General Data Protection Regulation - GDPR

EU Data Protection rules set to change

After four long years of political negotiations and lobbying, the EU agreed the final wording of the General Data Protection Regulation ("GDPR") in December 2015. This will impact every entity that holds or uses European personal data both inside and outside of Europe.

The new Regulation will introduce widespread changes to current law and will greatly increase financial sanctions for non-compliance (*up to 4% of annual worldwide turnover for groups of companies*).

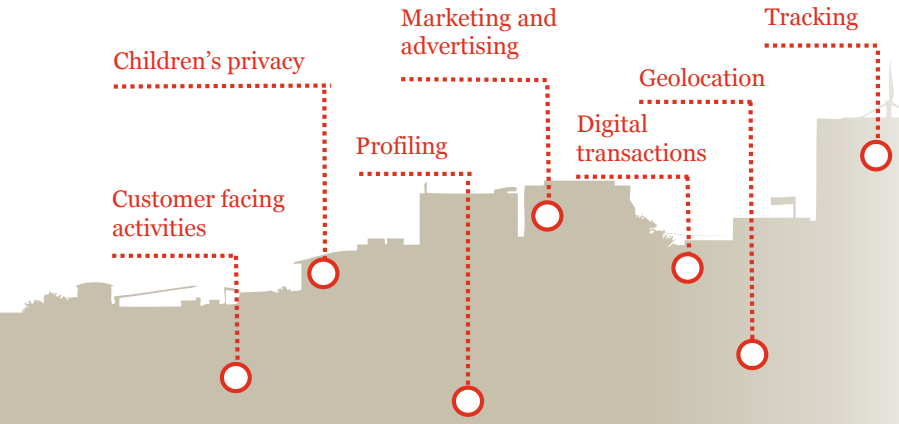
Fines - up to 4% of annual worldwide turnover

You have until the 25th May 2018 to implement all the necessary changes to your systems and operations to meet the new compliance requirements.

Your organisational strategy and approach to comply with the GDPR will need to encompass the **three key components** reflected within the Regulation; a new compliance journey, a new transparency framework and a new enforcement, sanctions and remedies framework.

Pinch Points

The features of business that are most affected by the GDPR are:



Points to consider

- Core components of your business that will be affected.
- Encompassing the three key components of the GDPR.
- You only have until the 25th May 2018 to comply.

The big innovations in the GDPR

The adoption of the GDPR will present numerous new challenges. The key issues to be aware of include:

Issue	Impact
Compliance	Your organisation will have to perform "Privacy Impact Assessments" and privacy audits as a matter of course. You will have to deliver on a new "Accountability" obligation, which means creating written compliance plans, which your business will have to deliver to regulators on demand.
Usage controls	Personal data will be subject to strict new usage controls. These include "data minimisation", "data portability" and "right to be forgotten" principles, which will require your organisation to limit the use of data, to enable individuals to take their data with them at the end of a relationship, and to delete and destroy data on request.
Consent	Obtaining consent to use personal data will be much harder to achieve and to prove.
Supervision	Regulators will also be empowered to carry out audits and inspections of your organisation on demand.
Breach disclosure	Your organisation will be required to report serious contraventions of the law to the regulators and to people affected. Public disclosure of failure is likely to fuel regulatory sanctions and compensation claims, as well as causing damage to your brand and reputation.
Fines	Serious contraventions of the law will be punishable by fines of up to 4% of annual worldwide turnover or €20m, which ever is higher.
Litigation	Citizens and pressure groups will be given the right to engage in group litigation ("class actions") to recover compensation for mere distress caused by contraventions of the law.

pwc

Preparing for the GDPR

Our key services

1. Gap Assessment & Maturity Review
2. Implementation support

We can provide tailored support across all required work streams to help organisations achieve GDPR compliance.

- Strategy and governance build
- Data discovery & mapping
- Policy development
- Privacy by design – PIA's
- Develop Information risk framework
- Identity and access management
- Security – complete cyber offering
- Training & Awareness
- 3rd Party security audits / contract reviews
- Internal Audit

Why PwC?

1. *Proven approach*
2. Proven team
3. Proven track record

Tried and tested approach to GDPR and industry leading proprietary GDPR tools

The only professional services firm that straddles the consultant – lawyer pillars

Recognised as a thought leader in data privacy by analysts such as Forrester, Legal 500 and Chambers UK

A very successful track record of delivering large complex GDPR projects.

Our approach incorporates, what the **legal requirements are for the GDPR** and interpreting these using Lawyers in our team that have also defended organisations in data protection breach cases. We also leverage the unique insights and real life **experience of the ex-regulators** in our team from the ICO that have implemented, enforced and written UK data protection standards.

Our experience

Retail & Consumer
- FTSE 100 Technology Retail Provider
- FTSE 100 Food and Clothing Retailer
- Food Supermarket

Health & Pharma
- Multinational Research and Pharma Company

Entertainment & Media
- International British Broadcaster
- Local UK Broadcaster
- National UK Publication

Financial Services
- Multinational private wealth provider
- International Insurer
- Private Equity Service Provider

Hospitality & Leisure
- Multinational Hotel Group
- Gaming company

Energy
- National Energy Provider

Key benefits

- Confidence over gaps and actions to achieve compliance
- Board and employee engagement
- Optimal GDPR compliance
- Customer & Regulator confidence

pwc