BIG PARTNERSHIP

The Ultimate Guide to GDPR:

Are you ready to “opt in”?

On 25th May 2018, the General Data Protection Regulations – otherwise known as 'GDPR' – was enforced, bringing the biggest change to data protection legislation in 20 years.

BIG Partnership has done the research and consulted with lawyers to prepare this ultimate guide to help your organisation to understand the key changes that GDPR brings to existing data protection laws. We'll cover what GDPR is and why it has happened. We also have a handy checklist to help ensure your business is prepared. Finally, we've looked at how the new regulations can benefit you as a business and a consumer.

What is GDPR?

In a nutshell, the GDPR updates existing data protection law to give individuals greater control over their personal information and improve how organisations process personal data. Improving privacy, increasing trust, and addressing the balance of control over personal data is a key feature of this new legislation.

Given the perceived complexity of the GDPR, it may be tempting to take the ostrich approach and bury your head in the sand. However, the GDPR is now fully effective across the UK and European Union (EU) and you cannot afford to ignore it.

The consequence of non-compliance has the potential to be significant, with organisations found in breach of GDPR facing fines of up to 4% of annual global turnover or €20 million - whichever is greater. In the UK, this will be governed and enforced by the UK Information Commissioner's Office (ICO).

> **Organisations found in breach of GDPR will face fines of up to 4% of annual global turnover or €20 million – whichever is greater.**

To help organisations navigate these changes, the ICO has created a comprehensive summary of the GDPR on its website. Loaded with some easy-to-digest guides and checklists, this is a good place to start if you are behind in your GDPR plans or you simply want to find out more about a specific area of the GDPR in practice.

Why is GDPR happening now?

Over the last decade, the digital landscape has rapidly evolved, with digital growth being driven by more affordable smartphones and mobile data plans. In addition, the growth of Over The Top services ("OTT") has increased significantly, with services such as Skype, Gmail, Facebook messenger and WhatsApp becoming a normal part of our everyday life.

With multiple digital touch points to engage with individuals, personal information is constantly being requested, stored and exchanged as part of these OTT services. Whilst data protection legislation is already in place to ensure that data collection and processing is managed responsibly, the world has moved on, and much of this legislation has become a bit dated.

Data hacks and breaches have also hit the headlines in recent years, heightening concerns about the security of stored data, as well as the level of personal information being requested by organisations in return for access to services, products, and digital information.

This changed digital landscape has undoubtedly driven the need for the new GDPR, which has now replaced the Data Protection Directive 1995. Whilst there will be similarities with the UK Data Protection Act 1998 (DPA), the GDPR will be more extensive in scope and application.

So, should you be worrying right now if you have only just worked out what GDPR stands for? The honest answer is yes, but this all really depends on the size, type and complexity of your business and, more importantly, whether you were already compliant with existing data protection law before GDPR came into force.

GDPR in seven steps

As the saying goes, better late than never. So, for those organisations that are still transitioning to comply with GDPR, or simply want to check that the core requirements are covered, here are some of the key things to consider to ensure you are on track to being ‘GDPR ready’.

> **From your PR agency to your print suppliers and events companies, if personal data is involved, these external parties (or 'processors') also need to be part of your planning.**

1 Make sure everyone is in the know

Ensuring that all the relevant people within your organisation are aware that GDPR is now fully effective and how the changes will impact your day-to-day business is an essential first step. Involving employees at all levels in your plans and openly communicating the changes that you will make in response to the GDPR will help to get buy-in and commitment to handle personal data in line with the GDPR.

At this stage, don't forget about the external parties that may be handling personal data on your behalf. From your PR agency to your print suppliers and events companies, if personal data is involved, these external parties (or 'processors' as they are known under the GDPR) also need to be part of your planning.

If you were already fully compliant with the Data Protection Act (DPA), the impact of these changes is likely to be less significant for your organisation than those that have been somewhat relaxed with processing personal data.

If you really don't know where to start, the ICO's guide, 'Preparing for the General Data Protection Regulation (GDPR): 12 steps to take now' provides an easy to understand overview of the GDPR and what is needed to comply.

