With the European General Data Protection Regulation (GDPR) now in place, the UK will see tougher fines and stricter regulations, across all industries. GDPR regulation for small businesses is a hot topic, but are you complying with the changes?

Read our GDPR key points for small businesses and get clear on your responsibilities.

The GDPR deadline was 25 May 2018

Before we get into the detail of GDPR and what it means for your small business, it’s worth making a note of the key things you’ll need to keep an eye on and action. Bear in mind that the changes came into effect on 25 May 2018.

Here’s our quick definition and overview, followed by a checklist to keep handy.
What is GDPR?

What does GDPR stand for: a meaning and definition

The European General Data Protection Regulation (GDPR for short) is built around two key principles.

1. Giving citizens and residents more control of their **personal data**
2. Simplifying regulations for international businesses with a unifying regulation that stands across the European Union (EU)

It’s important to bear in mind that the GDPR applies to any business established in the EU and may apply to companies based outside of the EU that process the personal data of EU citizens in certain circumstances. See the GDPR checklist below for information on what ‘personal data’ includes.

The government has confirmed that Brexit will not affect GDPR, or its immediate running. It’s also confirmed that post-Brexit, the UK’s own law (or a newly-proposed Data Protection Act) will directly mirror the GDPR.

**GDPR overview**

- Businesses whose activities involve ‘regular or systematic’ monitoring of data subjects on a large scale (in other words processing extensive personal information), or which involve processing large volumes of ‘special category data’ must employ a Data Protection Officer (DPO). Their role will be to ensure the company complies with the obligations under the GDPR. They’ll also be the contact for any data protection queries.

- The GDPR may apply to any business that processes the personal data of EU citizens, including those with fewer than 250 employees (contrary to common misunderstanding).
Serious breaches (that is, any breach which has an impact on the rights of data subjects) must be reported to the regulator (in the UK this is the Information Commissioner’s Office (ICO)). This should be within 24 hours where possible, but at least within 72 hours and the report must include information regarding what led to the breach, how it is being contained and planned next steps.

- Individuals will have more rights on how businesses use their data. In some instances, they have the ‘right to be forgotten’ if they no longer want you to process their personal data and you have no other legal grounds (for example the individual is no longer a customer so your contract with them no longer gives you a legal right) to keep the data.

- Failure to comply will result in harsher penalties. Before, the ICO could fine up to £500,000 but the GDPR allows fines of up to €20 million, or four per cent of annual turnover, whichever is higher.

**GDPR checklist for UK small businesses**

Remember, your checklist needs to take into account past and present employees and suppliers as well as customers (and anyone else’s data you’re processing which includes collecting, recording, storing and using the personal data in any way).
1. Know your data. You need to demonstrate an understanding of the types of personal data (for example name, address, email, bank details, photos, IP addresses) and sensitive (or special category) data (for example health details or religious views) you hold, where they’re coming from, where they’re going and how you’re using that data.

2. Identify whether you’re relying on consent to process personal data. If you are (for example, as part of your marketing), these activities are more difficult under the GDPR because the consent needs to be clear, specific and explicit. For this reason, you should avoid relying on consent unless absolutely necessary.

3. Look hard at your security measures and policies. You need to update these to be GDPR-compliant, and if you don’t currently have any, get them in place. Broad use of encryption could be a good way to reduce the likelihood of a big penalty in the event of a breach.

4. Prepare to meet access requests within a one-month timeframe. Subject Access Rights are changing, and under the GDPR, citizens have the right to access all of their personal data, rectify anything that’s inaccurate and object to processing in certain circumstances, or completely erase all of their personal data that you may hold. Each request carries a timeframe and deadline of one month (which can only be extended in mitigating circumstances), from the original date of request.

