GDPR: Was all the fuss worth it?

The state of affairs nine months on.

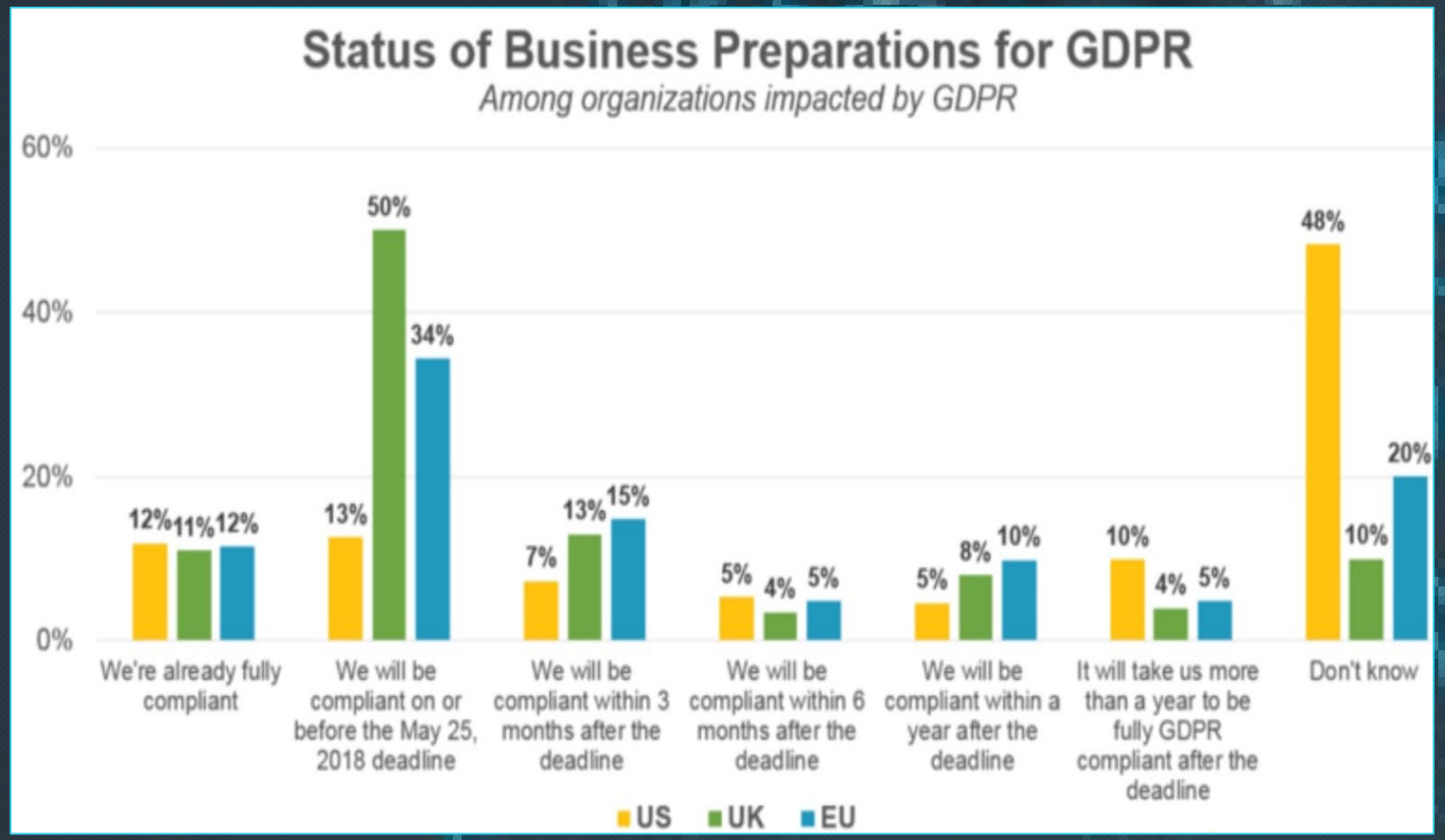
Andrew Denley
Mark Foulsham
Brian Hitchen

