IS YOUR BUSINESS PREPARED FOR THE GDPR?

How you handle your customers' personal information is changing as businesses need to be compliant with the new GDPR by 25 May 2018. Read our essential guide to get your business in shape ahead of the EU's new data rules.

Pinsent Masons

HISCOX
EVER ONWARDS

GOODBYE DATA PROTECTION ACT, HELLO GDPR

On 25 May 2018, the European General Data Protection Regulation (GDPR) will apply. And, as it is an EU regulation, the GDPR will automatically take effect without the need for it to be locally implemented by member states.

Never heard of the GDPR? You're not alone. A recent government report – The Cyber Security Breaches Survey 2018 – found that while awareness among larger businesses was widespread, many smaller businesses were 'often' unaware of the GDPR.

Who does the GDPR apply to?

The GDPR applies to 'controllers' who are established in the EU, as well as those organisations who are not established in the EU but offer goods or services to, or monitor the behaviour of, data subjects within the EU. Therefore, it substantially extends the territorial scope of organisations who have to comply with data protection laws (in comparison to the UK Data Protection Act 1998 (DPA).

The focus is no longer on the use of equipment located within an EU member state; instead, the focus is on those who are targeting EU citizens. This means that non-EU organisations not previously caught under the DPA for targeting an EU market or EU citizens, will now be caught by the GDPR, despite lack of presence or use of equipment in the EU.

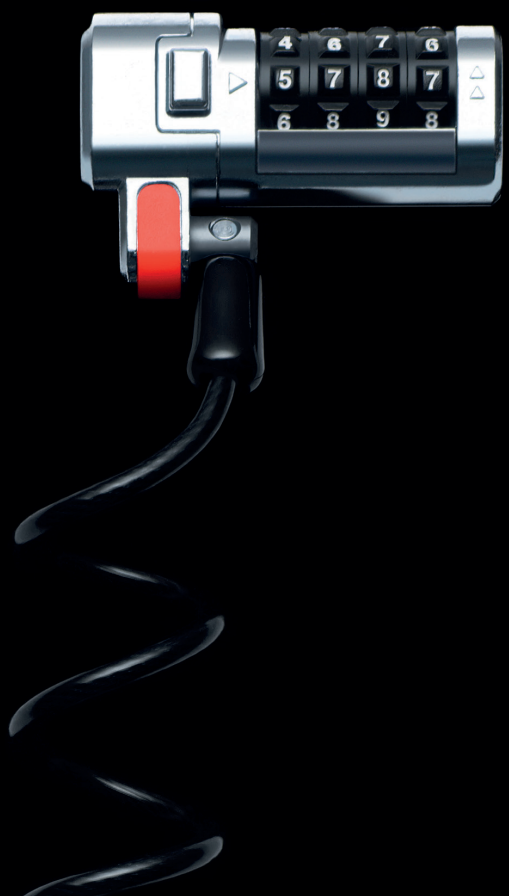
For the first time, the GDPR also introduces statutory obligations for processors. Under current data protection laws, the controller party has statutory responsibility for the processing of the personal data. However, the GDPR introduces statutory obligations for processors.

The 'controller' is the party who determines 'why' the personal data will be processed (i.e. the purpose of the processing) and, where the controller appoints a processor, the processor determines 'how' the personal data will be processed (i.e. the method of the processing). Typically, an IT services provider will be a 'processor' and its customer will be the 'controller'.

The new processor obligations relate to the requirement to put in place GDPR compliant processing clauses (see section 2.6), security measures, security breach notification (see section 3), international transfers, data protection impact assessments (see section 2.8), data protection officers (see section 2.9) and record-keeping. Fines may be imposed on processors (see section 4). Other enhanced supervisory authority powers such as auditing also apply to processors.

We're leaving the EU – won't that mean UK businesses can ignore the GDPR?