5. Train your employees, and report a serious breach within 72 hours. Ensure your employees understand what constitutes a personal data breach and build processes to pick up any red flags. It’s also important that everybody involved in your business is aware of a need to report any mistakes to the DPO or the person or team responsible for data protection compliance, as this is the most common cause of a data breach.
6. Conduct due-diligence on your supply chain. You should ensure that all suppliers and contractors are GDPR-compliant to avoid being impacted by any breaches and consequent penalties. You also need to ensure you have the right contract terms in place with suppliers (which puts important obligations on them, such as the need to notify you promptly if they have a data breach). See ‘How can I check my suppliers are GDPR-compliant?’ further down.

7. Create fair processing notices. Under GDPR, you’re required to describe to individuals what you’re doing with their personal data. See ‘Fair processing notices’ below for more information.

8. Decide whether you need to employ a Data Protection Officer (DPO). Most small businesses will be exempt. However, if your company’s core activities involve ‘regular or systematic’ monitoring of data subjects on a large scale, or which involve processing large volumes of ‘special category data’ (see ‘Is my data sensitive?’ below) you must employ a Data Protection Officer (DPO).

What constitutes ‘large-scale’ data processing?

The GDPR doesn’t yet fully define what constitutes ‘large-scale’, but some examples include the processing of patient data by hospitals, travel data and transport services, and customer data by an insurance company or bank.

Hanging on to old data?

One of the key principles of GDPR is to require companies not to hold on to personal data for longer than necessary, or process it for purposes that the individual isn’t aware of. Identifying your data categories – what personal data you have, and why – will be very helpful in ensuring you’re compliant with the GDPR.
How does the GDPR define ‘consent’?

Customer or individual ‘consent’ has been redefined and has become much tighter as a result. On top of this, requests for consent can no longer be hidden in small print but must be presented clearly, and separately to other policies on your website or communications – so no more pre-ticked boxes.

Consent may not be required for pre-existing personal data, as long as you have a legal basis that’s compliant with the current legislation (the DPA).

The principle here is that inactivity is no longer a legitimate way to confirm consent. Remember, this applies to you too, as a consumer with personal data rights of your own, and may be a welcome change!

Fair processing notices

It may sound complicated, but a fair processing notice is about giving people clear information about what you’re doing with their personal data. Your fair processing notice should describe:

• why you’re processing their personal data (the purpose), including the legal basis you have, such as consent (check the ICO’s privacy notices page for more information)
• the categories of recipients you may be sending the personal data to (customer, employee, supplier, etc)
• how long you’ll be holding onto the data (the ‘retention’ period’), or the criteria used to determine these time periods

You’ll also need to notify individuals of the existence of their personal data rights.
GDPR is so complicated – why should I care?

It’s easy for small companies with a stack of to-dos to see the GDPR as a burden. But in reality, it’s something that can be used to your advantage, adding value to your business.

By proving to potential and existing customers that your organisation is compliant with new laws that protect the rights of citizens just like you (and your customers), you could bring in more business.

No one likes having their data lost, stolen, damaged, misused, or shared without proper consent, and doing everything you can to protect your customers and grow their trust could be a unique selling point.

So, from fines to compensation claims, there are certainly serious reasons to get GDPR-compliant. But on a real-world level, see it as being worth your while to get organised behind the scenes, earn your customers’ trust, and be the company that respects personal data, rather than letting it sit on a long-forgotten spreadsheet.

Does GDPR apply to my business?

It’s important to bear in mind that the GDPR applies to any business established in the EU and may apply to companies based outside of the EU that process the personal data of EU citizens in certain circumstances.

So the first question you need to ask yourself is, how often does your business deal with personal data? This includes your
customer data of course, but have you factored in supplier data? Past and present employees? And is there anything else you’ve collected, that doesn’t fall into any of these groups?

If you’re collecting any of this data routinely, you need to comply with the GDPR, whether the data is on a spreadsheet, on your computer network, your mobile phone, or in the cloud.

Another key question is whether your business currently falls under the DPA. If so, the ICO has confirmed that the GDPR applies to you, but remember, the GDPR is much stricter than the DPA.

