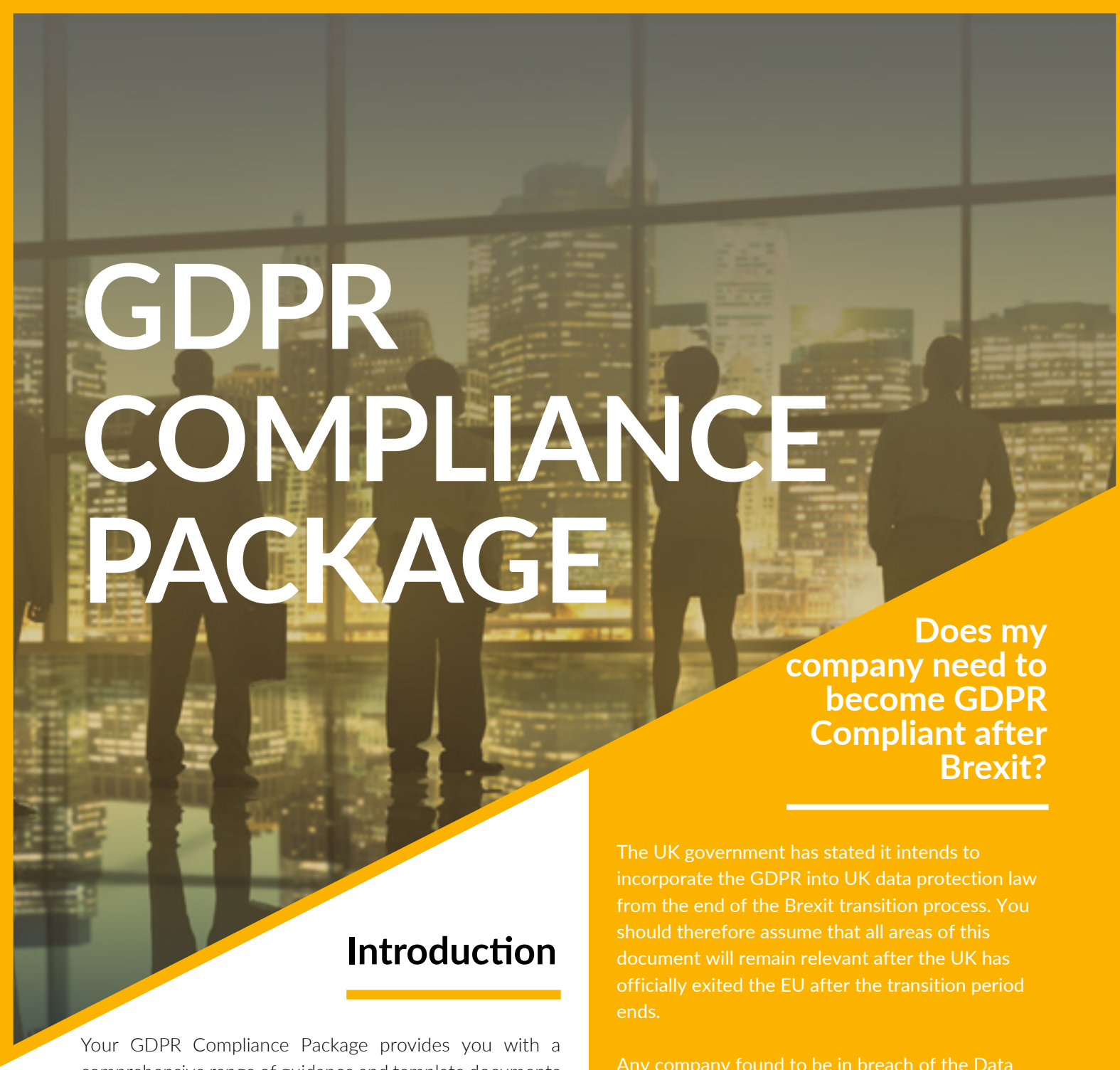


GDPR COMPLIANCE PACKAGE

Introduction

Your GDPR Compliance Package provides you with a comprehensive range of guidance and template documents which will allow your company to become GDPR compliant.

What is GDPR?

GDPR stands for the General Data Protection Regulation. It is a set of regulations brought in by the European Union, and later incorporated by the UK into law under the Data Protection Act 2018, to strengthen the rights of individuals in relation to how companies collect, process and store their data.