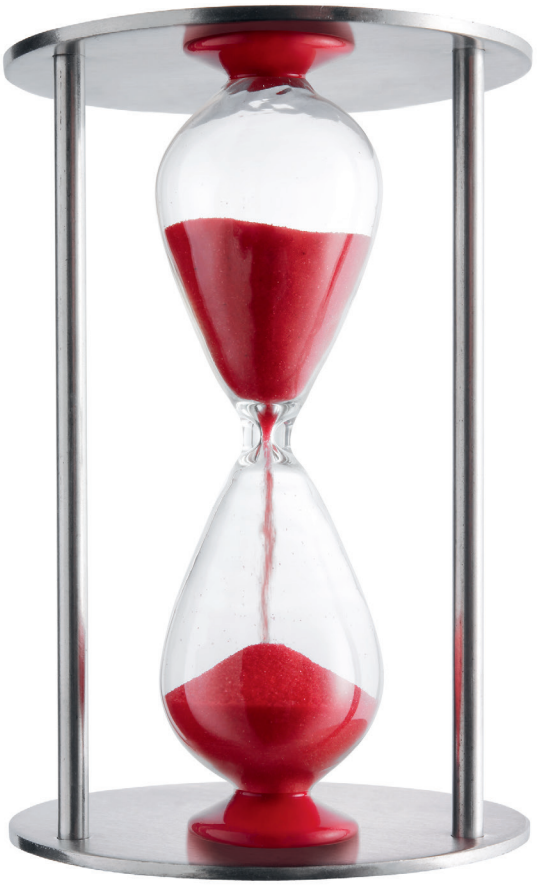
With the GDPR's implementation date of May 2018 happening before the likely March 2019 date of the UK's withdrawal from the EU, businesses will still need to be compliant with the GDPR for a period of at least ten months. And, although the UK's data protection status after Brexit is still unknown, the government has suggested that it intends to implement equivalent GDPR rules post-Brexit (see the Data Protection Bill announced in the 2017 Queen's Speech) in order to make sure that the frictionless movement of data between the UK and the EEA continues after we leave. However, it's best to check regularly for relevant developments as things can change very quickly.



IN THIS GUIDE

With not long to go until its implementation – and remember 25 May 2018 is the deadline for companies to be compliant, as there will not be a further grace period – we have produced this simple guide for SMEs. It will help you understand what actions you need to take now, as well as what will happen if you experience a personal data breach under the new regulations.

Read on to help make sure your business is ready for 25 May 2018.



> “ Remember, 25 May 2018 is the deadline for companies to be compliant – there will not be a further grace period.

1. WHAT IS THE GDPR AND HOW DOES IT APPLY TO YOU?

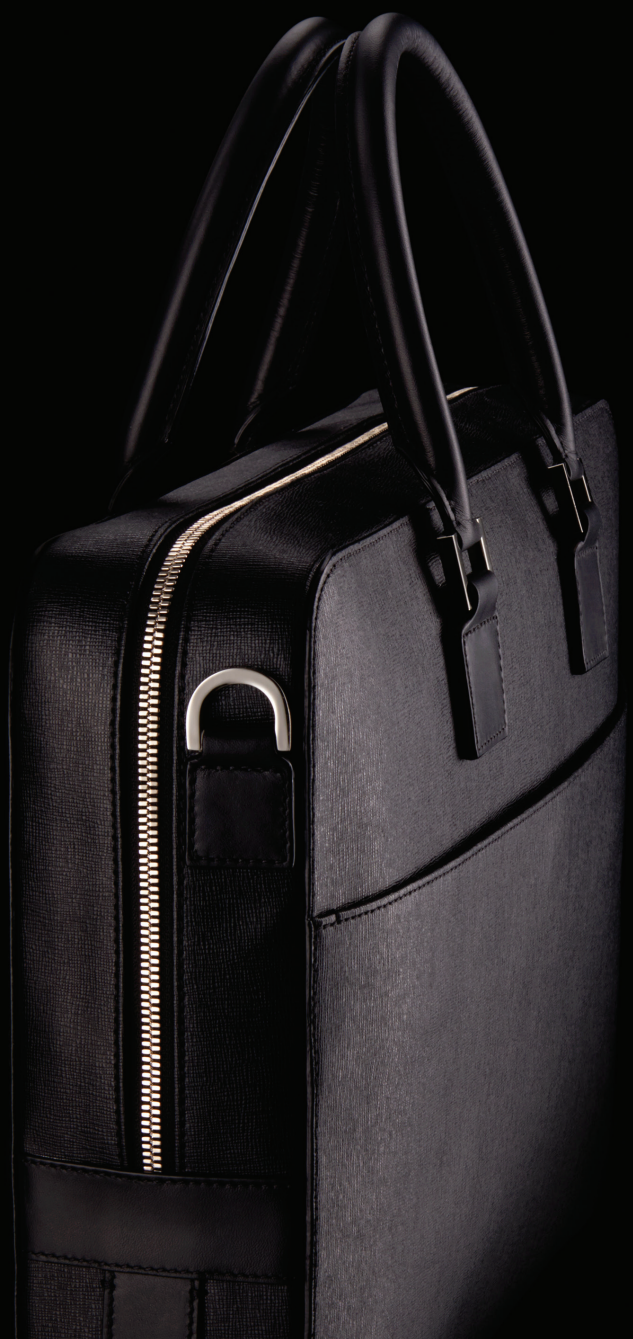
Designed to help safeguard data protection rights for individuals, the GDPR introduces a single set of rules across the EU when it comes to how organisations handle data relating to identifiable individuals. That means if your business holds personal information such as names, addresses, HR records, customer lists and even online identifiers such as a computer's IP address, you could be subject to certain requirements of the GDPR.