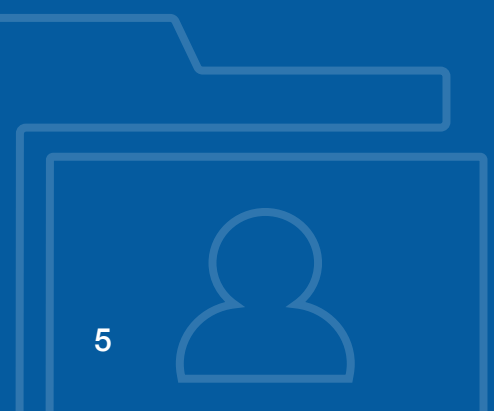
2 Understand what personal data means in your business

Under the GDPR, personal data is 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.'

Essentially, if an individual can be identified in any way through information you process, it will be subject to the GDPR. Despite some uncertainty over how and if the GDPR will apply to personal data in a professional capacity, according to the ICO, the GDPR will also apply to business-to-business personal data processing.

With that said, applying the 'rules' of the GDPR when processing any type of personal data is the best approach to be sure that you are within the law and to reduce the risk of any data breaches.

If you are still unsure of what constitutes as personal data within your business and how the GDPR applies to you, you can explore the ICO's 'Getting ready for the GDPR resources' page with checklists, FAQs and advice on all things GDPR related.