GDPR - Recap

- The Regulation
  - 177 Recitals and 99 Articles
- EU Directive
  - Working Party 29, European Data Protection Board
- ICO Commitment
  - Guidance and Assistance
- DPA 2018
  - Broadly based on the GDPR but with changes specific to the United Kingdom

Business Readiness pre May 2018

- Business attitudes
- Commitment
- Preparation
- Achieving compliance



May 25th came and went

How did business react

May 25th – came and went

- ICO releases a statement
  - *"…….it's important that we all understand there is no deadline. 25th May is not the end. It is the beginning"*
- *Many businesses still viewed GDPR as a 'Year 2K" issue*
- *There was confusion as to who should register with the ICO*
- *GDPR was still being mis-reported by the Press*
- *The World didn't end and Business continued as normal*
- *Huge fines were not suddenly levied by the ICO*

Data complaints and breaches rise

- In the first nine months since GDPR became law the ICO has reported:
  - 19,000 complaints from the general public ranging from subject access to data security
  - In excess of 8,000 data breaches have been reported
- In the UK the ICO has yet to bare it's teeth although it has issued a £500K fine to Cambridge Analytica (the maximum fine under the DPA1998)
- The ICO has stated that it will encourage compliance over financial penalty

GDPR across Europe

- Germany reacts five days after the introduction of GDPR
  - The Regional Court in Bonn issued a ruling on the practical application of the GDPR
- In France the data regulator, (CNIL), reported in late September 2018:
  - It has received over 3,500 data protection complaints -a 64 percent increase compared to the same period in 2017
  - It has received 600 data breach notifications during the same period.

Globally it is estimated that 25% of the population has suffered data compromise

Google Fined

- France’s data protection authority (CNIL) have levied a €50M fine against Google for failing to obtain adequate consent from users when processing their data for the purposes of personalised advertising.
- The Swedish data protection authority (Datainspektionen) have, this week, started an investigation into Google’s practices and stating Google are in breach of Articles 5,6,7,12,13 and 25 of the Regulation.

The journey to compliance

Uncertainty and mis-information

- There was (and still is to a degree) uncertainty around
  - Whether compliance is necessary
  - The role of Data Controller and Data Processor
- The media consistently published incorrect information
- Businesses without access to skilled resources tended to over-compensate
  - Insistence that contract staff register with the ICO for data handling

Problems faced by business

- Some businesses adopted a Legal based approach, some a Risk based approach
- The former often attempted to apply every letter of the law – all 99 Articles
  - Key priorities of the Regulation were not being addressed
- Resource issues
  - Many relied on their IT teams/suppliers who often lacked key skills
- Lack of engagement at senior level (complacency)
- Nine months on from May 2018, the ICO, however, believes that GDPR is now very much on business agendas

GDPR Compliance around the globe

- In 2017 Dell Dimension Research undertook a global survey on preparedness. Of the 800 responders they found:
  - More than 80% of responders knew little or nothing about GDPR
  - Close to 70% of IT and Business professionals were unaware of whether their companies had any plans at all
  - In Germany 44% of responders felt ready to GDPR
  - Responders in the Benelux area were least prepared (26%)
- TrustArc's 2018 global survey of 600 US, UK and EU companies found only 20% had achieved a defensible GDPR compliance

Future Landscape

GDPR, DPA2018……

Post Brexit landscape

- Whatever the deal, the UK Government is committed to Data Protection
- The ICO is expected to rigorously apply the DPA-2018
- Compensation claims under Article 82 of the GDPR will still apply under section 168 of the DPA-2018
- Will there be a DPA-2018 Certification?
  - Chapter 2, Paragraph 17-8 relates to Article 42 of the GDPR which ‘encourages’ authorities to introduce certification

Brexit ‘no deal’ implications

- EC’s Consumer Directorate had stated that the UK will be considered a ‘Third Country’ citing ‘Considerable uncertainties’
  - the EU may not regard the UK as safe for data!
  - The UK cannot count on ‘Adequacy by default’
- The UK Government has made clear that data can flow from the UK to the EC but for data transfers from the EC to the UK then EU Transfer rules will have to be applied.
- In principle (in the UK) the GDPR will not apply, only the DPA-2018
- But if a company operates in Europe, then GDPR compliance is mandatory.
- The ICO will *not* be the regulator for any European-specific activities caught by the EU version of the GDPR

Source: ICO

So what should you do?

