WHITE PAPER

DATA PROTECTION:
A COMPREHENSIVE GUIDE TO THE GDPR

www.bulletproof.co.uk

DATA PROTECTION: A COMPREHENSIVE GUIDE TO THE GDPR

"The GDPR is a challenge for many organisations, owing to its far-reaching and often transformative impacts to businesses across the UK"

INTRODUCTION

The GDPR is a challenge for many organisations, owing to its far-reaching and often transformative impacts to businesses across the UK and beyond. With the Information Commissionner's Office (ICO) able to levy large fines for both non-compliance and data breaches, it's critical that every organisation understands their requirements under this data protection regulation.

This white paper will provide a high-level understanding of the GDPR's strategic aims and the challenges these present to UK businesses. In addition, it will present helpful tips for interpreting, implementing and maintaining the new legislation and a business' approach to managing personal data.

WHAT IS THE GDPR?

The General Data Protection Regulation (GDPR) is a modern overhaul of data privacy regulations, designed to reflect the digital age. With the evolution and widespread use of the internet, the rise of social media and the ubiquitous use of smartphones, tablets and IoT devices, we leave a trail of vast and often unchecked amounts of personal data behind us. The old regulation was struggling to address the contemporary uses of personal data, making a regulatory revamp like the GDPR inevitable.

The GDPR is an EU-wide initiative, unifying all existing data protection regulations. In the United Kingdom, the Data Protection Act (DPA) 2018 acts as the implementation of the GDPR, tailored to how the regulation applies in the UK.

At its core, the GDPR's goals are to increase individuals' rights and enhance privacy, transparency, and accountability. It does this by determining how personal data of EU residents must be handled, what permissions are needed, and how this data can be lawfully collected, processed, and protected. It also gives data subjects more rights and control over what can and cannot be done with their data.

We can split the GDPR's aims into six main areas:

1. To strengthen individuals' rights
2. To create a clear and robust set of rules concerning the free movement of data
3. To ensure consistency of the rules
4. To set global data protection standards
5. To provide a high level of data protection across all industries
6. To enforce an effective and efficient response to data breaches

"The GDPR is an EU-wide initiative, unifying all existing data protection regulations"

WHO DOES THE GDPR APPLY TO?

"The GDPR applies to anyone processing individual information of an EU resident. This applies no matter where in the world your business is based, or the size of the business"

The GDPR applies to any business, organisation or body that holds or processes information of EU residents (also known as data subjects). This could be a retail business that holds personally identifiable information on customers, such as delivery addresses and card details. It could also be a school that holds personal data of their staff and students such as dates of birth and contact numbers.

DATA CONTROLLERS AND PROCESSORS

In legal terms, the GDPR applies to data controllers and data processors. You are deemed to be a data controller if you are the one who decides the means and intended purposes of data processing. Similarly, you are considered a data processor if you process data on behalf of the controller. For example, if a bank takes customers' personal data (names, addresses etc.) but stores this information with a third-party data centre, in this instance the bank is the data controller and the data centre is the processor.

If you are a processor, you are required to ensure that the maintenance and processing of personal data is in-line with the regulations. This means if your business or organisation is responsible for a data breach, then legally, you are significantly more liable.

As a processor, you must follow all instructions referring to the processing of personal data (given by the controller) to the letter, whilst also ensuring security best practices are always upheld. However, if you are the controller, your main responsibilities concern how personal data is to be processed. You will decide what can and cannot be done.

Put simply, the GDPR applies to any organisation or business processing individual information of an EU resident. This applies no matter where in the world your business is based, or the size of your business.

IMPORTANT ARTICLES

The Data Protection Act 2018 (DPA 2018) is the UK's implementation of the GDPR and will apply to just about every business or organisation. Short of reading through all 99 Articles, we have provided details on those we feel will have the most impact on businesses.

Article 5: Principles relating to the processing of personal data

In short, Article 5 shapes the responsibilities for the data controller and what they're accountable for. The data controller must demonstrate that data is:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant, and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data

Article 6: Lawfulness of processing

This Article states that data processing shall be lawful if any (and at least one) of the below apply:

- The data subject has given consent to the processing of their personal data for specific purposes
- Processing is necessary for the performance of a contract or compliance with a legal obligation
- Processing is necessary to protect the vital interests of data subjects
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority
- Processing is necessary for the purpose of the legitimate interests pursued by the controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject

Article 7: Conditions for consent

This Article addresses the consent of data processing. Data controllers must be able to demonstrate that:

- A data subject has consented to the processing of his or her personal data
- If written consent is given, it was presented in a manner clearly distinguishable from other matters
- A data subject shall have the right to withdraw their consent at any time

Article 15: Right of access by the data subject

With this Article, the data subjects have the right to obtain confirmation of whether the controller is processing any personal data concerning them. In addition, the subject has the right to the following information:

