Grant Thornton

An instinct for growth™

Getting data protection right

Applying the General Data Protection Regulation

Contents

What was the fuss about?

Iain Bourne
Head of Personal Information and Privacy

On May 25 2018, data protection law saw its first radical overhaul for 20 years. The months leading up to it were fuelled with GDPR mania and misinformation across the media. But May 25 came and went and – in general – it has been business as usual. No one has received a fine of 4% of their global annual turnover and no one has been banned from processing their customers' personal information.

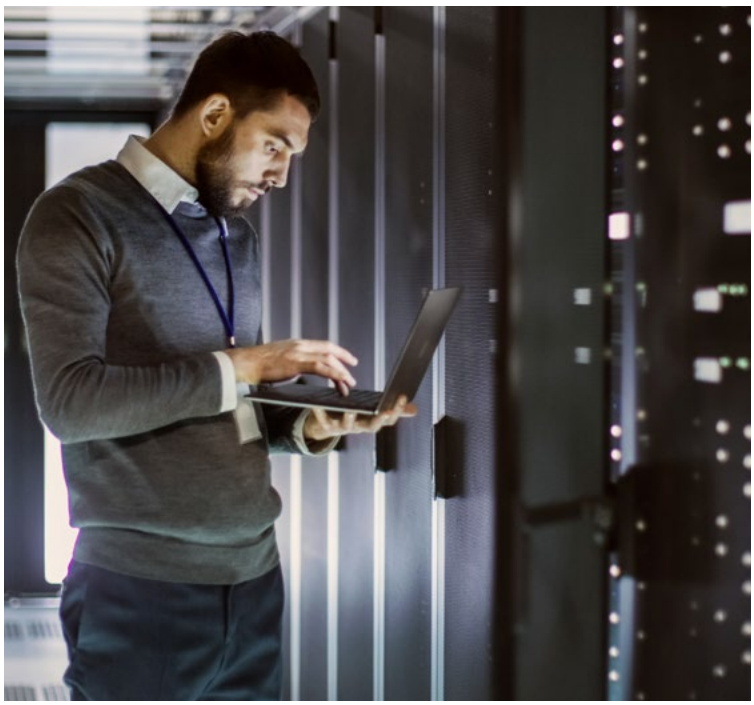
But that doesn't mean they aren't going to be. With such high penalties, it's not worth the risk. By now, firms should have robust GDPR programmes in place, nonetheless, many organisations aren't there just yet and are still working towards achieving compliance. The changes needed are extensive and there isn't a quick fix. At some point a firm will be fined, which may set the bar for enforcement in the future.

Regulations are about more than just compliance. It's about best practice and respecting your customers' data. For some, this will require a degree of cultural change that may take years to truly embed. But they must do this. With over 100 countries having data protection laws across the globe, it will continue to be an important topic for businesses and those who do not take data protection seriously risk being left behind.

What has changed?

Data protection law is not going away. The UK's newly revised data protection law gives stronger rights to people and sets out organisations' compliance duties in great detail. Although it is based on familiar concepts and principles, there is no doubt that the GDPR requires organisations to do more to demonstrate their compliance, and the penalties for failing to do so can be far higher than they used to be.

Personal information is going up in the public and corporate agenda. The penalties for not complying with data protection law are higher than ever – but the law is complicated and often misunderstood. We can help your organisation to adopt practical measures to address the areas of greatest data protection risk, to reduce the likelihood of regulatory action and to develop a positive, sustainable approach to handling personal information.



GDPR changes at a glance

The GDPR protects the personal information of people across the EU. It gives them rights over their information and increases organisational accountability for the collection, use, security and disposal of personal information.

The key features of the GDPR include:

- Enhanced rights for individuals – including the right to object to certain types of profiling and automated decision making
- Obligations on organisations to publish more detailed privacy notices – informing individuals of their data protection rights and of how their information is being used
- Stringent consent requirements – if required, consent must be explicit and freely given for a specific purpose, and must be easy to retract
- Data processors – new requirements are imposed on data processors, including compliance requirements to be addressed contractually
- Breach reporting – significant data breaches must be reported to regulators within 72 hours
- Privacy impact assessments – organisations must formally identify emerging privacy risks, particularly those associated with new projects
- Privacy by design – organisations must design data protection into new business processes and systems
- Record keeping – organisations must maintain a record of the processing activity they carry out

What does good look like?

In the run up to May 25, a number of misunderstandings sprung up around the GDPR. These will gradually subside as organisations begin to understand what compliance looks like in practice. For organisations to get used to the new environment, they must first understand the basics of effective data protection and what good looks like.

An effective GDPR programme is based on the following key building blocks:

- Appropriate governance arrangements – including individuals' rights
- Effective policies and procedures for personal information
- Adequate technical and organisational security measures
- Maintaining an information asset register
- Ongoing training and awareness
- Applying privacy by design and default
- Embedding the accountability principle

Common misunderstandings around the GDPR include:

- You need consent to keep employee records
- You have to appoint a DPO
- Overseas data transfers are now illegal
- You will get fined for not being 100% compliant
- You can't disclose personal information to other regulators/agencies
- You have to notify every data breach to the regulator
- You must delete personal information on request

How should you approach the regulation?

