General Data Protection Regulation
Preparring for a new era in Privacy
2017
General Data Protection Regulation

The key points

The General Data Protection Regulation
After four years of negotiations, the EU General Data Protection (GDPR) is upon us and will be enforceable from 25 May 2018. The new law will introduce a range of requirements that will have significant impacts on organisations. Combined with increasing demands from consumers, privacy is now firmly positioned at the top of the corporate agenda.

Significant New Requirements
The GDPR mandates organisational accountability and will require organisations to implement robust privacy governance and in general take a more proactive approach to privacy compliance. In addition, documented privacy risk assessments will be required for new systems and technologies, and security breaches will have to be notified to regulators within 72 hours. It is estimated that an additional 28,000 new Data Protection Officers will be needed in Europe alone to deal with the requirements.

Harmonisation and Enforcement
For global organisations, the GDPR harmonises much of the currently fragmented legal framework for privacy across Europe, providing one data protection regulation for all member states. While the regulations have been harmonised, the GDPR introduces a new maximum monetary penalty of 4% of annual global turnover that can be imposed in cases of serious non-compliance.

International Reach
Organisations based outside the EU that process data to offer goods or services to European residents, or to monitor the behaviour of European residents will also be subject to GDPR requirements. How enforcement will apply in practice remains to be seen, but organisations that are not in scope of current EU data protection rules may find themselves subject to significant new requirements.

The Legal and Compliance Perspective
The GDPR introduces significant new requirements and challenges for legal and compliance functions. Organisations will need to put in place additional governance and controls.

The Technology and Digital Perspective
New GDPR requirements will mean changes to the ways in which technologies are designed and managed, including a focus on profiling and security.

The Data Perspective
Individuals and teams tasked with data governance and data management will be challenged to provide clearer, proactive oversight on data storage, journeys, and lineage.
General Data Protection Regulation

The Regulation in numbers

- 28,000: Estimated number of new Data Protection Officers required in Europe*
- 250m: Cost of 4% fine for a typical FTSE 100 company
- 72: Hours given to report a data breach
- 190+: Countries potentially in scope of the regulation
- 7: Core individual rights afforded under the GDPR
- 80+: New requirements in the GDPR

4%: Potential fines as a percentage of global turnover

*Source: IAPP Study (2016)
The Consumer Perspective
What Privacy means to consumers

Our consumer surveys, which look at consumer attitudes towards data use by organisations and privacy across the UK, show that consumers are increasingly concerned about the use of their data. On the other hand, consumers are also more willing to engage with organisations they trust and perceive to offer the greatest privacy protections.

At its heart, the GDPR aims to strengthen consumers’ rights, and those organisations that are transparent and open are more likely to reap the rewards.

When compared to the national average, people who believe that companies tell them how their personal data is used are:

- 2X MORE CONFIDENT that companies keep personal data safe
- 2X MORE CONFIDENT that companies use personal data to offer better services
- 3X MORE CONFIDENT that companies do not sell personal details to other companies without their knowledge
- 3X MORE CONFIDENT that companies always remove personal details when passing on personal data to other organisations

It provides consumers with a range of new rights, including the controversial ‘right to be forgotten’ (right to erase), as well as a new right to ‘data portability’, where individuals can request their data to be sent to other organisations. Whether consumers will exercise these rights in practice remains to be seen, but the impact on organisations could be significant.

Responsible analytics means greater transparency, more tailored benefits, and ceding control of data to customers. If organisations make it easier to manage personal data, 49 per cent of consumers say they are likely to use the data to make better decisions and 53 per cent would update personal data held by a company to keep it up to date.

Customers are more willing to trust and engage with forward-looking organisations. These organisations have responsible big data practices that complement traditional values like quality, service and social responsibility. Consumers are confident that companies keep their data safe, know how their data is being used and understand the benefits – nearly twice as willing to give up personal information than those who are not.

Big data is the new normal for organisations wanting to understand their customers. In 2014, 50 per cent of British consumers say they are aware of organisations collecting data about them and their activities, up from 35 per cent last year.

Public confidence in data use remains consistently low. This year, 63 per cent of adults say they are not confident companies keep their personal data secure from loss and theft, and 72 per cent feel companies are not telling them how they are using their personal information.

Responsible analytics means greater transparency, more tailored benefits, and ceding control of data to customers.
Privacy as a concept is broad and far-reaching. For this reason, the GDPR impacts many areas of an organisation, not just legal and compliance. It also engages functions tasked with information technology and security, data governance and information management, as well as sales, marketing and digital.

Who should care?