**I employ fewer than 250 people. What should I do?**

Being a small business doesn’t mean you fall out of the GDPR scope. It’s recognised that small businesses have fewer resources and pose less of a risk to data protection, so there may be more leniency by the ICO in relation to any non-compliance.

However, you’ll still want to ensure you’re compliant with the principles of the GDPR. This is because your business must still comply if it’s involved in regular processing (which includes collecting, storing and using) of personal data. It’s easier to follow the GDPR and get compliant, than to spend time figuring out how you can avoid complying, especially if you’re working without legal guidance.

It’s also important to note that even if your company falls under one of the exemptions, if you’re contracting with a larger company that conducts large-scale processing you may also be subject to the harsher end of the GDPR’s regulation.

Aside from the law, responsible data handling is a basic principle of good business upkeep. If you’re a one-person
band but aware that your records are a bit all over the place, have you thought about how you’d explain a breach to your trusted customers?

What data does the GDPR legislation apply to?

You’ll see a lot about ‘personal data’ when reading up on the GDPR. It’s now got a more detailed definition, and the regulation has clarified that things like an IP address (the unique string of numbers that identifies every Internet-communicating computer) count as personal data. There are lots of other things though that will fall into the personal data category, so make sure you’ve checked the GDPR itself (using the handy links at the end of this article).

Quick check: Focus on your lists. Does your business hold HR records, customer lists and contact detail records, for example? Most do.

This is confirmed by the ico.org.uk, who state; “You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR”.

Manual vs. auto-filing

Whether it’s you keeping a spreadsheet of customer contact details, or an automated digital capture system, the GDPR will apply.

Is your data ‘sensitive’?

Article 9 in the GDPR defines ‘special categories of personal data’ and this includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. They also cover genetic data, biometric data, data concerning health and data concerning a person’s sex life or sexual orientation. Generally, you’ll need explicit consent from individuals whose special category
personal data you want to process, although Article 9 sets out a number of exceptions to this rule.

**How is the GDPR law different from the DPA?**

There are similarities between the GDPR and current Data Protection Act (DPA). However, crucial developments and rulings within the GDPR mean you’ll need to get clear on the new legislation, whether you’re up-to-date with the DPA or not.

**The GDPR changes your accountability**

One thing that really sets the GDPR apart is the changes made to the ‘accountability’ of data processors. This is a change from under the DPA, which placed more responsibility on the data controller (note, it’s still worth brushing up on your DPA compliance, as lots of its basic principles are pretty much repeated in the GDPR).

These are basic principles you’ll need to think about. Don’t get too hung up on whether you’re a controller or processor as both parties are required to make changes in order to comply with GDPR. At this stage, the key thing is to think about the personal data your small business collects, holds, uses, and shares, and how confident you are that the new principles hold true.

**Am I a data controller or a data processor?**

The GDPR applies to data ‘controllers’ and ‘processors’. In general, processing is defined as any operation performed on personal data, such as storing, collecting, recording, organising, sharing, erasure, consulting, etc. A controller is a data processor too, but they will also decide the purpose of the data processing activities.
For example, if you’re a small business offering a plumbing service and your customer details are managed using a contacts management app on your phone, hosted by a third party, this would generally make you the controller and the third party the processor. If on the other hand, you manage all of your data on a spreadsheet you’ve built yourself, you’re both controller and processor.

If you’re a data processor

For processors, the GDPR carries a specific set of legal obligations some of which require you to:

- keep up-to-date personal data records and details of your processing activities and categories, including details of your ‘data subject categories’ (customers, employees, suppliers, etc), the categories of processing carried out (transferring, hosting, altering, receiving, disclosing, etc)
- keep details of any transfers to countries outside the European Economic Area (EEA)
- implement appropriate security measures, which may include pseudonymisation and encryption, and prove you’re regularly testing these measures
- be ready with a general description of the technical and organisational security measures you keep in place

If responsible for a breach, you’ll definitely have more legal liability than under the DPA. If a data subject, maybe one of your customers, has suffered as a result of a data breach, they could make a claim against the data processor directly.

