www.pwc.com

Your GDPR compliance journey

pwc

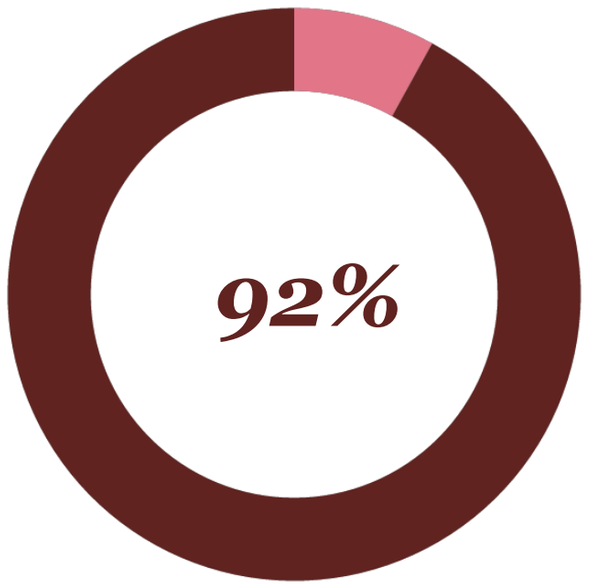
What is GDPR?

The GDPR is a new law in the European Union (EU) providing for **uniform data protection regulation throughout the EU**. When it goes into effect on May 25, 2018, it will represent **one of the highest standards of data protection in the world,** creating a **consistent, global, and unified legal** basis for data protection and enforcement across the Member-States. It will supersede the existing EU Data Protection Directive, which came into effect almost 20 years ago in 1998.

Key GDPR requirements

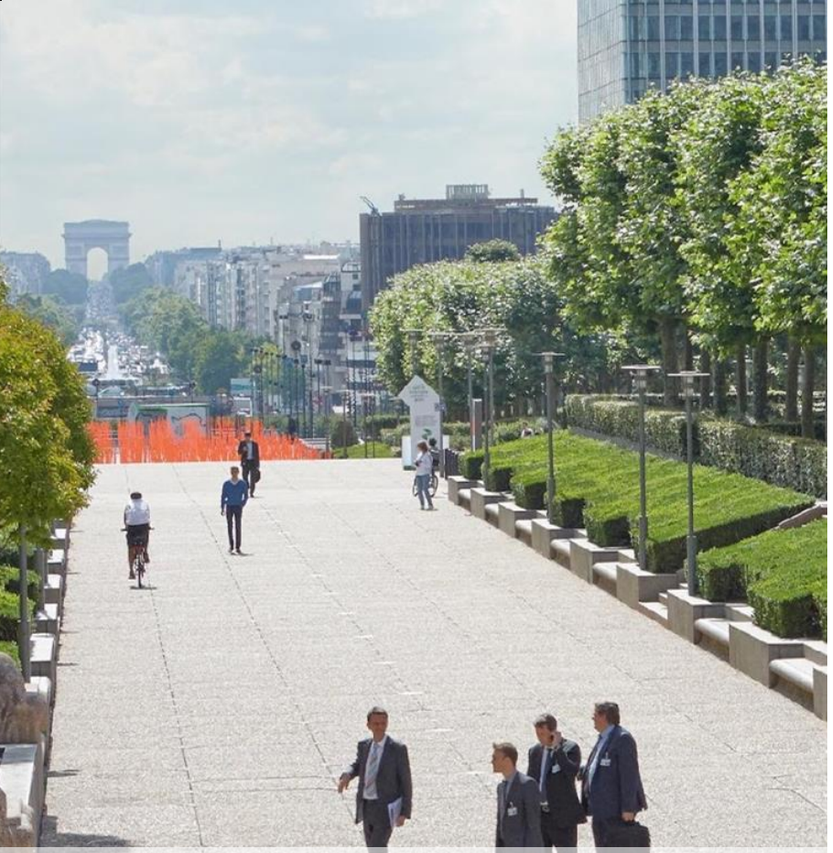
Organisations doing business in Europe are seeing five GDPR requirements in particular cause the biggest impact on their future business plans:

