GDPR

explained for small businesses

lawbite

Understanding your legal requirements under GDPR can be confusing due to the sheer volume of guidance available and the ever-evolving nature of the laws surrounding it.

As a small business owner, it's important not to feel too intimated by GDPR laws. Once you grasp a few basic principles, it's just a case of seeing how they apply to your company and following the correct procedures to ensure your compliance.

To help you gain a better insight into GDPR and your legal requirements, we've put together this guide which should answer some of the most commonly asked questions.

TABLE OF CONTENTS

What is GDPR?

The General Data Protection Regulations (GDPR) gives rights to individuals and relates to their personal data. This, in turn, means that organisations bear a regulatory burden and have obligations and responsibilities to ensure that an individual's personal data is protected.

Since GDPR became law, large, medium and small businesses have been getting to grips with its various requirements, including having appropriate procedures, data security arrangements, compliant privacy policies and contracts.

In respect of your business, you may have asked yourself, or you have been asked, the question (or something to the effect of):

- Does the GDPR apply to my business?
- Does my business process personal data?
- What exactly is data processing?
- What is a lawful basis for processing?

In this section, we cover these key questions.

What is personal data?

Personal data is any information relating to an identified or identifiable natural person (i.e. a living human being). GDPR refers to such persons as "data subjects".

Examples of such information relating to a person include:

- Their name
- Email address
- Place of residence
- Date of birth
- Telephone number
- Place of work
- Salary or bank details

Further examples can include:

- Opinions about a person
- Preferences
- Feedback
- Disciplinary records
- Appraisals
- Email conversations (mainly where people are being discussed).
- Location (based on where a person's device is)
- Website cookies (and similar types of web or app trackers)
- IP addresses

The definition of personal data is purposely extensive, intending to capture a wide range of information which could somehow build a profile, story, or understanding about a person. This means something that reveals their physical or physiological attributes, genetic makeup, mentality, economic situation, culture, expressions, views or behaviour.

Only data that is truly anonymous or data that has had an individual's identity permanently removed (and rendered incapable of identifying an individual) is not considered personal data. GDPR is not concerned with anonymised data.

What is data processing?

Data processing or "Processing" is also broadly defined. It is essentially any operation performed on personal data. The list of examples is long and includes:

- Collecting
- Recording
- Organising
- Structuring
- Storing
- Hosting
- Altering
- Retrieving
- Consulting
- Using
- Making available
- Combining
- Restricting
- Deleting (or erasing)

Does the UK GDPR apply to my business?

It is very likely, yes.

Any UK business processing personal data is caught by the UK GDPR (we'll come onto what UK GDPR is soon) and is required to comply with its requirements.

As long as your business has customers, staff, or contacts, it will likely be processing data. This means practically all organisations in the UK are subject to the UK GDPR and require a legal basis for processing personal data.

In practice, you'll most likely be processing personal data in many of your routine activities:

- Sending an email or chat message to a colleague or client is data processing
- Attaching files
- Handling spreadsheets
- Using software

The above also means that you're data processing under the UK GDPR.

Organisations, of course, differ significantly in terms of what processing activities they carry out, their size and the amount and types (varying sensitivity) of personal data they process.

Therefore, the UK GDPR will apply differently to different organisations, and the risk will vary from business to business.

What might happen if a business fails to comply with the UK GDPR?

The UK GDPR is enforced by the Information Commissioner's Office (ICO).

The ICO has extensive powers, including investigating and issuing enforcement notices for non-compliance. In severe cases, the ICO can also issue significant fines.

What should my business do?

Now you understand the basics of GDPR and data processing, you now need to make sure your business is compliant. Here are some useful first steps you can take:

- Have a solid understanding of what kind of personal data you're processing
- Determine whether you have a legal basis for processing data under GDPR
- Undertake appropriate training
- Have written policies
- Make sure your website is GDPR compliant. This means having a privacy policy, cookies policy and cookie notification

If you're using a third party to process customer data (examples include data hosting and marketing/IT/HR services), then you'll need a Data Processing Agreement.

To get started, you can download our professionally drafted GDPR documents below.

Download our
Data Processing Agreement

Download our
Website Cookie Policy

Download our
Website Privacy Policy

GDPR changes after Brexit and UK GDPR

During the Brexit transition period, from January 2020 to 1 January 2020 (EU Exit Day), GDPR applied to UK organisations as it had done since its implementation in May 2018.