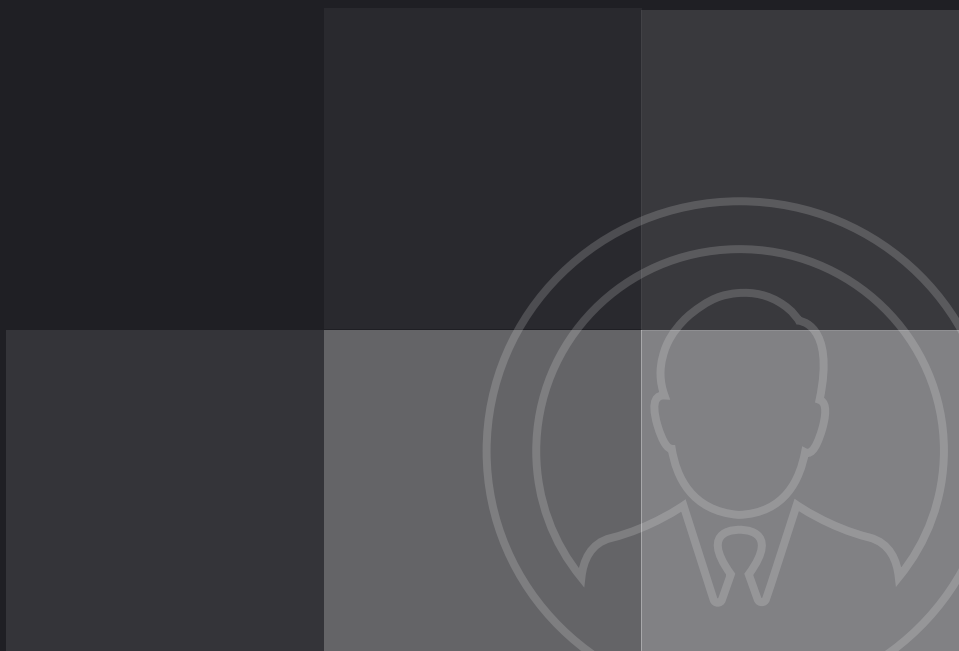


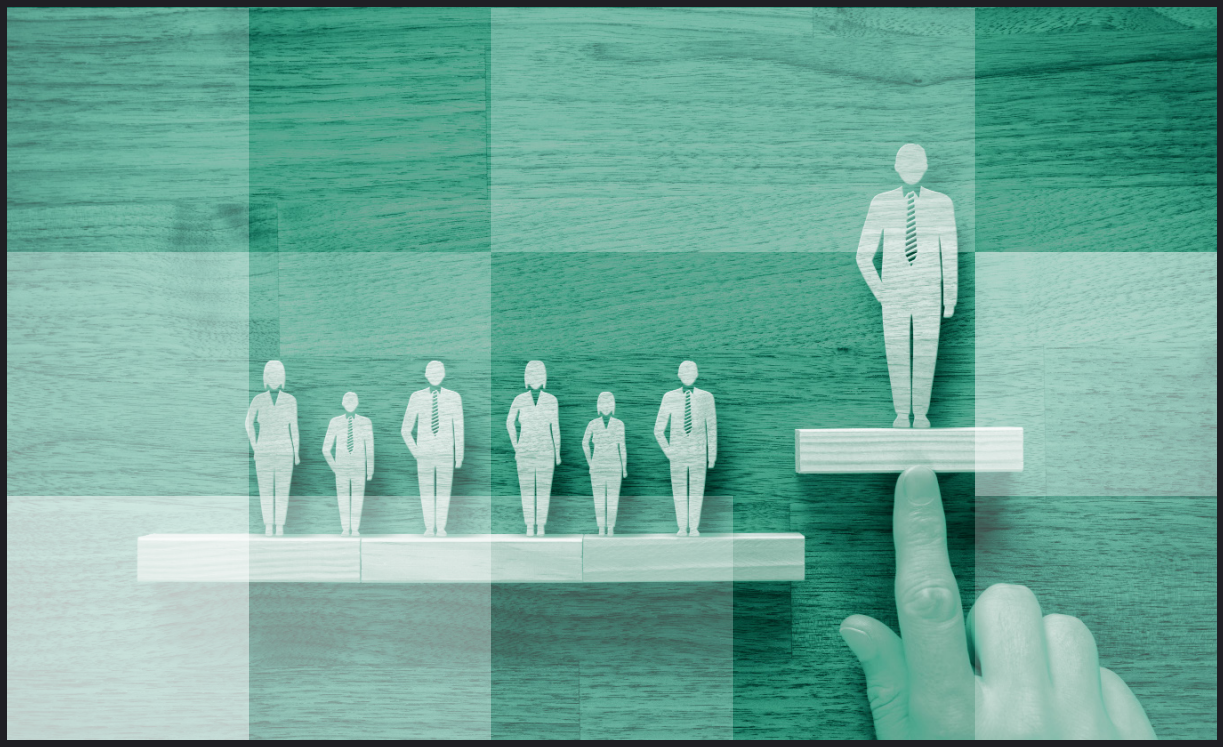
> **Personal data is 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.**

3 Consider appointing a designated GDPR lead

As you embark on the journey to prepare your business for the GDPR changes, you may want to consider appointing a steering group and designated individuals to take on the role of data protection expert within your organisation.

A designated point of contact for the wider business will be useful for employees and suppliers to obtain more information on your specific data protection policies and processes, in addition to reporting any risk of non-compliance or an actual data breach now that GDPR is in place.





If you are a public authority, or if you carry out certain types of processing activities, you may need to formally appoint a Data Protection Officer (DPO) under the GDPR. For all other companies, appointing this role is voluntary – but taking the step of appointing a DPO demonstrates a level of commitment to good data protection practice.

Either way, it is important to plan for how your organisation will operate under the GDPR in practice, as organisations found in breach of GDPR could face fines of up to 4% of annual global turnover or €20 million - whichever is greater.

Fines aside, the negative impact on brand value and consumer trust could be the greatest cost of all. How you respond to a personal data breach and demonstrate to the ICO and your customers that you have taken the necessary steps to manage personal data responsibly, is equally as important as the steps you are taking now to ensure you will operate responsibly under GDPR on a day-to-day basis.

4 Map your data and address the gaps

Undertaking a data audit and documenting any personal data that you process will provide a complete understanding of what you currently hold within your organisation.

This data audit will help to identify any gaps in your personal data processes that need to be addressed. Mapping this data from the point it was obtained will also help you to respond to personal data requests from individuals under the GDPR, and to manage any data breaches swiftly and responsibly for the ICO.

Under the GDPR, all organisations are required to document personal data to a certain extent. However, a more formal process for this will be required if you are an organisation with 250 or more employees. The ICO website outlines the formal requirements for documenting personal data, including when this is mandatory.