- Mandatory data inventorying and record keeping of all internal and third-party processing of personal data;
- Mandatory data-breach notification to regulators and individuals whose information is compromised following information-security failures;
- Comprehensive individual rights to access, correct, port, erase, and object to the processing of their data;
- Routine data-protection impact assessments for technology and business change; and
- Mandatory data protection officers and an overall rethinking of privacy strategy, governance, and risk management.



of survey respondents say GDPR compliance is a top data protection priority

PwC, GDPR preparedness pulse survey, December 2016



68% of respondents say they will invest between £1 million and £10 million on GDPR readiness and compliance efforts

PwC, GDPR preparedness pulse survey, December 2016

Potential GDPR risks

Reputational Risk Non-compliance with the GDPR could result in brand damage, loss of consumer trust, loss of employer trust, and customer attrition.

Operational Risk Under the GDPR, individuals may impose data processing bans, suspend data transfers, and order the correction of an infringement, resulting in restricted operations and invalidated data transfer.

Financial Risk As a result of non-compliance, **fines of up 4% of the total annual turnover** of the preceding financial year may be enforced. In addition, companies may experience loss of revenue, as well as high litigation and remediation costs.

Regulatory Risk Regulators may also require the provision of information, conduct audits, and obtain access to premises.

Questions you should be asking

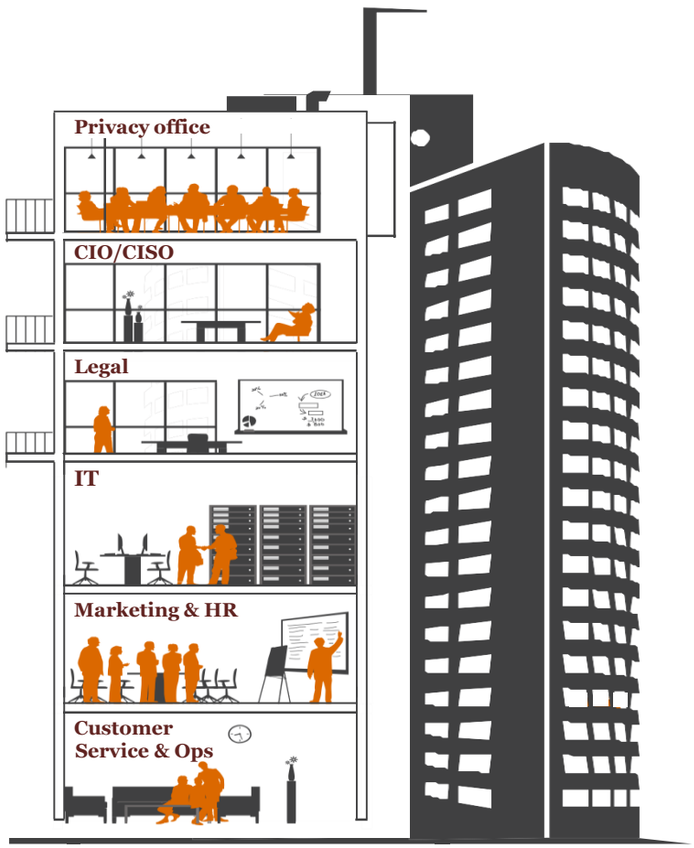
The scope and requirements set forth in the regulation are deep and complex; many companies must begin remediation efforts now to ensure compliance. The GDPR requires that companies take a **programmatic approach** to Data Protection, which means they need to develop defensible programs for compliance and be able to prove that they are acting appropriately.

Questions to help determine where to get started:

- What is our data footprint (e.g. employee data, consumer data, business customer data)?
- Are we prepared to provide evidence of GDPR compliance to regulators, who may now request it on demand?
- Do we have visibility of and control over what personal data we collect? How it is used? With whom the data is shared?
- Do we have a Privacy by Design program in place, with Privacy Impact Assessments, documentation, and escalation paths?
- Do we have a tested breach-response plan that meets the GDPR's 72-hour notification requirement?
- Have we defined a roadmap for GDPR compliance?
- Have we identified a Data Protection Officer (DPO), as required under the law?
- Have we adopted a cross-border data transfer strategy?

The role of key stakeholders in GDPR compliance

GDPR requirements impact the entire organisation and will need cross functional support as remediation activities are identified and implemented.