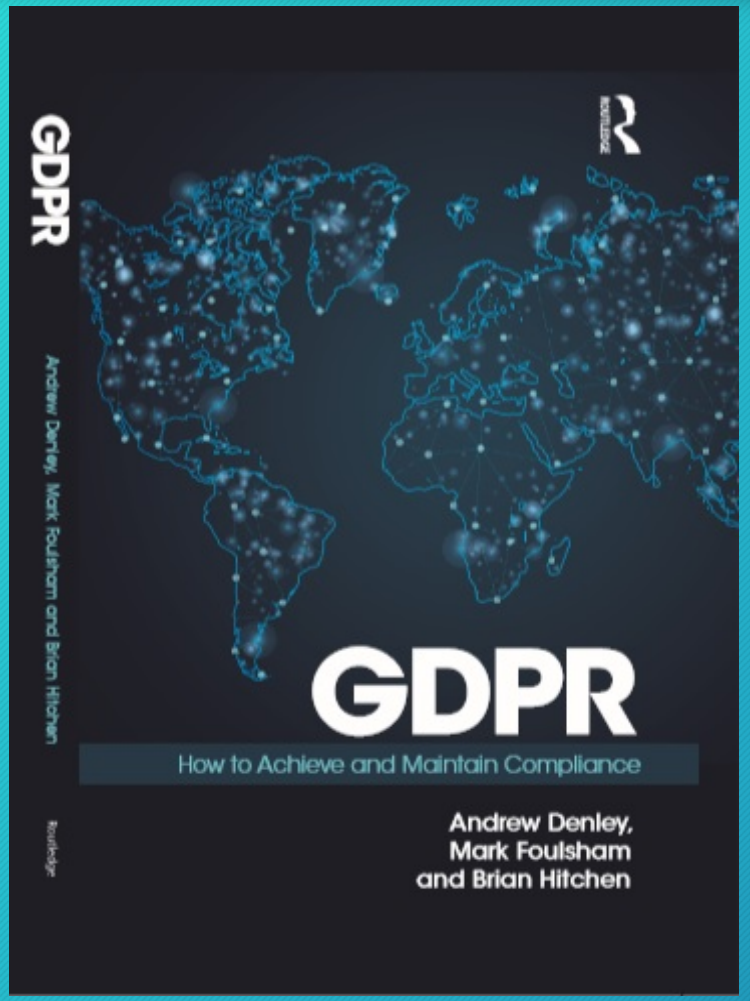
What should be you GDPR Strategy?

- Irrespective of whether you believe you have achieved compliance, partly achieved or not achieved at all you MUST progress and strive for continuous improvement
- Data protection MUST be built into your BAU – (*Data Protection by Design and Default – Article 25)*
- Keep abreast of case-law – there will be changes
- Getting the basics right will ease the journey
- Get professional help

What could non-compliance mean?

- There is a minimal threat of an ICO fine so companies, whilst registering with the ICO, are not rushing toward GDPR compliance, which may be a mistake
- There appears to be an increasing threat of compensation claims under Article 82 *"Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"*
- Legal firms offering 'Data Chasing' services
  - Run a search on 'Cambridge Analytica' or BA
- There still appears to be a misunderstanding between 'Data Controller' and 'Data Processor' leading to assumptions of liability for data
  - Parties who should be compliant are assuming that the other party is compliant!

Achieving and Maintaining GDPR Compliance



- This book:
  - Shows you how to prepare your GDPR project
  - Explains which Articles you'll need to consider and those which you don't
  - Provides examples and scenarios
  - Shows you how to apply Information Security
  - Shows you how to manage GDPR as part of the business
  - Guides you through security in supply chain management
  - Plus lots more!

Questions

- Mark Foulsham mark.foulsham@keyenable.com
- Andrew Denley andrew.denley@key2enable.uk
- Brian Hitchen brianhitchen@hotmail.com