Does my company need to become GDPR Compliant after Brexit?

The UK government has stated it intends to incorporate the GDPR into UK data protection law from the end of the Brexit transition process. You should therefore assume that all areas of this document will remain relevant after the UK has officially exited the EU after the transition period ends.

Any company found to be in breach of the Data Protection Act 2018 can receive large fines or criminal prosecution from the Information Commissioner's Office (ICO). You should ensure your company is GDPR compliant to reduce the risk of fines, prosecution, and negative publicity.

How to use this package

You should read all of the information contained in this package, and complete all of the templates and actions outlined in the documentation. This will ensure you are covered for every aspect of GDPR compliance.

Become GDPR - aware

Your company's first step towards GDPR compliance must be to promote awareness of GDPR and its implications. This starts with identifying all of the key stakeholders across your company, and to subsequently appoint project leads from key areas to work alongside each other as part of a wider GDPR working group.

These key areas could range from IT or marketing, to HR and sales. GDPR effects all aspects of company operations, and so each area of your business should be involved to promote awareness. You may want to subsequently plan and record a meeting between yourself and those appointed key leads to brief them on GDPR, compliance policy and its implications for each corresponding team.

You must also initialise your GDPR preparations by appointing a Data Protection Officer. You may also want to appoint a Virtual Data Protection Officer depending upon your company needs.

Remember: although the number of individuals you appoint to data-related roles (either formal or informal) will inevitably vary based upon company size, you must be able to illustrate to regulators, consumers and stakeholders that your company takes GDPR seriously.

1. Find out what data you currently hold

To demonstrate to regulators that your company is collecting, processing and storing data in the appropriate manner, it is critical that you know what data your company currently collects and what that data is being used for at present.

This means your company must conduct an immediate review of all key business functions. As part of that review, your company must subsequently identify the various pieces of data you are collecting, identify where it is being stored and identify how it is being processed. To prove compliance, you must first know exactly what information your company is storing and in what way it is secured.

Next, your company will need to audit existing data storage arrangements and all of the contracts associated with third party processors to ensure that both your company – as well as the companies you do business with – are fulfilling all GDPR requirements regarding data processors and the deployment of appropriate safeguards.

2. Review all third-party contracts

One of the greatest threats your company is likely to face whilst working to comply with GDPR may not actually be how your company uses and processes data. Instead, your biggest hurdle could turn out to be how your company's partners, vendors or suppliers use and process data.

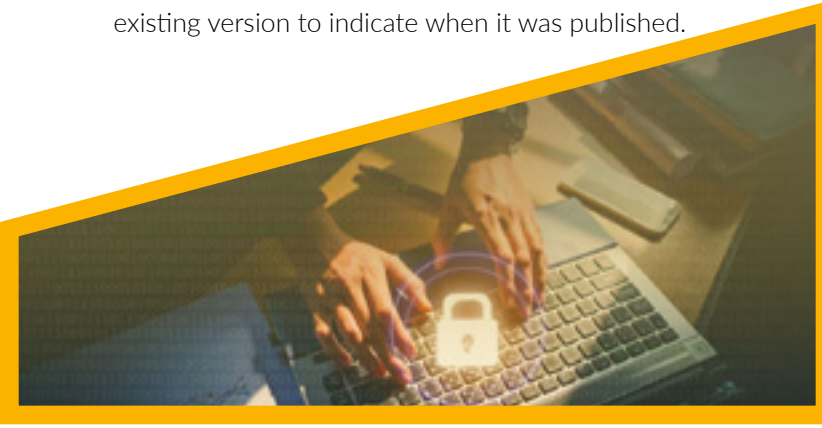
As a data controller, it rests with you and your company to conduct a thorough review of all existing suppliers, vendors, partners or other stakeholders to ensure they are GDPR compliant. You should aim to secure a written contractual agreement explicitly defining the responsibilities, liabilities and associated processes being carried out by each party – and more importantly how those processes exist within full compliance of GDPR.

3. Update your privacy policy

If you have an existing privacy policy in place on your website, the changes to data protection introduced by GDPR will mean that you must now make substantial changes to your online privacy policy. Likewise, if you do not currently have a privacy policy visible on your company website, it is crucial that you now add this information.