Privacy Office

Appointing a Data Privacy Officer (DPO) is one of the most important GDPR requirements. Among other tasks, DPOs will help with consumer notice and transparency; Privacy by Design; and conducting Privacy Impact Assessments (PIAs)

CIO/CISO

GDPR compliance will require considerable resources and investments. Many CIOs have already added a line item to their budgets. CISOs will be tasked with promoting GDPR security requirements throughout the data lifecycle; and assist with required data breach notification and incident response.

Legal

Companies will look to the Office of the General Council (OGC) to help with implementing data transfer mechanisms; defining data controllers and processors; and managing contract process and model clauses. The OGC will also help drive GDPR required data breach notifications.

IT

A good portion of compliance with the data-portability requirements will fall to IT. In addition to enabling data portability, IT will ensure compliance with the rights of access; authentication; enhance development lifecycle; and manage consent indicators and logs.

Marketing and HR

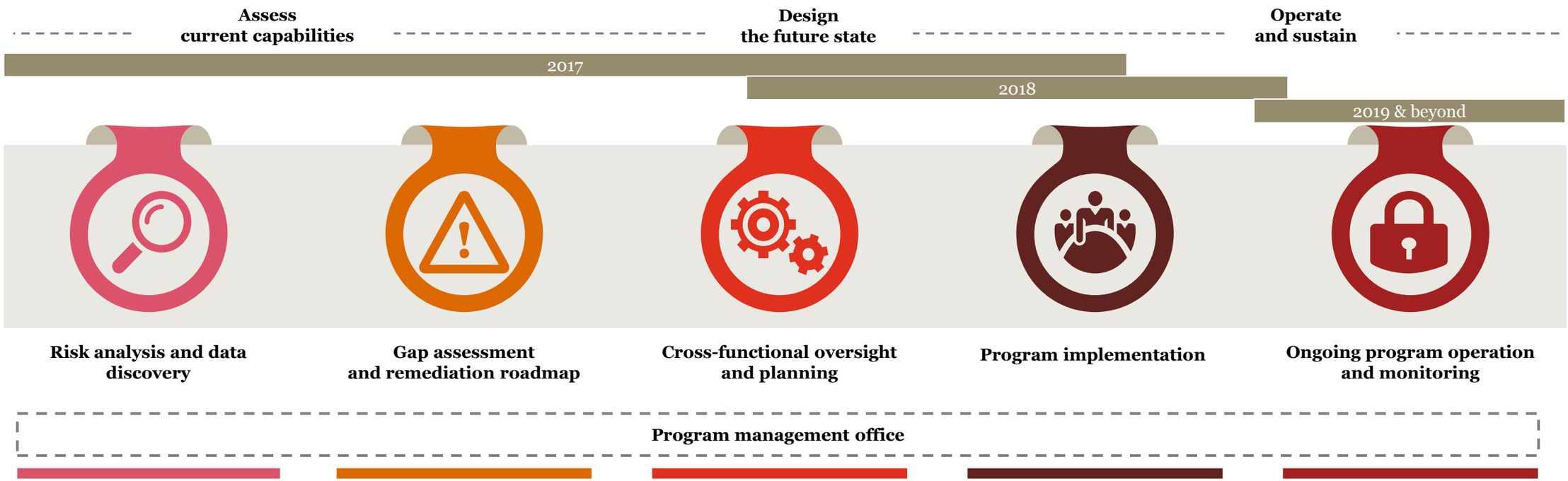
Marketing and HR can help keep the business compliant with GDPR employee and customer privacy requirements including: adherence to consent guidelines; training employees on privacy; and limiting data access. Marketing and HR will also be tasked with automating the decision-making processes.

Customer service and ops

Customer service and Ops may be tasked to implement strategies and systems for customer and employee rights of access and remediation compliance. This includes queries associated with the “right to be forgotten”.

Your GDPR compliance journey

GDPR compliance will be a challenge for many businesses. Only the proactive will be prepared. Your compliance journey involves many considerations including harsh regulatory and litigation risks for non-compliance. Proactive businesses are assessing their current capabilities, designing their future state and operationalising ongoing programs to allow for sustainable and demonstrable compliance. This 5 step approach can help assist in the process of transforming your privacy program.



