Gearing up for GDPR Compliance - Practical steps to ensure compliance with the revised data protection regulation.

Chris Bernau

October 2016

pwc

Agenda

1. *What do we know about GDPR?*
2. *How should we approach GDPR?*
3. *What can Internal Audit do?*
4. *Can GDPR bring commercial benefits?*

1. What do we know about GDPR?

GDPR is definitely happening!

- Regulation came into effect April 2016 (replaced Directive 95/46/EC)
- Enforcement date set for 25th May 2018
- Affects companies operating in EU **AND** those with European personal data
- Brexit is unlikely to change the ICO stance on GDPR compliance
- Directive is principles based and requires interpretation. Awaiting guidance from ICO.

There are key changes to the existing legislation

Right to be forgotten

Can you dispose of all instances of personal data if requested? Do you know where it all is?

Stronger enforcement

Do you know that fines for non-compliance can be as severe as **4%** of **global** annual turnover?

Data portability

Will your current systems and processes allow the timely transfer of an individual's personal data to a competitor?

How data is used

Insurers and asset managers will need to gain consent for the use of personal data, including analytics, transfer to third parties and across borders.

More frequent disclosure

All data breaches will have to be disclosed to the regulators, and in some cases to the affected individuals.

http://www.eugdpr.org/the-regulation.html

2. How should we approach GDPR?

The GDPR raises many complex issues in a global operating environment.

Many entities will want to prioritise how they tackle the challenges of the GDPR, which often includes taking a risk based approach so that critical economic and high risk issues are addressed first.

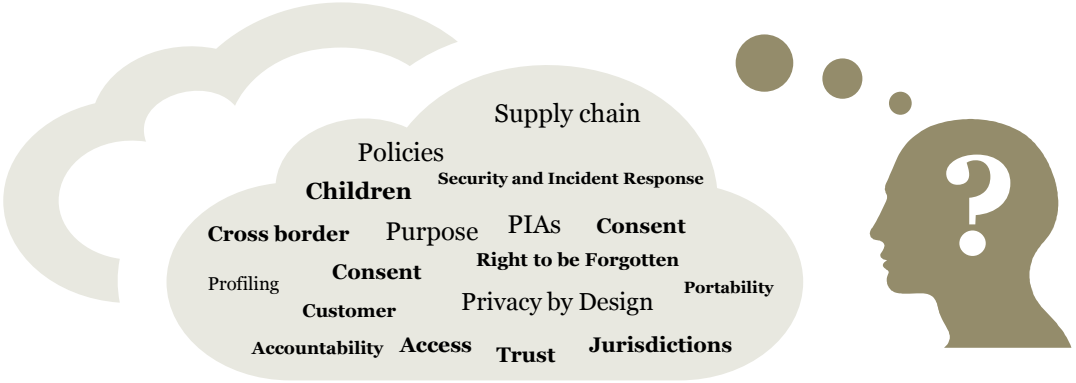
In our experience optimum programme design begins with a vision, which states the objectives and provides an ongoing reference point for the future, ensuring that the business priorities always remain at the forefront.

Once the vision is agreed, a strategy can be developed, and then the programme structures can be put in place. This vision and strategy based approach is particularly relevant for large and complex international companies.

We expect that regulatory investigations and litigation under the GDPR ***will hold organisations to account for their vision and their means for achieving it.***

Our approach - Think differently and begin with a Vision!

What are the priorities in the GDPR? What are yours?



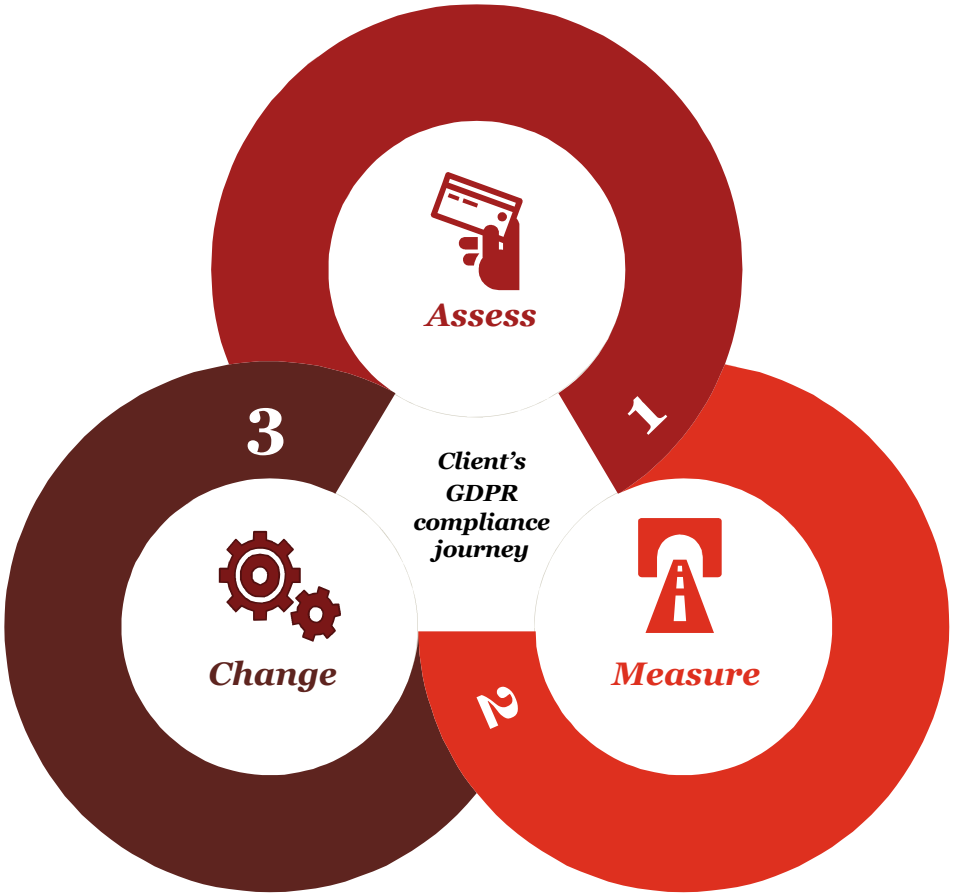
Data Protection Vision = What is your 'Desired End State'?

