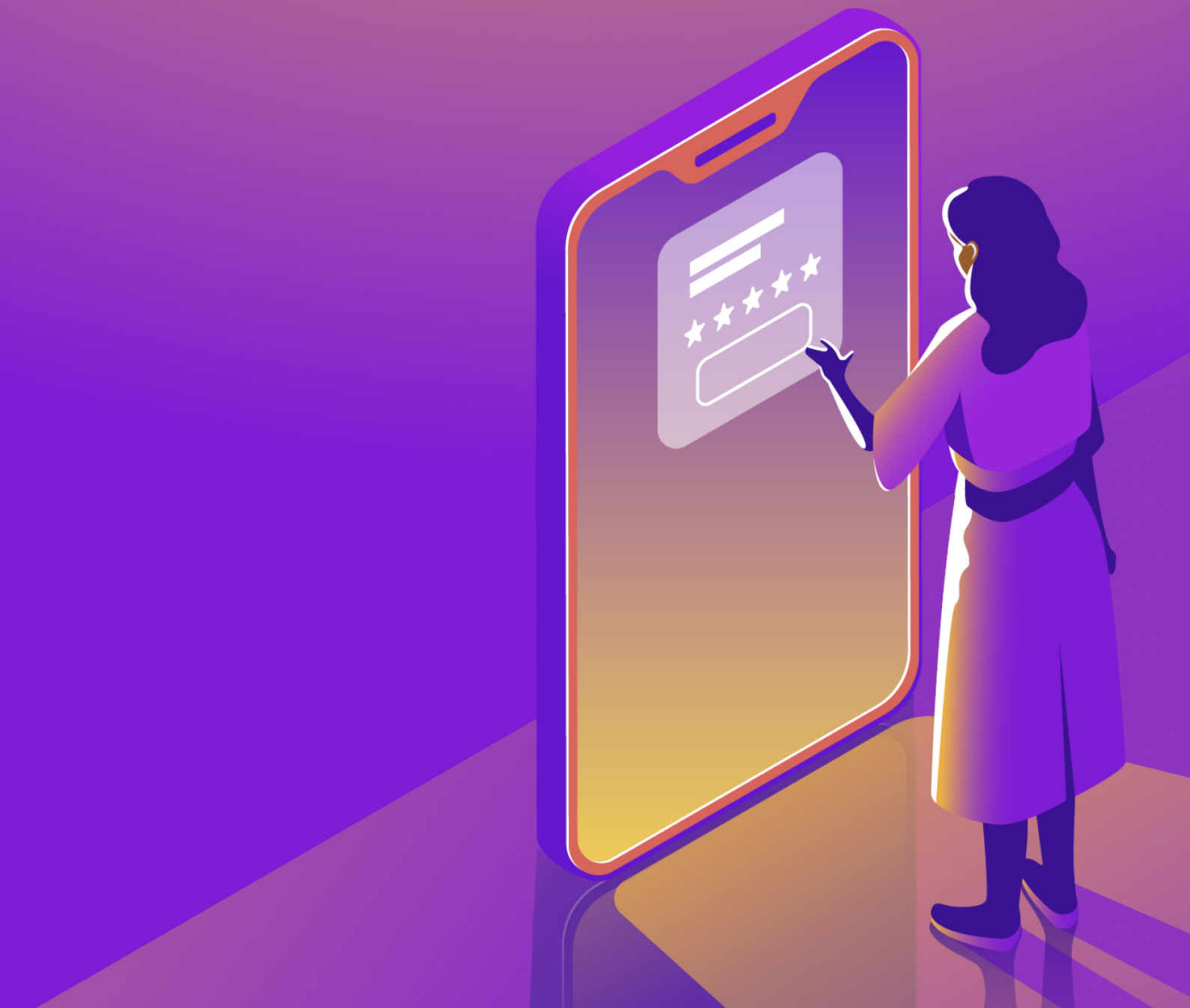
Getting to grips with

GDPR



Nearly all organisations deal with information that is described as ‘personal data’. Many of us have heard of something called ‘GDPR’. But how many of us understand what it is, and feel confident about complying with it? ‘GDPR’ stands for ‘General Data Protection Regulation’.

This booklet should help demystify some of the language around GDPR and help you and your company get to grips with the legislation.

Who is involved in GDPR compliance?

GDPR has created a number of new roles or new terms for existing roles.

Data Subject

The citizens of the EU using goods and services provided by the data controllers.

Data Controller

Decides the purpose and methods of processing personal data. They decide what should be collected and how it should be collected.

Data Processor

Responsible for directly processing personal data based on the instructions of data controllers. This could include third parties or subcontractors.

To take a chain of gymnasiums as an example. The members of the gym are Data Subjects. The company that owns the gymnasiums decides what data it needs to run its business and how this should be collected – they are the Data Controllers. The web developers who capture the data at the owners behest are the Data Processors.

In addition, some businesses have further requirements...

Data Protection Officers (DPO)

GDPR introduces a duty for you to appoint a data protection officer (DPO) if your business carries out certain types of processing activities.

DPOs must be appointed If your business is any of the following:

1.Public authorities

2. Organisations that engage in large-scale systematic monitoring

3. Organisations that engage in large scale processing of sensitive personal data

If your organisation doesn't fall into one of these categories, then you do not need to appoint a DPO.

Who enforces GDPR?

ico.
Information Commissioner's Office

In the UK, the Information Commissioner's Office (ICO) is responsible for enforcing the GDPR laws. The ICO has the power to conduct criminal investigations and issue fines. It is also provides organisations guidance about how to comply with GDPR.

What are the rights of Data Subjects?