- General Counsel/ Legal
- Privacy Officer
- Chief Risk Officer
- Chief Compliance Officer

Legal and Compliance
The GDPR introduces new requirements and challenges for legal and compliance functions. Many organisations will require a Data Protection Officer (DPO) who will have a key role in ensuring compliance. It is estimated that 28,000 new DPOs will be required in Europe alone. If the GDPR is not complied with, organisations will face the heaviest fines yet – up to 4% of global turnover. A renewed emphasis on organisational accountability will require proactive, robust privacy governance, requiring organisations to review how they write privacy policies, to make these easier to understand.

Technology
New GDPR requirements will mean changes to the ways in which technologies are designed and managed. Documented privacy risk assessments will be required to deploy major new systems and technologies. Security breaches will have to be notified to regulators within 72 hours, meaning implementation of new or enhanced incident response procedures. The concept of ‘Privacy By Design’ has now become enshrined in law, with the Privacy Impact Assessment expected to become commonplace across organisations over the next few years. In addition, organisations will be expected to look more into data masking, pseudo-anonymisation and encryption.

Data
Individuals and teams tasked with information management will be challenged to provide clearer oversight on data storage, journeys, and lineage. Having a better grasp of what data is collected and where it is stored will make it easier to comply with new data subject rights – rights to have data deleted and to have it ported to other organisations.

Who should care?

- Chief Data Officer
- Chief Operating Officer
- Chief Marketing Officer
- Data Stewards
- Digital Leads
Perspective – Legal and Compliance

General Counsels, Chief Compliance Officers, Chief Privacy Officers and Data Protection Officers: Your privacy strategies, resourcing, and organisational controls will need to be revised. Boardrooms will need to be engaged more than ever before.

A Revolution in Enforcement
Fines of up to 4% of annual global turnover
Serious non-compliance could result in fines of up to 4% of annual global turnover, or €20 million – whichever is higher. Enforcement action will extend to countries outside of the EU, where analysis on EU citizens is performed. But how will this play out in practice? Will US organisations, for example, take heed of EU data protection authorities?

Data Protection Officers
Privacy specialists in high demand
Organisations processing personal data on a large scale will now be required to appoint an independent, adequately qualified Data Protection Officer. This will present a challenge for many medium to large organisations, as individuals with sought-after skills and experience are currently in short supply. Organisations will also be challenged to demonstrate an independent reporting line, which could cause issues with incumbent positions.

Accountability
Burden of proof now on the organisation, not the individual
The current requirement to provide annual notifications of processing activities to local regulators will be replaced by significant new requirements around maintenance of audit trails and data journeys. The focus is on organisations having a more proactive, comprehensive view of their data and being able to demonstrate they are compliant with the GDPR requirements.

Privacy Notices and Consent
Clarity and education is key
Organisations will now consider carefully how they construct their public-facing privacy policies to provide more detailed information. However, it will no longer be good enough to hide behind pages of legalese. In addition, there is a significant shift in the role of consent, with organisations required to obtain ‘freely given, specific, informed and unambiguous’ consent, while being able to demonstrate these criteria have been met.
Perspective – Technology

Chief Information Officers, Chief Technology Officers and Chief Information Security Officers: Your approach towards the use of technology to enable information security and other compliance initiatives will need to be reconsidered, with costs potentially rising.

**Breach Reporting**

Breach reporting within 72 hours of detection

Significant data breaches will now have to be reported to regulators and in some circumstances also to the individuals impacted. This means organisations will have to urgently revise their incident management procedures and consider processes for regularly testing, assessing and evaluating their end to end incident management processes.

**Encryption**

Encryption explicitly called out

The GDPR formally recognises the privacy benefits of encryption, including an exemption from notifying individuals of data breaches when data is encrypted. However, this does not mean that organisations can afford to be complacent, and the exemption may not apply when weak encryption has been used. Given the potential fines, organisations will have to further increase their focus on a robust information and cyber security regime.

**Online Profiling**

Intensified debate over profiling

Individuals will have new rights to opt out of and object to online profiling and tracking, significantly impacting direct-to-consumer businesses who rely on such techniques to better understand their customers. This applies not just to websites, but also to other digital assets, such as mobile apps, wearable devices, and current and emerging technologies.

**Privacy-by-Design**

Recognised good practice becomes law

The concept of Privacy By Design (PbD) is nothing new, but now it is enshrined in the GDPR. Organisations need to build a mind set that has privacy at the forefront of the design, build and deployment of new technologies. One manifestation of PbD is Privacy Impact Assessments (PIA), which are now required to be undertaken for new uses of personal data where the risk to individuals is high.
Chief Data Officers, Data Stewards, Chief Marketing Officers, and Digital Leads:

Your information management activities have always supported privacy initiatives, but under the GDPR new activities are required which specifically link to compliance demands.

