information, financial and transactional data	To carry out a contract we've made with you and to exercise our legitimate interests to recover debts owed
To manage our customer relationship with you	Identity, contact information, marketing and communications preferences	To carry out a contract we've made with you, to comply with legal obligations and to exercise our legitimate interests to keep our records updated

Marketing and communications

[COMPANY NAME] may send you marketing communications if you have given us your contact details and opted-in to marketing communications.

You can opt-out of these marketing communications and manage your preferences at any time.

Our company obligations

As a data controller, [COMPANY NAME] is legally responsible for the data you provide us with. In honouring that responsibility, we pledge to uphold our commitments under GDPR and the Data Protection Act 2018.

We will only ever use your data:

- In ways that are both fair and legal
- As described within this policy
- In ways that are necessary for the purposes described

In addition, [COMPANY NAME] processes the personal data you submit to us or we collect as a data processor. As part of this role, [COMPANY NAME] takes all necessary precautions to secure the personal data we collect, process and store.

We may occasionally use the data you provide us with for marketing, relationship management or account management activities. These activities are designed to ensure you have adequate information about other products and/or services we offer, that we have reason to believe you may be interested in. You have the right to opt-out of these activities at any time.

Third-Parties

[COMPANY NAME] never shares your personal data with third-parties unless those parties have been explicitly mentioned within our privacy statement.

Our security

As part of our ongoing commitment to GDPR, [COMPANY NAME] will report any security breaches or attempted breaches to the relevant authorities within 24 hours. We will subsequently contact all those affected by the breach within 72 hours of its occurrence.

Legitimate interests

As part of the Data Protection Act 2018, [COMPANY NAME] observes the right to share selected information with third-parties that use data for non-marketing purposes. This could include (but is not limited to) organisations that provide credit assessments, identification services and fraud prevention activities.

Contact us

[COMPANY NAME] is committed to upholding your rights. If you have any questions, comments or concerns about this privacy policy or wish to exercise your rights in relation to your personal data, please contact [NAME OF DATA PROTECTION OFFICER] at [COMPANY NAME].

We will process any request within 20 days. Subject Access Requests are normally performed free of charge, but we may need to charge individuals for excessive or unreasonable data requests.