As with many other EU laws, the principles and regulations of the GDPR were transposed into what is now known as the UK GDPR. From Brexit Day, the EU GDPR ceased to apply to UK personal data. However it continues to apply to EU personal data processed by UK-based organisations.

UK organisations that process personal data from an EU/EEA Member State must comply with EU GDPR principles, the UK GDPR, and the Data Protection Act 2018 (DPA 2018).

EU-based organisations processing UK personal data must observe UK GDPR and EU GDPR.

What is Adequacy?

If the EU grants another country Adequacy, it means that, following extensive investigation and consideration, the EU Commission has decided that a particular country's data protection laws are 'adequate'. Therefore, additional safeguards are not required when sending personal data to and from an EU State.

Adequacy was granted to the UK in June 2021. However, it can be withdrawn if the European Union perceives that the UK law enacts data protection and privacy laws that move it too far away from the EU GDPR.

Do I need to appoint an EU/EEA-based representative?

Businesses that process data from EU/EEA data subjects and don't have an office or other form of base in an EU/EEA Member State must appoint a representative.

The GDPR personal representative requirement applies to organisations that:

- Provide products or services in the EU
- Monitors the behaviour of individuals located in the EEA

A GDPR representative can be an individual or company (such as a lawyer or GDPR consultant).

They must be based in a Member State where some of the organisation's data subjects are situated.

As the representative is the face of a company's compliance in the EU, care must be taken in choosing a suitable person or company to fill the position. You should consider the most appropriate jurisdiction when deciding which is right for you.

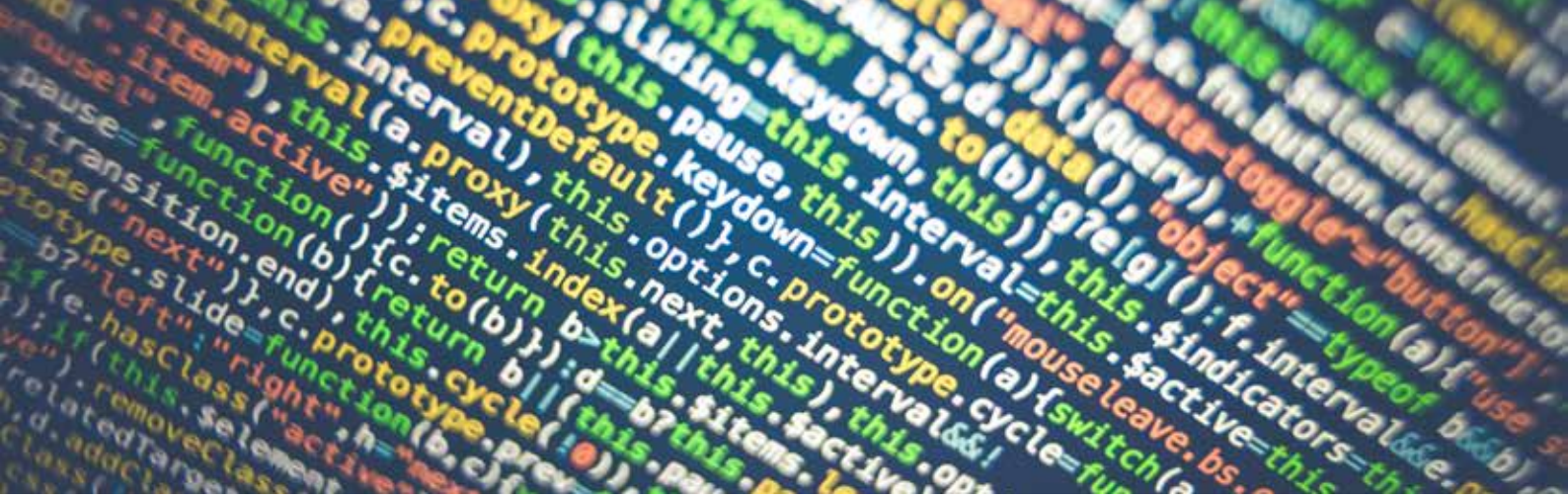
The GDPR only requires one representative to be appointed in a member state where the customers are based, given the differences between each EU country's interpretation of the GDPR processes and cultural differences between the various nations.