**Data Inventories**

**Stronger need to identify and track data**

Organisations will have to take steps to demonstrate they know what data they hold, where it is stored, and who it is shared with, by creating and maintaining an inventory of data processing activities. Data leads will have to work closely with privacy colleagues to ensure all necessary bases are covered. A thorough system for maintaining inventories needs to be implemented.

**Right to be Forgotten**

**A stronger right for consumers to request deletion of their data**

A new ‘right to be forgotten’ is further evidence of the consumer being in the driving seat when it comes to use of their data. Depending on regulatory interpretation, organisations may need to perform wholesale reviews of processes, system architecture, and third party data access controls. In addition, archive media may also need to be reviewed and data deleted.

**Right to Data Portability**

**A new right to request standardised copies of data**

A new right to ‘data portability’ means that individuals are entitled to request copies of their data in a readable and standardised format. The interpretation of this requirement is debatable, but taken broadly the challenges could be numerous – amongst them achieving clarity on what data needs to be provided, extracting data efficiently, and providing data in an industry-standardised form.

**New Definitions of Data**

**New concept of pseudo-anonymous data**

The GDPR recognises the concept of pseudo-anonymous data and expands the definition of personal data, placing a greater emphasis on data classification and governance. Previous ambiguity over certain data types, e.g. cookies, has now been clarified to be within the definition of personal data. Indeed the scope has been expanded so that even nicknames and internal identifiers used by companies are included.
GDPR Compliance

The effect of Brexit on UK organisations

On 23 June 2016 the United Kingdom voted to leave the EU. The effect of the referendum decision may impact the UK’s adoption of the GDPR. Nevertheless, the GDPR will still apply to UK businesses offering goods or services within the EU. A further consideration is whether the UK can and will attain ‘adequacy’ status when operating outside of the EU, allowing the free flow of personal data to and from the EU to continue. The key implications, together with the adequacy issue, are explored below.

Extra-territorial Reach – Organisations offering goods or services within the EU, or monitoring the behaviour of EU citizens, will still have to comply with GDPR rules.

UK Data Protection rules – Whatever happens with the UK adoption of GDPR, an update to the Data Protection legislation seems inevitable. Any UK successor legislation will likely have to deal with similar requirements, in view of the UK’s likely intention to apply for ‘adequacy’ status (see diagram opposite).

Regulatory Enforcement – It has yet to be clarified if UK regulatory authorities, post Brexit, can or will apply the same level of punitive measures that the GDPR has introduced. The European Commission has not indicated that it will expect to see a comparative punitive framework in countries seeking an equivalent level of Data Protection Standards.

Supply chain management – Existing contractual agreements may exist with suppliers and/or clients regarding the transfer of personal data outside of the EU or European Economic Area (EEA). Organisations are already conducting reviews of such contracts, amending terms where necessary.

Adequacy rule and the free flow of personal data between the UK and the EU: Once a date is set for withdrawal from the EU, the UK authorities will have a decision to make. In order to allow data to continue to move freely between the EU and UK, it will be necessary for the UK to achieve ‘adequacy’ status in the eyes of the European Commission. The European Commission may decide to accept or deny this application, leading to the following implications below:
Practical Steps to GDPR Compliance

Building a change programme

A combination of both tactical and strategic actions will be required to address GDPR compliance, often over a period of months and maybe years. The diagram below plots out key elements that will be required in order to genuinely drive organisational and cultural change and embed the GDPR requirements into business as usual. The scale of the programme will depend on an organisation’s current privacy maturity and the complexity of the remediation required.

<table>
<thead>
<tr>
<th>Foundational Activities</th>
<th>Typical Remediation Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stakeholder awareness</td>
<td></td>
</tr>
<tr>
<td>Readiness assessment</td>
<td></td>
</tr>
<tr>
<td>Data inventories and mapping</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td></td>
</tr>
<tr>
<td>Legal and compliance</td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

GDPR formalised 25 May 2016

- Make sure stakeholders are fully aware of the GDPR and the impact it will have on the organisation. Ensure that key messages are understood by the Board and senior management – and gain buy-in for remediation and change programmes.
- Conduct a Readiness assessment to understand how near or far away your organisation is from relevant new requirements of the GDPR and the potential effort required.
- Compile an inventory of the personal data that is collected, who it is shared with and what controls govern its use. Authorities will expect this information to be made readily available.
- Use the GDPR to assess your holistic approach to privacy – do you have a Data Protection Officer? Who is ultimately accountable? How are you going to bring together different areas of the business to manage privacy risks on an ongoing basis?
- Review approaches to capturing consent. Re-draft privacy notices and determine how compliance will be demonstrated.
- Deploy technology and processes to bring about a Privacy By Design culture, and create robust breach management procedures, consider masking and encryption.
- Ensure the organisation has the right data governance practices to respond efficiently to the new rights afforded to individuals, such as the rights to erasure and portability.