> **All individuals will have enhanced rights to ask for a copy of the personal information that is held about them and individuals can request that their data is deleted.**

5 To refresh or remove? That is the question

Under the GDPR, you must have a lawful basis for processing this personal data. If your lawful basis is 'consent', individuals will now have greater rights under the GDPR to withdraw their consent at any time.

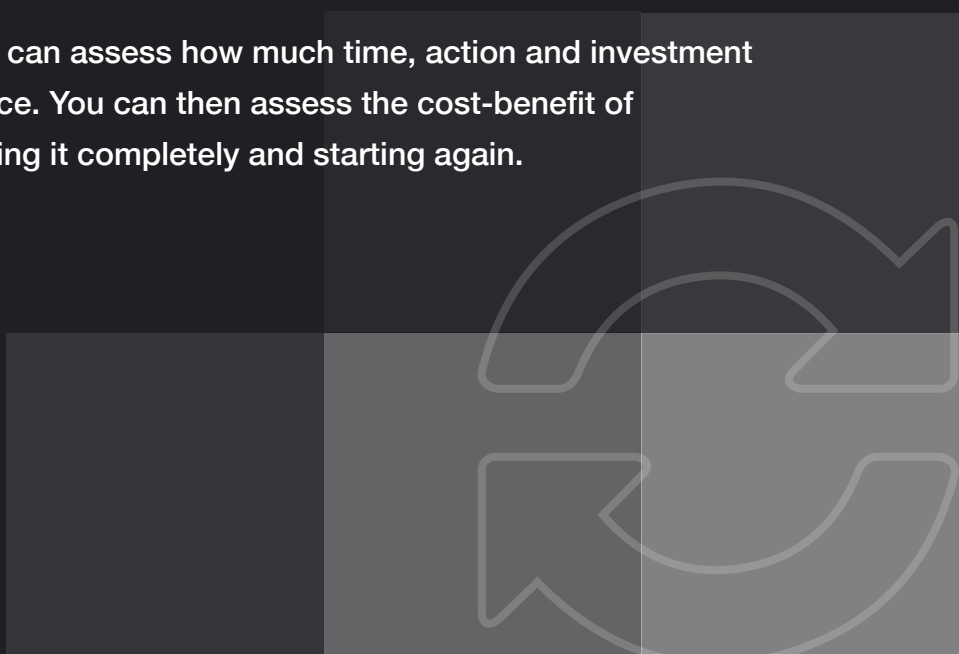
All individuals will have enhanced rights to ask for a copy of the personal information that is held about them and individuals can request that their data is deleted (also known as the "right to be forgotten").

This will be challenging to respond to promptly and fully if you are unsure about the personal data you hold, how this data was obtained, and how this data is being used by your organisation.

One option to consider is taking the 'Wetherspoons approach' and deleting all the personal data that you hold on customers and clients, and then start again. However, this is rather drastic, and most of this personal data may already be compliant.

An alternative approach is to plan for and undertake a personal data audit to identify gaps in your processes. Ideally this will have been done before the GDPR was enforced, but as personal data audits and mapping are recommended under the new regulations to ensure compliance, putting steps in place to undertake this is essential.

Once you have done this, you can assess how much time, action and investment is needed to ensure compliance. You can then assess the cost-benefit of refreshing your data or removing it completely and starting again.



6 Review your personal data protection policies and processes

Transitioning your organisation to become GDPR compliant will no doubt require some changes to your current data protection policies. You may also need to review and update your current processes regarding consent and privacy notices.

Where you are relying on consent to process personal data, if your data processes currently fall short of the GDPR standards for consent, you may want to consider sending a ‘re-permission’ or ‘re-consent’ email to your databases to cleanse this data.

To give control to the individual, you can offer the option to refresh preferences, in addition to the option to ‘unsubscribe’ from your database at any time.

Upon the GDPR coming into force, consent was redefined to require a positive opt-in, meaning that the use of pre-ticked boxes or any other method of default consent will not be considered acceptable. Being clear and concise with your consent terms and how you will process personal data is now an absolute must under the GDPR.