How is GDPR applicable in the UK post-Brexit?

Data protection and privacy compliance measures are ongoing commitments. A surefire way to accidentally commit a UK GDPR breach is to rely on the compliance measures you put in place when post-Brexit GDPR laws were applicable.

To protect your business, and the data it holds and be post-Brexit compliant, you can take the following five steps:

1. Map data flows to and from the EU/EEA to identify what compliance steps need to be taken. In turn, data flows within the UK should be regularly mapped to ensure that if a breach occurs or a 'Subject Access Request' is made, you can swiftly isolate the data affected/required.
2. Check if you need to appoint an EU/EEA-based representative and put one in place if necessary.
3. Identify if an EU supervising authority qualifies as a relevant LSA for your business' data transactions.
4. Amend existing contracts and template terms to include relevant data transfer wording and appropriate referencing to the UK and EU GDPR.
5. Implement the new SCCs, IDTA and the Addendum to ensure that data transfers are compliant.



Understanding the difference between a data controller and a data processor

The terms data controller and data processor are fundamental to GDPR. Because they're often interchangeable, it can be confusing to keep track of the data protection and privacy duties and responsibilities assigned to each role by GDPR and the Data Protection Act 2018. This can lead to an unintentional GDPR breach which may result in a heavy fine and reputational damage.

What is a data controller?

A data controller is a "natural or legal person, public authority, agency or other body which, alone or with others, determines the purposes and means of processing personal data".

A controller decides on the data processing issues of what, why, and how.

What is a data processor?

A processor is "a natural or legal person, public authority, agency or other body which processes personal information on behalf of the controller".

A processor is a separate legal entity from the controller, and they process data on behalf of the controller and have no purpose of their own for processing the data.

How can I tell the difference between a data controller and a data processor?

It can be tricky. Below are some questions created by the ICO that can help businesses to ascertain whether they're a data controller or a data processor.

You're likely to be a data controller if you:

- Are the organisation that collects the data in the first instance and has the legal basis to do so
- Decide what the personal data is to be used for
- Decide whether to disclose the data and, if so, to whom
- Determine whether subject access and other individuals' rights apply or whether there are exemptions
- Choose how long to retain the data or whether to amend the data in a way that is not routine

You're likely to be a data processor if you decide:

- The methods used for personal data collection and storage
- How the data is secured
- The means used to transfer personal data from one organisation to another
- How personal data is retrieved
- The method for ensuring a retention schedule is adhered to
- How personal data is deleted

The above lists are not exhaustive. Broadly speaking a processor decides on the technical matters concerning the data but the controller determines what the data is used for and its content.

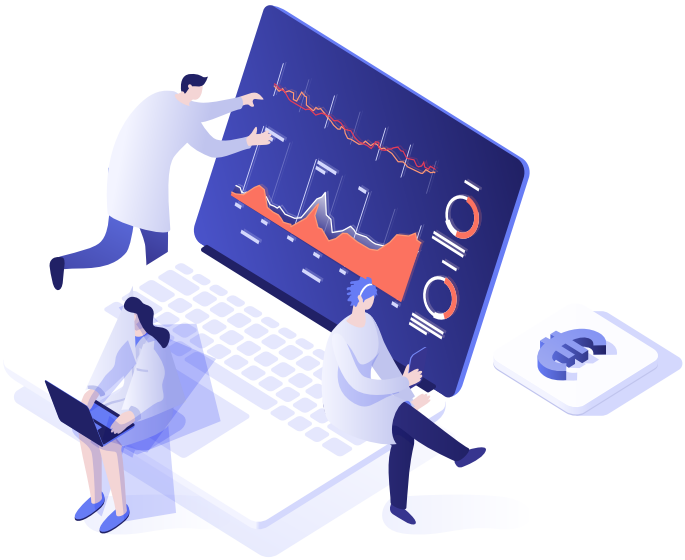
What is a joint controller?

A joint controller is where two or more controllers work jointly to determine the purposes and means of processing. This may occur in situations where a joint venture is formed or in the initial stages of a company merger.

The GDPR provides for specific duties in the case of joint controllers, including:

1. The controllers must establish who is responsible for conducting GDPR compliance obligations such as security measures, breach notifications, and a legal purpose for collecting data. These arrangements must be transparent and available to data subjects.