This GDPR program can help companies identify, reconcile, and respond to current and future cross-territory regulations.

PwC offers a complete portfolio of GDPR services

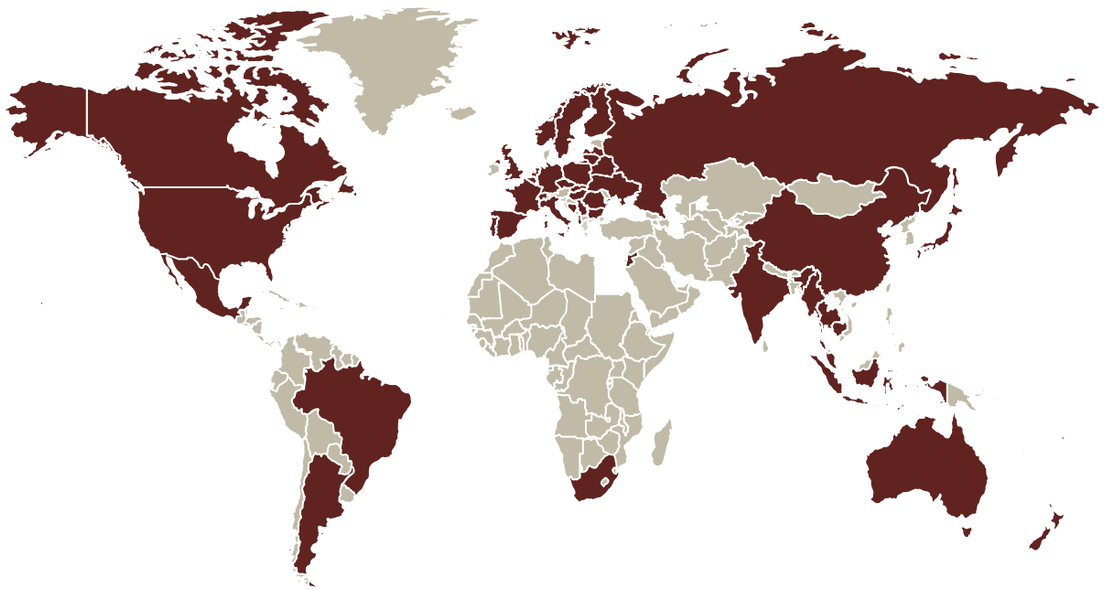
Broad network of experienced teams
PwC's GDPR program is led by experienced teams who tap into a broad network of resources. They help businesses conduct thorough risk assessments based on GDPR requirements, rethink data governance strategy and help implement holistic data-privacy enhancements and compliance-monitoring processes.

Experience
PwC's 25 years of experiences guiding companies through the myriad of privacy and data protection regulatory compliance obligations, including the early stages of GDPR, combined with our unique insights into, and relationships with, the various global privacy and data protection regulators (EU DPAs, FTC, OCR, FCC, etc.), helps us provide companies with recommended solutions that are practical and can stand-up to regulatory scrutiny.

Proprietary tools and accelerators
PwC has designed a wealth of automated and electronic tools, templates, and accelerators honed through years of helping our clients achieve their privacy program goals. These tools and accelerators can help jumpstart GDPR compliance efforts and quickly deploy meaningful advancements to privacy programs and operations.

EU privacy reach
We have over 100 dedicated individuals based in the EU providing a range of privacy related services. We have privacy leaders, outlined below, in every major EU location.

2,900+cybersecurity and privacy practitioners
Our 2,900+ practitioners include highly trained and specialised consultants, lawyers, auditors, technologists, and industry veterans with experience helping global businesses across industries.



PwC GDPR Contacts

Asam Malik
PwC | Director
Mobile: +44 (0) 7932 012 997
Email: asam.malik@pwc.com

Gareth Neal
PwC | Senior Manager
Mobile: +44 7711 589 155 | Office: +44 161 245 2274
Email: gareth.p.neal@pwc.com

Andrew Powell
PwC | Manager
Mobile: +44 (0) 7518 343839 | Office: +44 (0)161 245 2380
Email: andrew.powell@pwc.com

James Smuts
PwC | Manager
Mobile: +44 784 180 3659
Email: james.smuts@pwc.com