Furthermore, you also need to be sure that you are re-engaging with people who want to be contacted. If you try to have another go at winning back your 'unsubscribes' with this approach, there is a good chance you'll be in breach of the GDPR.

Taking a more positive view, the need to re-consent can also be a good opportunity to show some creativity and re-engage with your existing subscribers. You can offer an incentive to respond, such as a prize draw opportunity or some new preference options. This will give your customers more control, whilst also helping you to improve engagement with your customers with more relevant communications going forward.

A prime example of a creative approach in this context is the GDPR campaign created by Manchester United FC. The football club issued an easy to understand animated video to explain how personal data is being collected and processed with some incentives to re-consent to continue receiving marketing communications from the club.

If you decide to contact your database to re-consent in any way, be sure that you are not contacting any unsubscribers who have already specifically informed you that they do not want to be contacted for marketing communications. Doing this will most definitely be a breach of GDPR and current data protection laws, as the airline Flybe and the carmaker Honda Motor Europe found out following an ICO ruling in 2017.

7 Don’t forget about crisis and response planning

In the same way that organisations will draft holding statements and prepare for a potential crisis, preparing an adequate response plan for a data breach, both in terms of the legal steps required under the GDPR and the steps you need to take to manage concerned customers and the media, is essential to do.

Talk to your PR agency to develop a plan and prepare for potential breaches. This might include media training for key spokespeople, developing a customer care plan to support individuals who might be affected, and preparing holding statements in advance to manage media enquires while you focus on dealing with the requirements of the ICO.

Ensuring that this response plan is clear and available to your employees is also good practice. This will enable you to respond to a personal data breach and exercise damage control without delay, with every individual taking responsibility for GDPR compliance and reporting.

The GDPR isn't just about customer relationships

When it comes to data protection law and processing the personal data of individuals, good practice and a commitment to full compliance with the law is everyone's responsibility.

Updating or putting in place new contractual arrangements with external suppliers and business partners to govern how you will use personal data will help to demonstrate compliance, and mitigate any potential issues with processing personal data beyond your organisation. This might include electronic mailshots, managing your website data processing, or printing personalised invitations for an event.

This step is key for the organisation ('data controller') as well as the supplier ('data processor'), as both will have responsibility to be GDPR compliant when sharing data with one another.

In addition to customers and external facing channels, don't forget about the individuals inside your own organisation. Communicating new data protection policies and GDPR specific notices internally with your employees is vital to ensure that every employee is aware of what the GDPR is, what it means for your business, and what steps you are taking to ensure that you are processing personal data responsibly.

> **Preparing for the new GDPR will require time, planning, and possibly some investment in legal advice to get your house in order.**

With great change comes great opportunity

Without doubt, preparing for the new GDPR will require time, planning, and, depending on the size and complexity of your organisation, possibly some investment in legal advice to get your house in order.

However, the silver lining of the GDPR is the potential to improve customer relationships and trust in your brand, products and organisation. Not to mention increased trust and confidence from your employees and your business network.

Reviewing and updating your databases in line with the GDPR is a chance to generate better quality personal data from customers and clients and ensure personal data is protected and handled with more care.

The requirement to contact these individuals also creates the opportunity to re-establish contact and ignite dormant individuals that will have the potential to become more engaged and valuable to your organisation.

The GDPR also provides a strong business case for proper data audits and investment in better data manage tools. In addition, business activities are likely to be more robust and easier to execute with the GDPR aiming to align data protection laws across the EU and enable data to move more freely and safely between countries.

Finally, better quality data that is lawful, fair, transparent and obtained for a valid purpose with full consent will promote greater trust and engagement between company and individuals.

This puts the customer at the heart of your thinking and actions, which can only be a good thing.

Contact BIG Partnership about GDPR

No-one can advise on GDPR better than a specialist solicitor, and our recommendation is that all businesses employ the advice of a solicitor in the run-up to GDPR. It's also essential to ensure your online and communications strategies are compliant – and that's where we can help. To discuss a GDPR compliant website, crisis strategies or media training, get in touch with your local BIG Partnership team by clicking here.

Author
Natalie Hilton
Account Director – Marketing Strategy