Changing how you manage personal data
The impact of the GDPR in the Channel Islands

The General Data Protection Regulation ("GDPR") was approved by the EU in April 2016 and comes into effect from May 2018.

The GDPR increases the rights of EU citizens with regards their personal data. This will impact every organisation that holds or uses European personal data both inside and outside of Europe.

The Channel Islands have also committed to enact equivalent legislation in line with the GDPR to ensure that the Islands maintain their 'adequacy' status.

The GDPR creates technical and operational challenges but also presents a major opportunity to transform your approach to privacy and ensure your operations are fit for a digital economy.

GDPR at a glance

It puts individuals back in control of their personal data

- Customers and employees have more power to control how businesses use their data.
- You could be required to report on, move or dispose of personal data if requested and you must have the capabilities to do this.
- Your options for using personal data are restricted, including profiling activities.

Data must be easily portable and forgettable

- You must be able to provide individuals with their personal data in a structured, commonly used and machine readable form.
- Your systems and processes will have to let you truly 'forget and delete' data upon request from the individuals, including long-term archives.

How you use data will be more transparent

- The rules on consent are getting tougher, and individuals can withdraw consent at any time.
- You'll be required to articulate all of the ways in which you use personal data, and make it clear to individuals what their data is being used for and who you have shared it with.

Third parties could put you at risk

- You'll remain responsible for individuals' personal data throughout the entire data lifecycle.
- You'll have to assure that data you pass to third parties, including outsourced functions, is handled in a manner compliant with GDPR.

Fines are getting bigger and the timelines are getting shorter

- Fines for non-compliance can be as severe as 4% of annual global turnover or 20m EUR – whichever is higher, enforceable from May 2018.
- You'll be under legal obligation to notify data protection authorities within 72 hours of a data breach, and individuals without undue delay.
- You'll have to keep records of your data processing activities, undertake privacy impact assessments and appoint a Data Protection Officer (DPO).

pwc

The GDPR's requirements pose complex and multidisciplinary challenges, which are likely to be fundamental to your operations and how you use personal data.

How can we help?

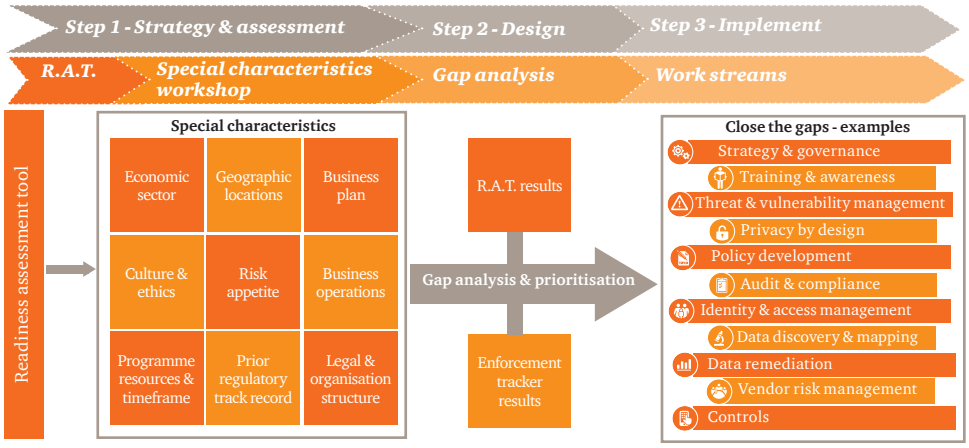
In the time available, organisations with significant personal data and complex processes will struggle to be fully compliant by May 2018. It's therefore essential that your organisation has a clear vision and a risk-based approach to your GDPR implementation programme.

Organisations who take a strategic approach will benefit most from the digital transformation opportunities by harnessing the value of the data you hold and ensuring your operations are fit for a digital economy. If not, you're likely to find that the GDPR is just an additional compliance burden and cost to your organisation.

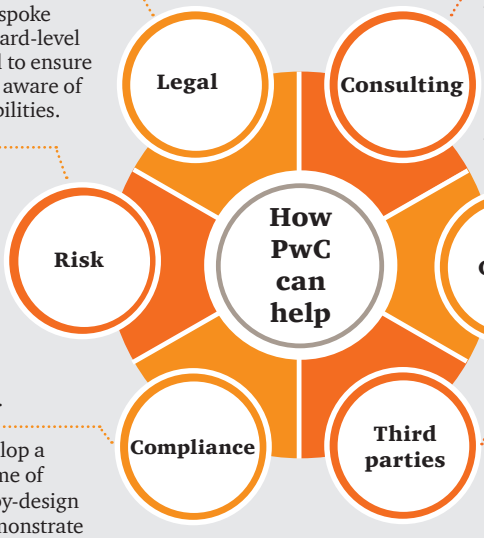
Design and deliver a programme relevant to your business

We recognise that one size does not fit all, and that every business has unique characteristics requiring a tailored approach to data protection. PwC has therefore developed an end-to-end methodology for delivering an optimised GDPR programme.

This approach will help you make informed decisions around managing and protecting personal data and a more targeted approach to data protection investment.



PwC's expertise covers the legal, consulting and assurance aspects of the GDPR in order to provide a one-stop service for your organisation



We provide bespoke training for board-level awareness and to ensure employees are aware of their responsibilities.

We can help you define a strategy for your privacy investment, and a tailored approach based on what matters most to your organisation and your appetite to risk.

We can make your contracts, policies and international data transfer solutions GDPR compliant.

We've the knowledge, experience and skills to build your accountability and governance frameworks.

Cyber security remains a cornerstone of data protection principles. We can help you assess your security, respond to breaches and build a secure environment for data.

We can help you develop a compliance programme of policies and privacy-by-design to ensure you can demonstrate accountability and governance.

We can work with you to assess your vendors' and partners' compliance with the GDPR and design your approach to vendor risk management.

Contacts

If you would like to discuss the issues raised in more detail, please contact one of the team below.

Jon Lowe
Senior manager
T: +44 1481 752028
E: jon.lowe@pwc.com

David Carney
Director
T: +44 1534 838266
E: david.carney@pwc.com

Frank Mullins
Manager
T: +44 1481 752074
E: frank.mullins@pwc.com

William Wilson
Manager
T: +44 1534 838346
E: william.wilson@pwc.com