Strategy = How will you deliver your Vision?

Structures = The programme elements to achieve your Vision

Outcome = Prioritised GDPR programme based on your economic goals, risk appetite and your 'Special Characteristics'

PwC approach to GDPR Compliance – making the vision a reality



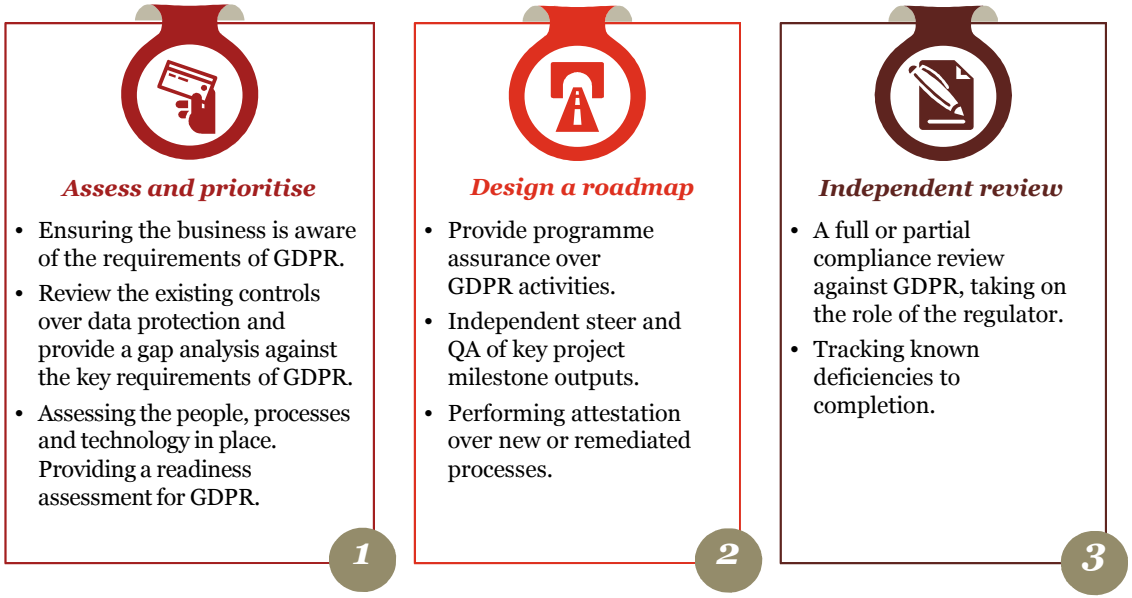
3. What can Internal Audit do?

Is Internal Audit ready to ask the right questions?

The European Commission has mandated compliance with the recently passed General Data Protection Regulation (GDPR) by May 2018. GDPR centralises all existing data protection regulation, updating it for the digital age. This GDPR gives rise to increased compliance requirements backed by heavy financial penalties *(up to 4% of annual worldwide turnover for groups of companies)* and a direct right of action for citizens in European courts.

The introduction of disruptive regulation is a great opportunity for Internal Audit to drive business change by proactively engaging with management to assess the readiness for GDPR. Being ready to provide appropriate independent challenge at the right stages of the **GDPR readiness journey** will be valued by the business and will provide vital support and steer to achieving compliance prior to the 2018 deadline.

What can Internal Audit do at each stage of the GDPR readiness journey?



4. Can GDPR bring commercial benefits?

Commercial benefits?

- Can we spend a few minutes as a group to discuss what benefits there may be (5 mins)

Commercial benefits?

- Doing the right thing with personal data can enhance brand values
- Data quality improvements – quality and consistency of MI should improve
- Getting consent right early will allow your firm to use data where others may not
- System updates / consolidation reducing long term IT spend
- Will make it harder for unregulated firms to enter the market and take share
- Avoidance of fines / reputational damage for non-compliance

How we react positively to enforced changes can make a real difference, particularly in a crowded marketplace.

www.pwc.com

151026-154131-NS-OS