A company's privacy policy is an outline that lets visitors to your company's website know what data you may be collecting, how you will ultimately use that data and how you will store it. GDPR has introduced explicit requirements in terms of what you must include in your company privacy policy – and it is also worth bearing in mind that data you collected prior to 25 May 2018 may no longer be valid under new consent rules.

Bearing that in mind, you will need to carefully and clearly word your privacy policy, and clearly record and label your existing version to indicate when it was published.



4. Identify your legal basis for processing data

As part of your company's review of existing data, you must also audit your company's processing activities to assess why they are necessary. Your company must subsequently be able to assign all processing activities a defined category, as specified under GDPR, in order to explain the legal basis for each activity.

For reference, the most common legal basis companies select for their processing activities is 'legitimate interest' – but there are a range of options to choose from.

The legal basis you choose to represent each processing activity is crucial, as this will dictate how you are permitted to collect required data and how long you should store it. If your company needs to carry out high-risk processing activities, you might additionally be required to complete a Data Protection Impact Assessment.

5. How you collect consent

Another aspect of the internal auditing procedures you must carry out, is to conduct a review outlining how you request, capture and store consent.

GDPR has introduced stringent changes in terms of consent. You need to verify ages or obtain parental permission if processing the data of children. You will also be expected to display a short privacy statement at the point of collection, explaining why you are collecting data, what individuals are consenting to by supplying that data, and how they can withdraw their consent at a later date, if they so choose.

Under GDPR, consent must be freely given, unambiguous and informed. This means you cannot collect consent using pre-ticked boxes, and you should identify any third-parties that may ultimately be involved in the storing or processing of data.

You will also be expected to store captured consent preferences in an easy-to-understand way that will enable you to quickly respond to and resolve requests to change consent preferences.

6. Ensure you are protecting individual rights

GDPR has been implemented with the rights of European Union citizens in mind. The sweeping changes companies are now being forced to implement are designed to improve life for individuals and protect their rights. With that in mind, your company must be able to demonstrate that you have implemented identifiable processes that uphold those rights.

These processes may include, but are not limited to how your company:

- Deletes data
- Deals with data requests
- Provides requested data
- Amends incorrect data
- Shares or transfers data
- Handles a data breach

The actual processes that apply to your company will depend on your own business and how it collects, processes and stores its own data.