- The purpose of the processing
- The categories of personal data concerned
- The recipients of the personal data, particularly those in third countries or international organisations
- Where transferred to a third country or international organisation, the data subject has the right to be informed of the appropriate safegaurds relating to the transfer
- Where possible, the envisaged period the personal data will be stored
- The right to request the rectification, erasure, or to restrict the processing of personal data
- Where the personal data is not collected from the data subject, any available information as to the source
- The existance of automated decision making, including profiling, meaningful information about the logic involved, and the significance and envisaged consequences of such processing for the data subject

Article 17: Right to erasure ("right to be forgotten")

The data subject should have the right for all personal data concerning them to be erased. Once this request has been made, the data controller is obligated to delete all the personal data concerning them in a timely fashion, assuming that:

- The data is no longer needed
- The data subject withdraws consent and there are no legal grounds to continue processing personal data.

There are exceptions when data may not be erased. Such as:

- Compliance with a legal obligation
- Reasons of public interest
- Archiving purposes on the grounds of public interest or scientific/historical research

Article 24: Responsibility of the controller

The controller will implement appropriate measures to ensure that processes are performed in accordance with the regulation. This can be achieved by deploying a data protection policy or gaining a certification (ISO 27001 etc).

Article 32: Security of processing

The controller and processor will implement appropriate technical and organisational measures to ensure the level of security is appropriate to the risk. This will include the below:

- The pseudonymisation and encryption of personal data
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process of regular testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing

Adherence to an approved code of conduct or an approved certification mechanism (such as ISO 27001) may be used as an element by which to demonstrate compliance with the requirements set out in this Article.

Article 33: Notification of a personal data breach

In the case of a personal data breach where there is a risk to the data subject, the controller shall without undue delay and, where possible, within 72 hours after having become aware of it, notify the personal data breach to the supervisory authority (for the UK this is the ICO). The notification must:

- Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects and personal data records concerned
- Communicate the name and the contact details of the Data Protection Officer or other contact where more information can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by the controller to address the breach, including measures to mitigate its possible adverse effects
- Document any personal data breaches, comprising the facts relating to the breach, its effects and the remedial action taken

Article 35: Data Protection Impact Assessment (DPIA)

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

Article 37: Designation of the data protection officer

The controller and processor shall designate a Data Protection Officer (DPO) when:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10

Article 46: Transfers subject to appropriate safeguards

Processors and controllers may only transfer data to a third country or international organisation if they can provide the appropriate safeguards. This is to say that information must be protected to the highest possible standards throughout.

ROLE OF THE DPO

The data protection officer (DPO) should be a single appointed person, with a good knowledge of data protection. The chosen individual can be an existing member of staff, a newly appointed member of staff, or even an outsourced consultant.

A DPO must not have any conflict of interest when it comes to fulfilling their role, for example, a member of your IT team would be unlikely to act as your DPO due to their role in managing personal data. A person responsible for determining the means and purposes of processing personal data cannot be a DPO due to the conflict of interest.

The DPO will be the point of contact for any data protection queries, be it from official regulatory bodies or data subjects themselves – and remember that data subjects include your own employees. The DPO will also ensure the business remains compliant with the GDPR by informing and advising controllers, processors and all employees involved with data protection.

The GDPR is a continuous process. Once implemented, regulation must be maintained. As a business you must always maintain the highest levels of security where personal data is concerned, be it via technology such as up-to-date firewalls or through management processes. A dedicated DPO will be able to constantly assess, advise and oversee every aspect of GDPR compliance.

WHAT IS MEANT BY GDPR IMPLEMENTATION?

The notion of GDPR implementation is a difficult one to define. The implementation process for one company or organisation may be completely different to another's. Much will depend on the nature of the business as well as the processes and technical platforms already in place. Broadly speaking, when we talk about GDPR implementation we are talking about the steps that will have to be taken to be compliant.

Implementation will involve a complete review of your current data management and processing practices. This will include technical, physical and management aspects.

As your cyber security posture needs to be as strong as it can possibly be, this will include testing or upgrading the systems you have in place.

Designing and rolling out training programmes for relevant staff will also come under implementation, as well as establishing adequate data management processes and even pushing out updated and relevant privacy policies. In short – implementation covers a wide range of aspects that can be difficult to keep track of.

If all of this seems like a bureaucratic nightmare, then a gap analysis will be a good place to start.

MYTH BUSTERS

Since its announcement, there have been many misconceptions regarding the GDPR. Ultimately, it aims to protect the personal data of individuals in an ever more connected age. It stands to do this by clearly outlining the responsibilities of businesses and organisations in regard to collecting and processing data.

Some current misconceptions are:

Implementation is going to be expensive

Naturally, this is one of the most pressing concerns for businesses, particularly smaller ones. However, the cost of GDPR implementation will vary depending on many factors, such as the size of your business, the amount of data being processed, your current level of compliance and the areas in which you are non-compliant.