1.1. Am I exempt as a small business?

Being a small business doesn't mean that you fall outside of the scope of GDPR – all companies, regardless of size, have to get on the front foot when it comes to data protection. Yet there are some areas where it is acknowledged that SMEs have fewer resources or that they process lower volumes of non-sensitive data. Therefore, it's also recognised that the 'appropriate' security measures an SME puts in place may be less robust than those required by a larger corporate processing high volumes of personal data and/or sensitive personal data. For this reason, an SME may be exempt from some of the more rigorous steps (such as the need to appoint a data protection officer – see section 2.9).

We are also seeing a number of larger organisations preparing themselves for the GDPR's arrival and looking to force their supply chain, by contract, to meet certain information security requirements. If you are able to demonstrate that your SME is ahead of the game, by having a GDPR compliant data protection clause in place, you may find yourself at a competitive advantage over your peers when it comes to tendering for business.

"If you demonstrate that your SME is ahead of the game, by having a GDPR compliant data protection clause in place, you may find yourself at a competitive advantage over your peers when it comes to tendering for business.



2. WHAT DO YOU, A SMALL BUSINESS, NEED TO DO TO BE COMPLIANT WITH THE GDPR?

There are several simple steps that you need to consider to make sure you are compliant by 25 May 2018.

2.1. Know what data you hold, where it is coming from and where it is going

First, it is important that you understand and record what 'personal data' you hold as a business, how it was captured, how it is held, how you use it, and where it is going. The GDPR defines 'personal data' as: '...any information relating to an identified or identifiable nature person ('data subject)'; and identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'. **The GDPR definition of 'personal data' is broader than under the DPA and includes IP addresses, device IDs, location data and genetic and biometric data.**

2.2 Are you relying on consent?

If you are relying on consent to process a data subject's 'personal data' (e.g. when processing sensitive personal data), the GDPR will make this a lot harder. The definition of consent has been tightened so that it must be 'unambiguous' when given. **And, where relied upon, consent will also have to be gained retrospectively for existing customers.**

In addition, requests for consent will also have to be presented in a manner that is completely separate, so they can no longer be hidden within other policies or small print on your website.

Where you are relying on consent to process 'personal data', being able to prove how you obtained it will be vital. Silence, pre-ticked boxes or inactivity will no longer be valid and customers/prospects will have to express their consent in a more unambiguous way (i.e. by ticking a box).

Think about:

- how consent is obtained at the moment, if at all
- what changes to your processes may be needed to make sure that you are able to show where, when and how people have adequately given you consent to process their data.

2.3. Data protection by design

Under the GDPR the protection of data has to be considered and baked into any systems/processes from the outset – both in terms of the way that computer systems are designed and the policies/procedures that are in place to dictate how people should use them.

One element that gets a much higher profile and attention from the GDPR is the use of encryption. Not only is this top of the list of suggested security measures, but the broad use of encryption can also reduce some of the burden and likelihood of a penalty being applied in the event of a data breach.

2.4. Right of data access

Individuals will have a number of rights when it comes to how you look after their 'personal data'. **Make sure there are appropriate processes and templates in place so that the data subject rights can be met within the new time scales (one month).**

Individuals will have the rights to:

- access all data held on the individual
- rectify inaccurate data
- restrict or object to the processing (in certain circumstances, e.g. marketing) of data
- export the data in a format that can be used in another IT environment
- completely erase all data on an individual (in certain circumstances).

