KPMG

Ready for GDPR?

Five steps to turn compliance into your advantage

Ready for GDPR?

The biggest change to rules governing data protection for more than 20 years comes into effect in May 2018, carrying fines of up to 4% of global turnover or €20m for businesses that do not comply, whichever is higher. The European Privacy regulators have made it very clear that they intend to use their new powers.

However GDPR is not just a threat, it is also an opportunity. In an age when personal information is a key asset and a business driver, getting your privacy strategy right can give you a competitive edge.

How can you turn GDPR to an advantage?
It starts with recognising that personal information is one of your organisation's most valuable assets.

From this, every business process using personal information will be seen as an opportunity. An opportunity to gain a better understanding of customers and the performance of your organisation and broader marketplace - by gathering and refining personnel data.

Managing this data requires a careful strategy to ensure that it's reliable and that customers understand what you are doing with their personal information and where required that you have gained their consent. This will ensure the insights it delivers are actionable, and reduces the risk that organisations won't be perceived as intrusive as customers see more tailored products, pricing or services.

Five steps to ensure compliance

Based on KPMG's extensive experience in working with organisations across sectors and geographies on privacy matters, we recommend the following five step approach. This could be used specifically for the purposes of the GDPR or as a broader privacy strategy approach.

1. Define your privacy strategy

What levels of privacy risk is your organisation prepared to accept? Where do you want to be compared to your peers? Which aspects of the GDPR are most critical for you and your customers? Who on the Board is accountable for it?

Defining your privacy strategy is the first step. Without it, you can't have a consistent and coherent approach. The strategy must be defined and articulated, and then presented to senior leadership for their endorsement. You need to get it on the Board's agenda fast. Our recent experience has shown that most organisations will need to put investment into a privacy improvement programme.

2. Where are you now?

In order to establish the size of the task ahead and what specific areas need addressing, you need to understand your organisation's current maturity. This is not a tick box exercise but a pragmatic, focused process to really understand the GDPR privacy risk exposures that exist across your business.

In undertaking these first two steps, you will also need to consider what aspects of the GDPR, and privacy in general, are the key drivers for your organisation. What matters most?

- **Compliance and legal** – creating an audit trail to show that you are meeting the technical requirements
- **Speed to market** – getting privacy right so that you have the flexibility to get new products to market quickly and can differentiate your services
- **Data explosion** – with the explosion of data that the Internet of Things and the greater use of artificial intelligence is creating, it is critical to manage the hugely increased privacy risks
- **Globalisation** – as organisations look to move data between different parts of the world, and with new privacy laws springing up in more and more jurisdictions, you need to ensure that you do not inadvertently 'cross the line'
- **Externalisation** – the huge growth in the use of the cloud to store data, and the use of external vendors, creates new privacy risks that must be managed
- **Customer portability** – with customers set to be able to demand their data is 'ported' to competitors, it will be easier for them to take their business to rivals, creating a new level of competitive threat for those who get things wrong
- **Reputation** – we only need to look at the damage done to brands that have fallen foul of data breaches and cyber-attacks to see the potential risk to corporate reputation

3. Take a pragmatic approach

You need to build a realistic plan which will help you manage your risk to an appropriate level, in line with your overall business strategy. This does not necessarily mean taking a leading position in every single respect - but a clear view of what success looks like for you.

Where do you want to start? This will depend based on your risk appetite but here are some areas we believe you should focus on:

- **Governance, inventory and risk** – these are all linked. You need to understand what data you hold, how you are going to manage it, and what risks are posed by it, so you can understand your risk appetite and apply the appropriate level of control
- **Individuals rights** – the Right to Erasure and the issue of data retention are heavily linked. If you don't know what data you have, and if you are storing more than is needed, how can you hope to be able to identify what should be removed under such a request? Furthermore, Subject Access requests will be free under the GDPR so you may receive a lot more of them - and will have only a month to respond
- **Incident management** – there is a new and very challenging requirement to report breaches to the regulator in 72 hours. Without robust incident management processes, could you mobilise an investigation and be able to report within the timescales?
- **3rd party diligence and contracts** – Data Controllers will be required to have an understanding of how their supply chain handles their Privacy Information (PI). You will be required to have explicit privacy clauses in contracts, a retention period, and the right to audit. Data Processors will be required to have the same protections in place as the Data Controllers
- **Training** - you need to ensure that your staff are aware of the impact of GDPR and have a decent understanding of how it applies to them. Everyone will need basic training, but high risk areas like HR or marketing will need focussed training on how to manage special category PI
- **3rd party assurance** - many organisations have improved third party management processes in recent years but few have developed a process that meets the needs of GDPR. Contracting with third parties requires urgent attention however ongoing assurance activities can take place post initial due diligence and the re-contracting process.