GDPR enforced 25 May 2018
How We Can Support You
Our Privacy and Data Protection services

We have a dedicated team of privacy specialists, with deep expertise in leading privacy programmes across large scale and complex organisations, embedding change. A summary of our key services is below, together with a short example of our work in each area.

Our Key Privacy Services

<table>
<thead>
<tr>
<th>Compliance and Readiness</th>
<th>Privacy Programmes</th>
<th>Technology and Digital</th>
<th>Risk Management</th>
<th>Training and Cultural Change</th>
<th>Cyber Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• GDPR readiness assessment</td>
<td>• Privacy programme development</td>
<td>• Data discovery, mapping, and inventories</td>
<td>• Privacy Impact Assessment and health check</td>
<td>• Privacy risk and compliance training</td>
<td>• Personal data breach investigation and management</td>
</tr>
<tr>
<td>• GDPR compliance roadmap</td>
<td>• Privacy strategy and roadmap development</td>
<td>• Privacy-by-design advice and application</td>
<td>• Policy analysis and design</td>
<td>• Training and awareness design and implementation</td>
<td>• Regulatory liaison advice</td>
</tr>
<tr>
<td>• Global privacy compliance assessment</td>
<td>• Target operating model design and implementation</td>
<td>• Online and e-Privacy</td>
<td>• Governance and compliance review</td>
<td>• Classroom and computer-based training</td>
<td>• Incident response and forensic investigation support</td>
</tr>
<tr>
<td>• GDPR technology impact assessment</td>
<td>• Change programme design and delivery</td>
<td>• Digital asset risk assessment and management (e.g. websites and mobile apps)</td>
<td>• Third party management</td>
<td>• Mergers and acquisitions data transfer and ownership</td>
<td>• Supplier and third party management</td>
</tr>
<tr>
<td>• Global compliance assessments</td>
<td></td>
<td></td>
<td>• Cultural change programme development</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

We designed and established a new privacy function for a global financial services organisation, creating a governance model, policies and processes, and bespoke privacy training.

We designed and implemented a group-wide privacy programme for a consumer business client, and delivered a gap analysis, a PIA procedure, policies, and a privacy operating model.

We supported the cyber response for a consumer business client which had suffered hacking and a data breach, providing advice on their customer notification and regulatory obligations.

Our team performed an assessment of a pharmaceutical organisation’s readiness with key GDPR requirements, issuing a formal report and prioritised compliance roadmap.

We designed and implemented a group-wide privacy programme for a consumer business client, and delivered a gap analysis, a PIA procedure, policies, and a privacy operating model.

Our team performed an assessment of a pharmaceutical organisation’s readiness with key GDPR requirements, issuing a formal report and prioritised compliance roadmap.

We supported the cyber response for a consumer business client which had suffered hacking and a data breach, providing advice on their customer notification and regulatory obligations.
Supporting your Journey

Our global team

We have privacy professionals across EMEA, supported by a wider global practice with experts in all major markets. Our experienced team of privacy professionals can deliver a wide range of services, from quick-win readiness assessments to full privacy remediation programmes.

Our privacy practice specialises in tackling complex data protection issues, working across industries and jurisdictions. We draw on the technology, data, and analytics expertise of our Technology Consulting practice, including from the Deloitte Digital design and development agency. This allows us to provide a truly holistic view of privacy.

Contact a member of the team for further information.

UK Team Contacts

Peter Gooch
Partner, UK Privacy Practice Lead
pgooch@deloitte.co.uk

Stephen Bonner
Partner
stephenbonner@deloitte.co.uk

Key EMEA Team Contacts

Erik Luysterborg
Partner, Belgium & EMEA Privacy Practice Lead
eluysterborg@deloitte.com

Annika Sponselee
Partner, Netherlands Privacy Practice Lead
asponselee@deloitte.nl

The Deloitte Privacy and Cyber Practice in Numbers

180+
UK cyber and privacy practitioners

1,400+
Global cyber and privacy practitioners

General Data Protection Regulation | Preparing for a new era in Privacy
This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

© 2017 Deloitte LLP. All rights reserved.