No single approach to compliance will work for all. It could be that your systems are as protected as they can be and that you have the relevant management processes in place.

In which case all that's required are some minor updates to your terms and conditions. If this is the case, implementation will not cost much at all.

For some, your business model may have to be redefined and new systems introduced. If this is the case, costs will be considerably higher. However, noncompliance can lead to large fines that will cost your business more than the costs of implementation, as well as the risk of reputational damage and potential legal action.

Mandatory reporting of data breaches is designed to punish organisations

The Supervisory Authorities (the ICO in the UK) review reported data breaches and consider many factors in determining any fines. They must ensure that their fines are proportionate. They are not out to punish organisations unfairly and, often, they don't fine at all.

By making organisations report breaches that pose a risk to the data subject, the Supervisory Authorities are ensuring companies don't hide any breaches to avoid reputational damage. By setting a timescale, they make sure the breach is dealt with quickly, thus hopefully reducing the impact and potential future risk. It is key when reporting to the Supervisory Authority that businesses provide the information mandated and there is good cooperation. Failure to do this is more likely to lead to a higher fine.

A DPO will be a costly asset

A current member of staff can be your appointed DPO providing their current role does not present a conflict of interest.

Perhaps the most cost-effective method however, is outsourcing. Having an appointed DPO doesn't mean they have to be in the building at all times. With an agreed amount of contact time per month, an outsourced DPO can carry out the same duties, but at a considerably reduced cost.

Companies and organisations must have a DPO

This is not necessarily true. Whilst it's a good rule to assume that you will need one, there are instances where a DPO is not necessary. The GDPR states that a DPO will be appointed if:

- The processing is carried out by a public authority or body, except for courts acting in their judicial capacity
- The core activities of the controller or the processor consist of processing operations which, by virtue of their nature, scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale
- The core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10

If you can prove your business is not subject to any of these, then you will not have to appoint a DPO. However, it is in your best interest to do so. A DPO can manage all things GDPR going forward and acts as a single point of contact for data protection related matters.

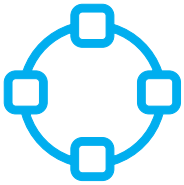
Nothing will change after Brexit

The UK's withdrawl agreement permits a transition period, running until December 31 2020, during which time current EU rules continue to apply in the UK and negotiations around what happens next can begin. During the transition period, the UK government and the EU are negotiating for a data protection arrangement which suits both parties. That might be an adequacy decision, a Privacy Shield-type agreement, or another arrangement that permits data to move freely between the UK and EU.

The key thing is here that The DPA (2018) is the UK's implementation of the GDPR so, even if you are processing only UK residents' data, the requirements of the GDPR will still be in place.

TEN STEPS TO GDPR COMPLIANCE

The journey towards compliance with the GDPR is not necessarily an easy one. For those organisations in need of some guidance, we have compiled a list of 10 steps to get you started:



1. DATA FLOW MAPPING

This enlightening process is where you identify all the processes in your business that handle personal data then map the flow of that personal data. A data flow map should record where it enters your business, who accesses it, where it's stored, how it's stored, where it leaves the business, and so on. Gaining a complete picture will involve the input of many different people in the business.

2. RECORDS OF PROCESSING

You must keep records of processing in order to document what personal data you are processing, the purposes of processing, where the personal data is transferred to, security measures to protect it, how long it is kept for (and etc). A lot of this will be easier to complete once you have undertaken your data mapping.

3. RISK FRAMEWORK & RISK ASSESSMENTS

A key part of the GDPR is being able to assess the risk to both the business and to the data subject of the processing of personal data. This requires a risk framework to be in-place so new and existing risks can consistently be assessed.

4. LAWFUL BASIS FOR PROCESSING

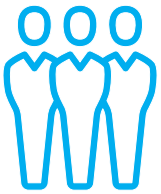
When processing personal data you must have a lawful basis to do so. If you do not have one, you cannot process personal data. Understand what personal data you are processing, identify what the lawful basis is, and document it.

5. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

Data protection impact assessments must be carried out for processes and activities that may present a high risk to the data subject. A DPIA is a risk assessment that helps to ensure that threats to data subjects have been considered and suitable controls implemented to mitigate these risks.

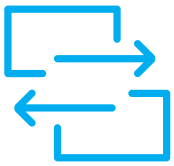
6. PRIVACY NOTICE

You must provide privacy notices (typically on your website) to data subjects in order to be transparent on what data you are collecting, the purpose for processing, the lawful basis, where the data is being shared, where it is being stored, how long it is being kept for, and so on.



7. THIRD-PARTY RELATIONSHIPS

As part of your data mapping you will have identified third parties that you share personal data with. You need to ensure you have suitable contracts in place with these organisations to make sure they understand their data protection obligations.