4. Coordinate and deliver

Focusing on areas of greatest risk, you need to ensure that controls are embedded as part of day to day business operations. This will require coordination across the business. Make sure you have the right blend of input from legal, IT, HR and marketing and enough resources. Don't underestimate the level of effort - personal information is everywhere in your organisation.

5. Embed into business as usual

Complying with the GDPR is about defining, implementing and then sustaining compliant processes. Post 2018 you will be required to demonstrate, on an ongoing basis, how you collect, use, retain, disclose and destroy personal information in line with the GDPR requirements. This impacts everything you do relating to personal information and is therefore a significant transformational activity for your organisation going forwards.

In short, the GDPR has to become business as usual. It's about embedding the GDPR's **accountability principle**. This requires you to show how you comply with the principles – for example by documenting the decisions you take about a processing activity. Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

How can you demonstrate accountability? You are likely to need:

- Documented risk management framework
- Up to date Personal Information Inventory
- Clear and defined roles and responsibilities for privacy
- Up to date, well managed privacy policies, processes and procedures
- An understanding of what 3rd parties are doing with your data
- Adoption of well-known frameworks such as ISO27001, Cyber Essentials

Reaching and maintaining a state of accountability will give you greater control over your data and be productive for the business far beyond the issue of simply complying with the GDPR. It will give you confidence that you can meet data privacy regulations around the world and, at the same time, put you in a position of strategic and commercial strength.

FAQs

It's OK, Brexit means this won't apply to us or be adopted by the UK
It's not OK! If you collect data about customers who are in the EU, whether the UK is inside the EU or not, then the regulations will apply – the GDPR has 'extraterritoriality'. The UK government has already said that it will comply with GDPR while it negotiates Brexit – and we will still be in the EU in May 2018. Even when the UK exits the EU, we will still need GDPR-equivalent rules because many UK organisations hold or process EU citizen data. Brexit is not a get-out-of-jail card.

We have good privacy controls in place
This is rarely the case, however, even if they are strong, for the purposes of the old Data Protection Act the requirements under GDPR means there is likely more work to be done to ensure compliance.

We're happy to do 'just enough'
This is a very dangerous strategy as the regulator is yet to set a clear bar. You may choose not to delete old customer data or not destroy old customer records, but are you going to continue marketing to your customers without permission? These are decisions that under GDPR must be recorded and be made by senior people within the organisation and even then, taking that level of risk without sufficient investigation of options would not be a defensible position in the event of an investigation by the regulator.

We have GDPR well under control in our organisation
The scope of data generated across an organisation is daunting – from HR to sales, and from marketing to finance. Getting a consistent, efficient and effective privacy approach is challenging – and needs strong board-level support and governance.

KPMG is the clear choice

We have a leading team of experienced privacy professionals both in the UK and across our network of member firms

We take a pragmatic and realistic approach based on the unique footprint of each organisation

Our extensive privacy experience already includes the design and delivery of GDPR programmes across multiple sectors

Our Privacy Management Framework is based on Globally Accepted Privacy Principles (GAPP) and is consistently adopted by KPMG teams across our network of member firms

Contact us

Martin Tyley
Partner
KPMG in the UK
T: +44 113 2313934
E: martin.tyley@kpmg.co.uk

Mark Thompson
Global Head of Privacy
KPMG in the UK
T: +44 7747 565630
E: mark.thompson@kpmg.co.uk

kpmg.com/uk