2. Each controller is liable for the damage caused by the processing activities, unless it can prove it is not responsible for the event giving rise to the damage.



What if my company doesn't fit neatly into the definition of data controller or data processor?

A grey area exists in which it is difficult to determine if a particular organisation is a controller or processor, especially in situations involving complex contracts and large supply chains.

If your business's position is ambiguous, you must take the following steps to protect your interests in case of a compliance or data breach:

- Make sure that any classifications of a data controller and data processor are documented, alongside the reasons for making the relevant decisions
- Don't base decisions on the contract. Instead, look at the facts of the relationship. For example, Article 28(10) of the GDPR states that if a processor decides the purpose and means of the processing, they're, in fact, a controller
- Document any changes to the classifications of controllers and processors and the reason for the changes
- Seek legal advice if you're uncertain about your role in a particular agreement

The role of a Data Protection Officer (DPO)

One of the most common questions we receive from businesses on the subject of data privacy and GDPR is "do we need a Data Protection Officer?".

There is no doubt that Data Protection Officers play an increasingly vital role in protecting UK businesses, so much so that demand for skilled staff to fill these roles has risen hugely over the past few years.

Given the enormous fines levied on some organisations, it is easy to see why. Google was ordered to pay £43.2m in 2019, and British Airways was fined £20m in 2020 for breaches of data privacy law. It is not just big firms being impacted. A number of fines in the region of £100,000 have been levied on SMEs.

What are the responsibilities of a DPO?

The responsibilities of a DPO are to handle all issues relating to the protection of personal data:

- Explain to those who control and process data within the organisation how to comply with the UK GDPR
- Monitoring compliance with the UK GDPR
- Provide advice on data protection impact assessments
- Cooperating with the supervisory bodies, e.g. the Information Commissioner's Office
- To act as a point of contact for the supervisory authorities

DPOs play a vital role in making sure that businesses remain compliant with data protection law at all times and avoiding any potential costly breaches.

Do you need to employ a DPO?

A business should appoint a DPO where:

- The processing is carried out by a public authority or body, except for courts
- The core activities of the data controller or the data processor consist of regular and systematic monitoring of data subjects on a large scale
- Processing on a large scale of special categories of data and personal data relating to criminal convictions and offences

Many businesses remain confused as to whether they still fall into the mandatory requirement for a DPO.

To answer this we need to clarify what is meant by **'core activities', 'regular and systematic monitoring', 'large scale' and 'special categories of data'.**

'Core activities' refers to the 'primary activities' of a business, not the activities that all businesses have to perform, such as payroll and storing information on clients. For example, a law firm processing information relating to a legal case would be considered a primary activity.

A business will be considered to be involved in 'large scale' data processing where they're handling extremely large volumes of data – e.g. whereas a hospital would come under this definition, a local GP surgery would not.

A business is considered to be carrying out **'regular and systematic monitoring'** if they're processing lots of data for tracking and profiling – e.g. an online retailer using data to make recommendations to prospective clients.

And finally, **'Special categories'** may include sensitive data, including information on health, race, political opinions or identity.

Are you still unsure if you need a DPO?

The UK GDPR as it stands is still rather unclear, leaving many businesses unsure if they fall within the mandatory requirement for a DPO. If you're in this position, speak to one of LawBite's expert UK data protection solicitors who will clarify your position.

By asking questions about the use of personal data within your business, we can confirm if a DPO is needed. In addition, we can explain how to go about appointing a DPO and the type of training they'll need.

Think of a DPO as an investment in your organisation, not a cost. Even if a DPO is not strictly necessary for your SME, hiring a person to fill this role will ensure that you don't fall foul of the laws on data privacy, and you'll mitigate and militate the risk of serious breaches and financial penalties.

Another reason is that by investing in a DPO, you're sending a strong signal to prospective clients and investors that you take the protection of data extremely seriously. This will offer them significant reassurance that your SME is adhering to data privacy best practice.

Here is a checklist to ensure you're compliant:

- Review your business's existing use of data – i.e. who are the 'data controllers' (those who determine if and why data needs to be processed) and 'data processors' (those who process data on behalf of the controller) within your business, what data you hold, and how data is processed?
- Assess whether a DPO is mandatory for your organisation. Speak to a specialist in data protection law if you're unsure.
- Appoint a DPO and ensure they receive the training, time, resources and support they need to perform their role.