8. INTERNATIONAL TRANSFERS

Your data mapping should have also identified where you might be transferring personal data outside of the EU. In these circumstances you need to consider what additional safeguards will be needed to protect this personal data in the same way as it would be if it was in the EU.

9. POLICIES & PROCEDURES

Accountability under the GDPR means companies have to not only protect the privacy of the personal data they hold, but also demonstrate they are doing so. Having robust policies and procedures helps with this and makes sure everyone in the business understands what needs to be done and their responsibilities.

10. APPOINTING A DPO

You may need to appoint a Data Protection Officer. This is a mandatory requirement for public bodies, or businesses that, as part of their core activities process large quantities of special categories of personal data (such as health data, sexual orientation, etc.) or if they conduct regular and systematic monitoring of data subjects on a large scale. Even if you're not technically required to have a DPO under the GDPR, it's good practice to appoint someone to be responsible for data protection within your organisation. Outsourcing this to a reputable company on a retainer basis is often the most cost-effective way of achieving this.

BUSINESS CHALLENGES

From everything we've shown so far, it should be no surprise that maintaining compliance with the GDPR is likely to be more challenging than its predecessor, with this wide-reaching legislation having transformational effect on some businesses. Key business challenges include:

Mandatory notification of a data breach

If your company has ever suffered a cyberattack, you'll understand the pressure this can cause. As mentioned in Article 33, in the case of a data breach where there is a risk to data sbjects, you'll need to notify the Supervisory Authority within 72 hours. Here in the UK, that's the Information Commissioner's Office (ICO). You must:

- Describe the nature of the personal data breach, including the categories and approximate numbers of data subjects and the personal data records
- Give the contact details of your DPO or other contact point
- Outline the likely consequences of the data breach
- Describe the measures taken to address the personal data breach, including mitigation

The strict 72-hour reporting time frame can make this task a challenge however, the ICO does recognise that you may have to do some investigation work to be able to provide full details. The key is to provide what you can without undue delay and within 72 hours of becoming aware of the breach.

Initial cost of compliance

Many companies have already discovered that the drain on time, resources and funds to become compliant with the GDPR can be quite high if not done efficiently. Enlisting experts to come in and help on a consultancy basis can save your organisation a lot of time and money, though it pays to shop around. Make sure the supplier gives you confidence that they have the right experience and certifications, and that you're getting a cost-effective package.

Resource planning

Even if you are not required to appoint a DPO under the GDPR, someone in the business still needs to be responsible for data privacy within your organisation. This person will be responsible for contacting the ICO, talking to data subjects, handing data subject access requests and more. The skills this requires makes it a challenge to resource from existing staff and costly to hire. Instead, consider an outsourced DPO. This delivers the required skill in a cost-effective monthly retainer.

Implications of consent

With the requirements over the use of consent being stricter under the GDPR, companies may need to make some changes to accommodate these and ensure they stay compliant. This will include:

- Consent must be freely given. Data subjects must not be forced to give consent and should have to take an action to give consent and thus explicitly opt in. Pre-checked boxes and asking data subjects to opt out is not allowed under the GDPR
- Consent must be infomed. the data subject needs to know the identity of the controller and the purposes of processing as a minimum
- For written consent, the text explaining consent needs to be easy to understand and clearly separated from any other requirements (such as there for signatures, etc)
- Consent to processing activities must be granular. If you want to ask the customer to consent to email marketing, telephone marketing and contact by post, each one will require specific, individual consent. You cannot have one tick box that covers everything
- Consent must be as easy to withdraw as it was to give. If you ticked a box to give consent, you should be able to untick a box to withdraw it
- Records of consent must be kept to prove consent was given and what it was given for and when
- Organisations may have to update privacy notices, internal policies & procedures, marketing emails, introduce cookie consent banners, implement new policies and, train staff

SUMMARY

The GDPR is not a technically prescriptive standard, rather it defines what permissions should be sought from EU/UK citizens and how such data can be lawfully collected, processed and protected. This means there's no easy document to follow to become compliant with the GDPR, though there are companies out there who can help, from initial gap analyses to full compliance implementation and beyond.

The GDPR represents the biggest change to data protection law in over 20 years. So long as you are taking active steps and present every intention of being compliant in a transparent way, you can most likely avoid any repercussions. However, to avoid hefty fines and PR nightmares, it pays to take compliance with the GDPR seriously.

"The GDPR represents the biggest change to data protection law in over ten years and so long as you are taking active steps and present every intention of being compliant in a transparent way, you can most likely avoid any repercussions"

Get in touch today to ensure that your business and your customers are protected:

+44 (0)1438 532 900

contact@bulletproof.co.uk

www.twitter.com/bulletproofsec

BULLET PROOF

01438 532 900

contact@bulletproof.co.uk

www.bulletproof.co.uk