2.5. Know what constitutes a personal data breach

Make sure you and your employees understand what constitutes a personal data breach (see section 3) and **put in place a process for flagging and escalating breaches internally**. This is vital to meet the strict time scales for response laid out by the GDPR.

Alongside the training needed for this, **you should try to develop and encourage a culture where employees feel comfortable in self-reporting when they have made innocent mistakes** – the root cause of the vast majority of data breaches.

2.6. Review terms and conditions and supplier contracts

Where a contract involves personal data, it is essential to analyse the relationship between the parties. Whether a party is a controller or a processor is a question of fact and law. In the context of IT services, it is often the case that the customer is a controller, and the IT service provider acts as a processor on its behalf.

Conduct due diligence on any suppliers that process 'personal data' on your behalf or jointly or in common with you to make sure that there are adequate protections in place to cater for the GDPR. This could be by either asking them to complete a due diligence form to capture what measures they have in place (which should then be reviewed to make sure that they are sufficient) or by conducting an on site audit.

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 provisions ensure that processors are contractually obliged to provide GDPR compliant data protection standards.

It is worth noting that **if you act as a processor for other companies, they will be looking to amend your contract with them on the same basis**, and new customers will increasingly focus on this. Being prepared will help both your negotiating position and give you a competitive advantage.

2.7. Review your fair processing notices (your customer facing privacy notices)

Because of the requirements imposed by the GDPR, your fair processing notices are now likely to get a lot lengthier. You will need to go into much more detail about the legal basis for processing the personal data and will also need to write your policies in a way that is understandable and accessible to your customers. There are also some differences in what you are required to provide, depending on whether you are collecting the information directly from data subjects or from a third party.

The information that should be supplied includes:

- the purposes for which you're processing the personal data as well as the legal basis for the processing (e.g. consent, legitimate interests, contractual requirement etc.)
- the recipient or categories of recipients you may be sending the personal data to
- the retention period or criteria used to determine the retention period
- the existence of each of the data subject's rights

For more on the requirements, please check the Information Commissioner's Office (ICO) guidance.

2.8. Data protection impact assessments

Before you begin data processing 'likely to result in a high risk to individuals' a **documented** risk assessment will be needed to identify and mitigate the risks, and demonstrate compliance with the GDPR.

What constitutes a 'high risk to individuals' is unclear, but it could include things such as the capture/processing of sensitive personal data like health information which could be very distressing to the individual if leaked.

This documented risk assessment is known as a 'data protection impact assessment' or 'DPIA'. A DPIA is a process designed to describe the processing, assess the necessity and proportionality of processing, and to help manage the risks to the privacy of the data subjects resulting from the processing of personal data (by assessing those risks and determining the measures to address them). **DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate that appropriate measures have been taken** to ensure compliance with the GDPR – a DPIA is a process for building and demonstrating compliance.

2.9. Understand whether you need to appoint a data protection officer (DPO)

If your core activities involve 'large-scale' monitoring or processing of sensitive personal data (this includes data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, the processing of genetic data, biometric data for the purpose of uniquely identifying an individual, data concerning health, sex life or sexual orientation), a DPO has to be appointed who must be independent of management and the team undertaking the processing. The DPO's responsibilities cannot just be delegated to the IT person. The EU doesn't fully define what constitutes 'large scale', but some of the examples that they have given include processing:

- patient data by a hospital
- travel data for people using a city's passenger transport service
- customer data by an insurance company or a bank.

3. WHAT IF YOU HAVE A DATA BREACH UNDER THE GDPR REGULATIONS?

The GDPR defines a 'personal data breach' as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. This means that a 'personal data breach' is more than just being hacked or losing personal data. This also applies to data held by you in any form – not just electronic. We may live in the digital age, but **paper-based data that is structured according to specific criteria should be treated with the same level of care.**

3.1. When should you report a personal data breach?

Breaches will have to be reported to the ICO unless they are 'unlikely to result in a risk to the rights and freedoms of individuals'. The examples of notifiable breaches provided by the ICO are where breaches may 'result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage'.