As a data processor, the severity of your penalty will reflect how serious the consequence of your failure to comply with your obligations placed on you by the GDPR or followed the instructions of your data controller. These obligations include ensuring sufficient security measures, and you’ll suffer further
penalties (see ‘What are the GDPR penalties?’ further down) if you fail to report the breach within the given time frame (a maximum 72 hours).

As well as this, if you’re a data processor and have paid compensation that the controller is partly or fully responsible for, you may be entitled to claim back the relevant damages from the controller themselves if you have a contract in place that states this. This area of claims is where cyber or professional indemnity insurance can come in handy, although you’ll always need to match the policy to your activities.

If you’re a controller

All controllers are by nature also processors and therefore subject to the same basic requirements. As a controller, the GDPR places obligations on you and your business to ensure any contracts you have with processors are compliant. Take a look at the section for processors above – it may be worth checking that their security measures and processes are GDPR-compliant before signing or renewing any contract.

Are you inside the EU?

The GDPR applies to businesses established in the EU that process personal data of any EU citizens, so far regardless of developments with Brexit. It also applies to organisations outside the EU which offer goods or services inside the EU.

How can I check my suppliers are GDPR-compliant?

Working with GDPR-compliant suppliers and contractors will reduce the risk of being impacted by a data breach, and any consequent fines and claims.
You could ask suppliers and contractors to complete a form that confirms the security measures they have in place, or you could conduct an on-site visit. If their existing measures aren’t sufficient, you should review your relationship to ensure they are compliant with GDPR.

Where your suppliers (as processors) are processing personal data on your behalf (as a controller), you have an obligation to update your contracts with them to include a number of mandatory clauses that can be found in Article 28(3) of the GDPR. These ensure that processors are contractually obliged to provide GDPR-compliant data protection standards.

GDPR consent – how do I get consent from my customers to use their data?

It’s great that you’re thinking about this, as consent is a key concern tackled by the GDPR.

The ICO has a dedicated page on its website covering consent.

GDPR consent checklist and principles (at-a-glance):

- Check your consent practices and existing records. Refresh where necessary
- Offer individuals genuine choice and control
- Where using an opt-in, don’t rely on pre-ticked boxes or default options
- Explicit consent means a very clear, specific statement of consent
- Keep your consent requests separate from other terms and conditions
- Be specific, granular, clear and concise
- Name any third parties who will rely on the consent
- Make it easy for people to withdraw consent (and tell them how)
- Keep evidence of the consent (who, when, how and what you’ve told people)
• Avoid making consent a precondition of your business services
• Consent should put individuals in control, build trust and engagement and enhance your reputation

What are the GDPR penalties?

The GDPR toughens up penalties already existing under the DPA. These existing penalties include:
• Maximum fines of £500,000
• Prosecutions, including prison sentences for deliberate breaches
• Obligatory undertakings, where your company has to commit to specific action to improve compliance

With the introduction of GDPR, these penalties got heavier.

Businesses in breach are liable to a dramatic increase in fines, with penalties reaching an upper limit of €20 million or four percent of annual global turnover, whichever is higher.

Insolvency will be a real risk for non-compliant businesses as a result of these fines. But bear in mind the possibility that individuals can also sue you if they suffer as a result of your data management. This could be for material damage or non-material suffering, such as distress.

GDPR compliance checklist, helpful links and resources

ICO resource centre (small organisations and the GDPR)
ICO 12-step checklist

The website and checklist above are great resource for small businesses looking to step in-line with the GDPR.

From there, these more general websites can give a good overview.
ICO GDPR overview
EU GDPR portal
Late payments increase by £1b: here’s how to recover debt

New research has revealed that late payments have increased by £1 billion on figures released just six months ago.

Which? research reveals the ‘least trustworthy’ tradespeople

New research by Which? has revealed the ‘least trustworthy’ tradespeople, according to homeowners.

HMRC investigate your finances without permission?

A new HMRC consultation reveals that they want the power to look at taxpayers’ financial information without their permission.