Implementing the GDPR has not been plain sailing and many organisations are still working towards achieving compliance. Typical challenges faced by businesses are set out below.

Collect personal information properly

This is the first stage of data protection compliance and covers areas such as drafting a privacy policy and deciding whether you need consent to collect peoples' information. This is an area of high regulatory risk and one where the requirements of the law are often misunderstood.

Use personal information responsibly

All organisations need personal information – about their customers or employees for example – in order to function. One of the basic requirements of data protection law is that personal information has to be used fairly. This means relevant members of staff must be trained so they understand what they can and cannot do with personal information. It is essential to embed a culture of respect for personal information.

Keep personal information safe

Data breaches can attract a lot of media attention and may lead to both reputational loss and enforcement action. Data breaches are not just security breaches, they can include issues concerning the integrity and availability of personal information.

We have proven expertise in the field of information security. Our experts can help you work out what personal information you hold and which systems it is stored on – this is the first stage of a comprehensive information security regime. We can offer expert advice on all aspects of cyber security, using techniques such as penetration testing and carrying out anti-phishing exercises.

Maintain good quality, up to date and relevant information

Too many organisations have a 'keep it all forever' culture and do not know the quality or origins of the personal information they hold. This is a liability from a regulatory perspective and leads to business inefficiency – for example, there is no point in sending our marketing to email addresses that are no longer in use.

Our information governance and records management specialists can help you to put your information assets in order and to make sure that your organisation holds good quality, up to date and relevant information going forward.

Give people their information rights

Individuals' rights lie at the heart of data protection law and failure to deliver them can be a regulatory red-line. Even if your organisation only receives a small volume of access requests, you must have procedures in place to make sure they are handled properly. Your organisation also needs to be ready to deal with the new individuals' rights, such as data portability – the right to have personal information provided in an electronic, easily transferable format.

We can help you put the procedures in place to make sure people can exercise the rights they are entitled to by law.

Share, disclose and transfer personal information securely

The new data protection rules were drafted with a networked world in mind, recognising that the exchange of personal information between organisations – and between countries – is becoming the rule rather than the exception. It is a key requirement of data protection law to have the right arrangements in place to protect personal information, wherever it is held.

How we can help

We offer a broad range of services, tailored to your business activities and operational requirements. We have extensive experience of planning and implementing UK, EU and global data protection compliance programmes.

Audit

Our skilled audit team can check that your data protection compliance issues are adequately addressed. Taking a risk-based approach, we prioritise the areas that are most likely to be of concern to the regulator, and to the people whose personal information you hold. Building the fundamental principles of data protection, we follow the personal information life-cycle, from its initial collection through to its final destruction.

Advisory

Data protection law can be confusing and difficult to translate into practical activity. Many organisations benefit from working with a third party to sense-check their compliance programmes. Our experts have significant industry experience and can assess whether your plans, policies and procedures are fit for purpose.

Benchmarking

We work with many clients across a range of business areas. We can help you to understand how your organisation compares to its peers and to design a compliance programme that is effective but not excessively resource intensive.

International support

Over 100 countries now have data protection laws in place. International operations are increasingly looking for a global solution to data protection compliance, albeit with some modifications to accommodate national variations in the law. We have an international presence and the local expertise to help you develop a worldwide data protection programmes.

Security and resilience

Data breaches can be very expensive to remedy and cause reputational damage. Our cyber security services use industry standard methodologies to identify, remediate and improve your organisation's security standards, ensuring it has the level of technical and organisational security required by law. We can help protect your organisation and advise on what to do in the event of a breach.

Training and mentoring

Data protection law is often misunderstood, its terminology can be off-putting and complicated. Our data protection training and mentoring services can demystify the law and give your staff an understanding of how to comply in practice. We have a plain-English, non-legalistic approach and will tailor our services to suit your organisational needs - including providing desk-top training materials as required.

Forms and templates

Data protection law contains the concept of 'accountability', which means being able to demonstrate to the regulator how your organisation approaches compliance. This involves recording your processing activity, having the right forms and procedures for handling information rights requests and putting privacy notices in place. We have an extensive collection of data protection forms and templates, which can help your organisation to demonstrate its accountability.

Contact us

We take a positive approach to data protection and believe that respecting people's information rights and having good information governance in place is good for business.

Taking a long-term, sustainable approach, we recognise that data protection is here to stay and is expanding globally. Evidence suggests that it is becoming a more important issue for the public and for organisations alike. Our team of subject matter experts can offer unique expertise and insight. For example, our Head of Personal Information and Privacy worked for the UK's data protection regulator for over 20 years and was the principle author of many of its most significant pieces of guidance. The regulatory insight we can offer will help our clients to focus on the areas of greatest risk, to demystify a very complex piece of law and to adopt a positive, sustainable approach.

Sandy Kumar
Head of Financial Services Group
and Business Risk Services UK
T +44 (0)20 7865 2193
E sandy.kumar@uk.gt.com

Manu Sharma
Partner, Head of Cyber, Data and Payment Services
Business Risk Services
T +44 (0)20 7865 2406
E manu.sharma@uk.gt.com

Iain Bourne
Head of Personal Information and Privacy
Business Risk Services
T +44 (0)20 7865 2375
E iain.b.bourne@uk.gt.com

Grant Thornton
An instinct for growth™

grantthornton.co.uk

DS152