Breaches will only have to be reported to the individuals concerned where there is a 'high risk' of the above.

3.2 How long before you report a breach?

Where a breach is reportable by a controller to the ICO, it has to be done without undue delay and, where feasible, not later than 72 hours after having become aware of it and that report **must** contain, as a minimum:

- the nature of the personal data breach including, where possible, the categories and approximate number of both the individuals and personal data records concerned
- the name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained
- a description of the likely consequences of the 'personal data breach'
- a description of the measures – proposed or taken – to deal with the 'personal data breach' and where appropriate, of the measures taken to mitigate any possible adverse effects.

> "Breaches will have to be reported to the ICO if they are likely to result in a risk to the rights and freedoms of individuals.

Processors are required to report to controllers without undue delay after becoming aware of a personal data breach. Note that where a controller has appointed a processor to process the personal data on its behalf, the controller is deemed to be 'aware' from the point that the processor notifies the controller.

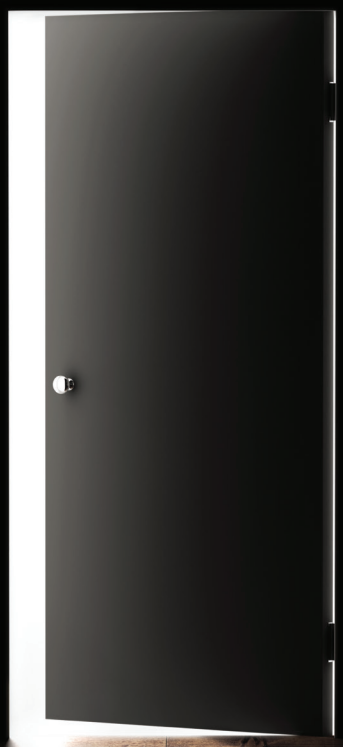
3.3. How to prepare for breaches

Given the broad definitions of 'personal data breach' and 'personal data', it's almost inevitable that organisations will have at least a minor breach (such as sending an email to the wrong person) at some point, so it's well worth giving some thought as to how you will respond as and when that time comes, particularly given the stringent time frames required for notification.

A simple, but thought-out, incident response plan can make a huge difference to minimise the impact on your business.

Things to consider are:

- who breaches should be reported to internally
- who needs to be involved in any investigation (this could be internal or external IT service providers, or specialist IT forensics)
- what the most critical systems and data are, to prioritise protection and restoration.



4. WHAT ARE THE CONSEQUENCES OF YOU FAILING TO COMPLY WITH GDPR?

While compliance with the GDPR may seem labour intensive, it will ultimately exist to make sure that you are able to best protect your customer's personal data. **We've seen that when organisations fail to protect personal data there can be a massive detrimental impact on their reputation.** So, compliance with the GDPR and the protection of customer's personal data is in the best interests of your business and in the protection of your hard-earned reputation.

4.1. The fines for non-compliance

Failure to comply with the GDPR (not just by experiencing personal data breaches, but through 'administrative failures' such as not completing – or even just not documenting – data protection impact assessments) could result in a regulatory investigation, which in itself takes time and effort on the part of a business, and potentially a fine being levied.

The size of the fine could be up to 4% of a company's global turnover (for the preceding financial year) or €20 million (whichever is the higher) for the most serious of breaches, or 2%/€10 million for those matters considered to be more administrative in nature. Although it would be very surprising if a small business was fined anywhere near these figures, the ICO has already demonstrated their willingness to impose financial penalties against SMEs, albeit paying attention to the business's ability to continue trading following any such monetary penalty.

5. WHERE CAN SMES GET ADDITIONAL HELP/SUPPORT?

There are extensive resources to help you make sure you are compliant by 25 May 2018.

These include:

- the ICO is providing lots of updates for small businesses including a data protection self-assessment toolkit
- law firm Pinsent Masons LLP has a specialist data protection team, offering a range of information and guidance on their Out-Law blog. It also has a dedicated data breach response line which can be contacted 24 hours-a-day, seven days-a-week, on +44(0) 20 7741 6127
- Hiscox offers a cyber and data risks insurance policy designed to provide rapid, expert response in the event of a data breach, which can (among other things) help a firm to comply with the stringent notification requirements of the GDPR
- data protection tips can be found on the Hiscox small business blog.