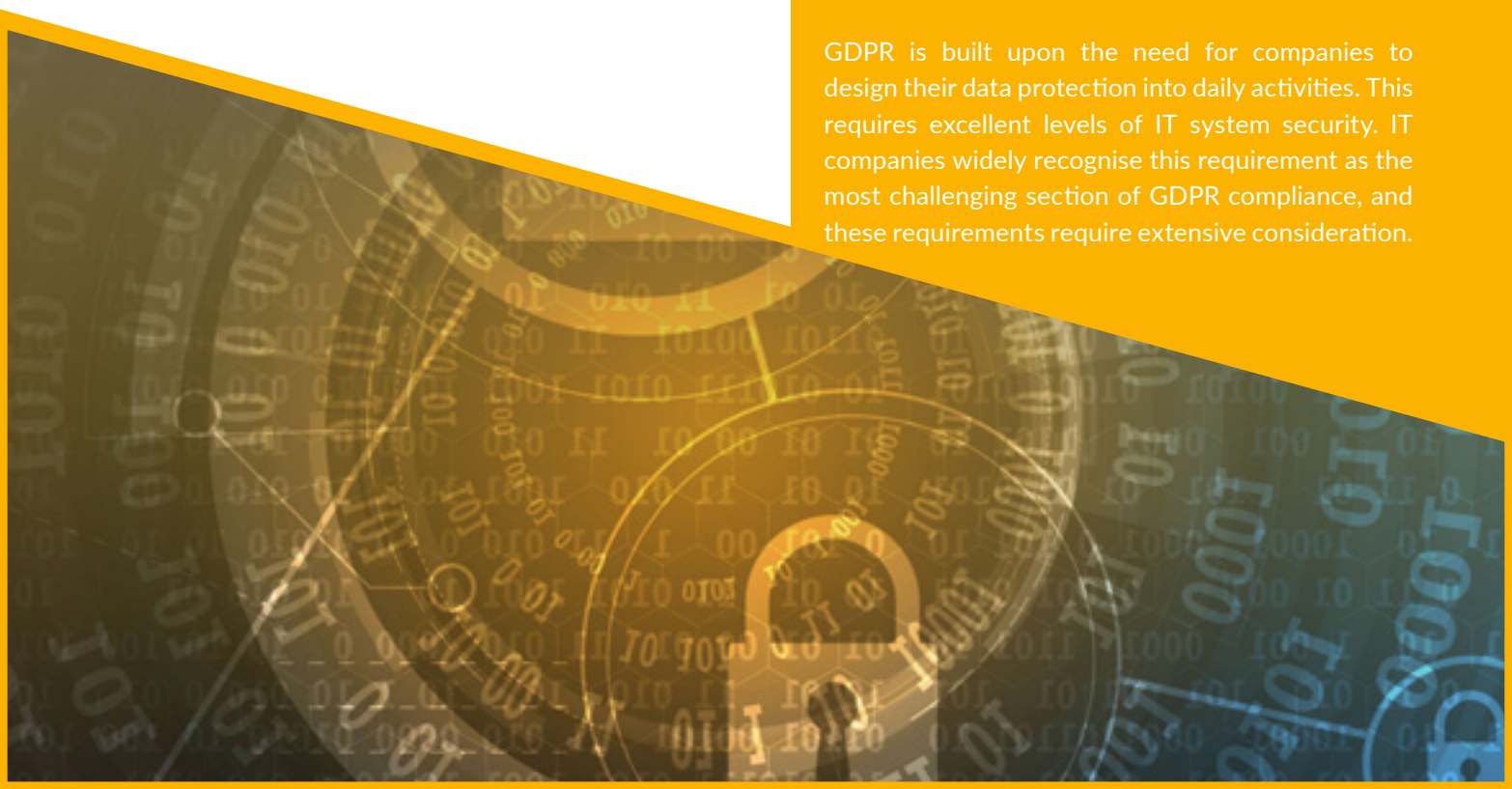
7. Review and enhance your company's data security

One major hurdle GDPR has introduced is the demand for greater data security that some small companies are not likely to have previously had in place.

As part of your GDPR compliance, your company will need to assess existing IT security measures and identify any vulnerabilities.

Assessing your company's existing IT data security measures is a central requirement of GDPR compliance, and one of the most challenging. GDPR requires your company to carry out data protection by design, meaning you must integrate data protection rules into all your processing activities and business practices. You must carry out a thorough review of your data protection policies and practices to ensure your company complies with GDPR IT security requirements. Your company is responsible for carrying out this review and putting in place the correct processes. This review should include penetration testing, upgrades to your current IT systems and vulnerability assessments. This part of the GDPR plan highlights the need for data restoration processes, secure system development and business resilience.

GDPR is built upon the need for companies to design their data protection into daily activities. This requires excellent levels of IT system security. IT companies widely recognise this requirement as the most challenging section of GDPR compliance, and these requirements require extensive consideration.



8. Always be prepared

GDPR is bound to impact virtually every aspect of your business. Therefore, a huge aspect of your company's GDPR plan will need to revolve around organisational readiness and adequate preparation. Implementation is bound to vary from company to company, based upon each organisation's specific processes and business needs.

There are several key steps all companies may want to perform to demonstrate to both regulators, as well as clients, a firm commitment to uphold their GDPR obligations. Examples include: carrying out regular internal data protection audits, staff data protection training and having documented data protection policies, such as a bring your own device (BYOD) policy and a clear desk policy.

These steps should be broadly outlined as part of your company's GDPR strategy document, and are likely to include organisation-wide commitments from all stakeholders.

9. Do not become complacent

The most crucial aspect of your company's GDPR compliance is to ensure you're constantly up-to-date in meeting all of your obligations. Because GDPR is such a sweeping piece of legislation, full compliance requires constant vigilance and ongoing compliance checks.

That means your company should be carrying out regular readiness checks, reviews and audits to find out whether your processes have changed and must be amended or documented accordingly. Likewise, your company must keep abreast of any regulatory updates that could be made to existing GDPR legislation in the future.

These recurring checks are crucial to ensure your company remains GDPR compliant.