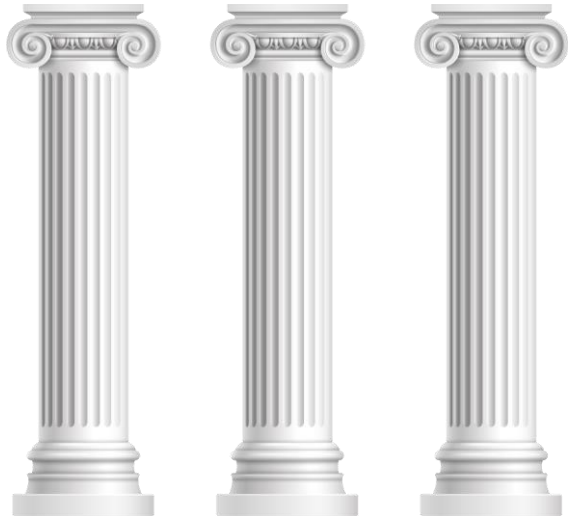
Business & Management



GDPR update

17 APRIL 2019

The webinar will begin shortly…

Business & Management
20 minute lunch

Louise Marshall

The GDPR one year on

Quick refresh: part 1

- GDPR came into full force and effect on 25th May 2018
- UK DPA 2018 enacted at broadly the same time
- UK's imminent departure from the EU will not affect its enforceability
- Wide ranging legislation with far reaching territorial scope: *wherever* the processing of personal data of EU citizens takes place, the GDPR will apply to processors.

Quick refresh: part 2

- Origins of GDPR in the Universal Declaration of Human Rights of 1948
- Well intentioned initiative to restore ownership of personal data to the data subject:
  - Controllers (and processors in certain circumstances) accountable
  - Obligations of Communication and appropriate Data Security
  - Data Subjects' rights, directly enforceable against Controllers
  - Administrative and/or judicial proceedings available to data subjects
- Sanctions include large fines but also order for cessation of all processing (AggregateIQ Data Services Inc, Canada) and reputational damage

Level of “Uptake” and resulting benefits

- End 2018: surveys by Marketing/Signals, TrustArc, Dimensional Research put 20 – 53% of business at implementation stage.
- CISCO’s 2019 Data Privacy Benchmark Study found that:
  - Compliant organisations were 15% less likely to suffer data breach
  - Where breach does occur, damage significantly more contained (79,000 records affected rather than 212,000)
  - 42% of respondents reported increased agility and innovation
  - 36% reported improved appeal to investors
  - 37% reported reduced sales delays caused by customers’ privacy concerns

Enforcement: part 1. The UK

- ICO (UK Supervisory Authority). March 2019 146 Sanctions.
  - 89 Fines
  - 31 Enforcement Notices
  - 14 Undertakings
  - 12 Prosecutions
- December 2018 10 largest ICO fines totalled £5,000,000
- Famous names:
  - BT : June 2018 £77,000
  - Equifax: September 2018 £500,000
  - Heathrow Airport : October 2018 £120,000
  - Facebook: October 2018 £500,000

Enforcement: part 2. Most frequent incidents of infringement

- Failure to register with ICO and pay appropriate fee (£35-£2900)
  - Several thousand UK firms failed to take this step. Fines up to £4,350
- “Spamming”: unsolicited emails or telephone calls (BT; Vote Leave Limited; Leave.EU.Group) Fines here in £ tens or hundreds of thousands
- Failure to put in place adequate data security measures (Article 32 GDPR): Equifax; The Conservative Party; Facebook; Heathrow)
- Failure in obligations of transparency and information (Facebook)
- Loss of personal data to departing employees.

Enforcement: part 3. Europe

- October 2018: Austria. €4,800. Failure of obligations of minimisation and proportionality (CCTV)
- November 2018: Germany. €20,000. Inadequate data storage and security arrangements (chat site passwords unencrypted)
- December 2018: Germany. €multiple. Failure to put Article 28 processor agreements in place, €5,000 per incident
- December 2018: Portugal. €400,000. Inadequate data security (hospital records)
- January 2019: France. Google. (lack of transparency, inadequate information and lack of valid consent)

Lessons to be learned?

- Ensure senior management buy in and support, this is not a “back-office only” matter.
- Much more care with data security.
  - Privacy by Design; DPIA; encryption; minimisation; annonymisation
- Past behaviours are not adequate for GDPR standards.
  - CCTV
  - Consent (BT and Google)
  - Lack of transparency/information
- Failure to put the data subject first.
  - Lack of awareness of what data is held/processed
  - Lack of knowledge about data which can be kept/must be deleted
  - => failure to respond properly to subject requests.
- Failure to document or record processing activity (Article 30)
  - Not quite a get-out-of-jail-free card but essential to demonstrate compliance
- Failure to register (and build a relationship) with the ICO.

There is still time to start

- Board awareness and accountability
- Determine whether you are Controller or Processor
- Register with the ICO
- Build out and maintain ROPA
- Data Mapping (Categories/Types/Purposes/Legal Bases/Storage/Sharing) =>
- Article 13 Privacy Notice (Google, remember?)
- Appropriate technical and organisational measures
- Complete DPIAs when in any doubt
- Determine if you need an EU Representative (no-EU businesses) and post Brexit, a UK Representative
- ASK FOR HELP.

Business & Management
Webinars and events – icaew.com/bamevents

Free 60 minute webinars – 10.00am

Manage change effectively
1 May

Economic update
5 June

Dealing with difficult conversations
3 July

Conflict resolution
9 October

Free 20 minute webinars – 12.30pm

AML update – What every business needs to know
8 May

Influencing and persuading – Promoting your brand
15 May

How accountants can become digital leaders
19 June

Marketing for finance – Top tips and shortcuts
10 July

Free event – 6.00pm

Why don't staff always do what you want them to do?
23 April

Online e-learning – 9.30am

Rapid month-end reporting – by day three or less
21/22 May

Business & Management

THANK YOU FOR ATTENDING

Contact the Business & Management Faculty

icaew.com/bam

✉ bam@icaew.com ☎ +44 (0)20 7920 8508

@ICAEW_finman

Join the Business & Management Faculty

icaew.com/joinbam

Upcoming BAM webinars and events

icaew.com/bamevents