GDPR grants people, in their capacities as consumers, citizens and so forth a range of specific data subject rights they can exercise under particular conditions.

Right of Data Breach Notification

In case of any data breach that is likely to result in unauthorised use and distribution of data, the Data Controllers will have to notify Data Subjects about the breach within 72 hours of becoming aware of the same.

Right to Access

GDPR gives Data Subjects the right to get information about how, where and for what purpose their personal data is being processed.

Right to be Forgotten

Also known as Data Erasure, the right to be forgotten entitles the Data Subject to have his/her personal data deleted from the logs of Data Controllers. The right to be forgotten also enables them to halt or cease further distribution and use of the data by third parties.

Right to Data Portability

GDPR introduces data portability — the right for a Data Subject to receive the personal data concerning them, which they have previously provided in a commonly used and machine-readable format and have the right to transmit that data to another Controller.

Right to Restrict Processing

Data subjects have the right to restrict the processing of personal data where:

- they have contested its accuracy;
- they have objected to the processing and you are considering whether you have a legitimate ground which overrides this;
- processing is unlawful;
- a business no longer needs the data but the data subject requires it to establish, exercise or defend a legal claim.

If a business has disclosed the personal data to third parties, then the business must inform them about the erasure of the personal data.

Right to Object

Data subjects have the right to object to:

- processing based on legitimate interests, the performance of a task in the public interest or the exercise of official authority (including profiling);
- direct marketing (including profiling); and processing for scientific/historic research or statistics.

GDPR Principles

The way you handle personal information must follow these 7 principles:

1 Transparency

Personal data must be processed in a lawful and transparent manner, ensuring fairness towards the individuals whose personal data you are processing.

2 Purpose Limitation

You must have specific reasons for processing the data and you must highlight those purposes to individuals when collecting their personal data. The act of simply collecting data for no purpose is no longer permitted.

3 Data Minimisation

You must only collect data related to fulfilling your specific reasons.

4 Accuracy

You must ensure the accuracy of the data, and directly relate that to your specific reasons.

5 Storage Limitation

The collected data should be stored for not longer than necessary to fulfil the purposes for which it was collected.

6 Integrity and Confidentiality

Appropriate technical and organisational safeguards must be in place to ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, damage or destruction.

7 Accountability

All organisations who process personal data must demonstrate compliance with each of the above Principles

Creating an online Privacy Policy

Privacy Polices are a legal requirement of any organisation handling data. For most companies, the most efficient way to notify data subjects of your policy is through your company website but privacy policies may also be provided by email or hard copy.

Under GDPR, business are obliged to notify individuals of what, how and why their personal data will be used and processed before collecting any personal data. If your organisation collects personal data on individuals, it needs a privacy policy on the company website.

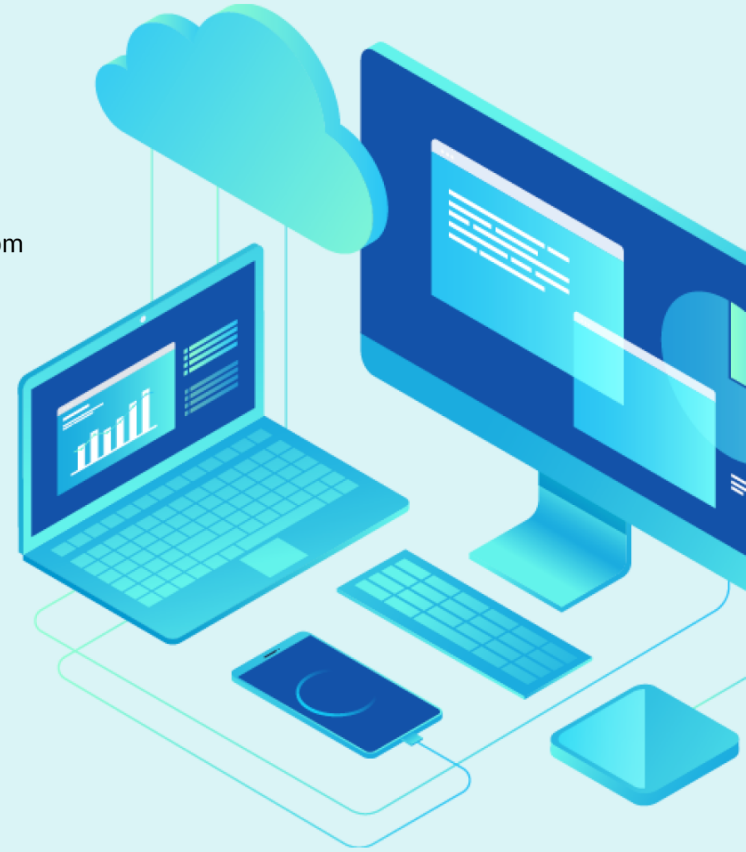
How should I write my Privacy Policy?

Your policy needs to written using clear and plain language. It has to cover all the data collection aspects of your website, including analytics and tracking for example.

What are the key points to ensure my Privacy Policy is GDPR compliant?

Before collecting any personal data, the following points should be covered in your Privacy Policy:

- Your company information, including full name, registered office details and business address
- Identity and contact details of the data controller and, where applicable, of the controller's representative
- What information you are collecting and why
- How consent will be obtained
- How you will be using the information collected
- How long the personal data will be kept for
- Explanation for how complaints can be made and to whom
- The contact details of the Data Protection Officer, where applicable
- Information about export of the collected data



Where must the Privacy Policy be displayed?

Your policy needs to be displayed in a prominent position on your website on every page - it should not be hidden away in sections such as 'Contact Us', for example.

How can you ensure your company is GDPR compliant?

There are five phases of work that can help ensure that your company is compliant with GDPR.