How to gain consent under the GDPR

While some businesses believe they're compliant with the GDPR all too often they're not. This is partly because the rules around gaining consent can be confusing and complex.

Gaining proper consent is not just asking permission to hold and use data, it is also necessary to explain to the individual (the 'data subject') their right to change their mind at any time.

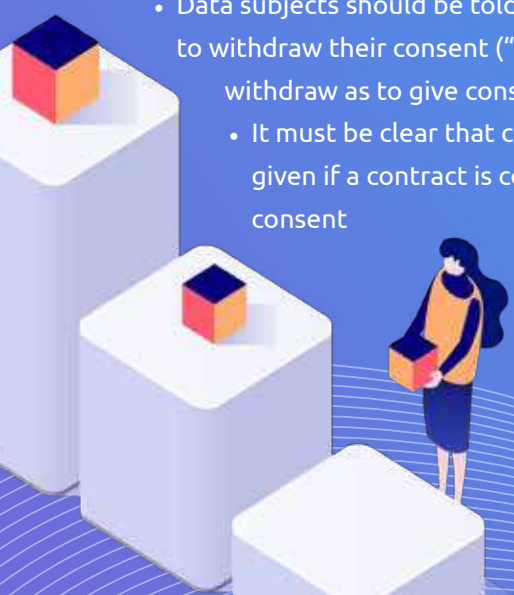
What are the consent requirements of GDPR?

Article 4 of the GDPR defined consent as "...the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Valid and invalid consent

Article 7 of the GDPR states that to gain valid consent:

- The data controller (i.e. the person who is making decisions about how and why data should be processed) must have a record of the consent for personal data to be used
- Information regarding written consent should be distinct and clear from other matters
- Data subjects should be told they have the right to withdraw their consent ("It shall be as easy to withdraw as to give consent")
- It must be clear that consent is freely given if a contract is conditional on that consent



'Freely given' in this context means that consent is given based on a genuine choice.

If it can be shown that consent is given but the data subject effectively had no choice but to agree to the use of their personal data, this would not be considered valid consent.

Consent may also be deemed invalid if:

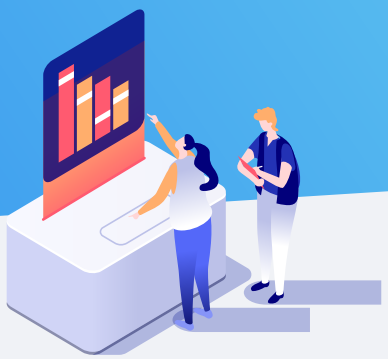
- It is unclear if a data subject gave consent
- The data subject was not aware they gave consent
- There are no records showing a data subject gave consent
- Consent was required as a precondition of a service but the processing is not necessary for that service

'Specific and informed' consent

The GDPR also refers to 'specific and informed' consent. This means that the data subject has the right to:

- Know the identity of the person making decisions about the use of their information (i.e. the data controller and any third-party controllers who will rely on the consent given)
- Consent to different reasons for collecting the data. This means that if the organisation collecting data is using it for several reasons, consent must be given for each reason

lawbite



How LawBite can help your business

We understand that GDPR compliance can seem overwhelming with many new rules and ongoing processes to comply with.

Every business is unique so a one-size approach doesn't always work.
Our GDPR lawyers will work with you to understand what your business needs and agree on a pathway to compliance.

Our GDPR legal services include:

- Legal advice provided by our expert data protection lawyers on what GDPR means operationally for your organisation
- GDPR health check for your business showing you what changes you need to make and giving you an action plan
- Identifying whether you're a data controller or whether you're a data processor
- Helping you set up contracts between data processors and data controllers
- Reviewing and drafting employment contracts and providing HR advice related to GDPR
- Helping you prepare the policies you need for GDPR compliance, e.g. Data Protection Policy, Privacy Policy, Cookie Policy, Security Policy and Retention Policy
- Advice on handling Data Subject Access Requests
- Advice on dealing with a suspected data breach
- Advice on how to gain compliant consent from customers to collect and use their data
- Access to legal and business document templates to help you set up GDPR contract

Book a free 15 minute call