



# *Audit and Assurance Faculty Webinar*

## *GDPR: issues for auditors*

PRESENTED BY RICHARD GILLIN AND EMIEL SPOOR

# *Presenters*



Richard Gillin  
Deloitte



Emiel Spoor  
Deloitte



Sophie Campkin  
ICAEW



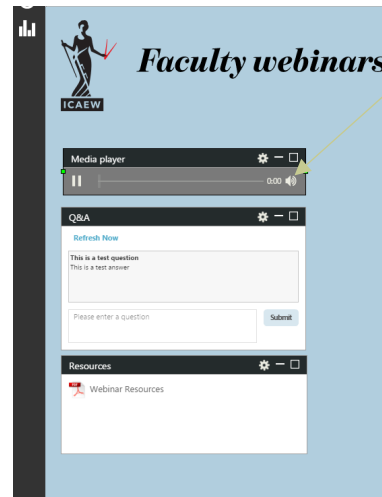
Jane Berney  
ICAEW

# *Join the Audit and Assurance Faculty*

- Monthly newsletter and publications
- Webinars and events
- Influence – have your say
- Thought Leadership
- Career Development

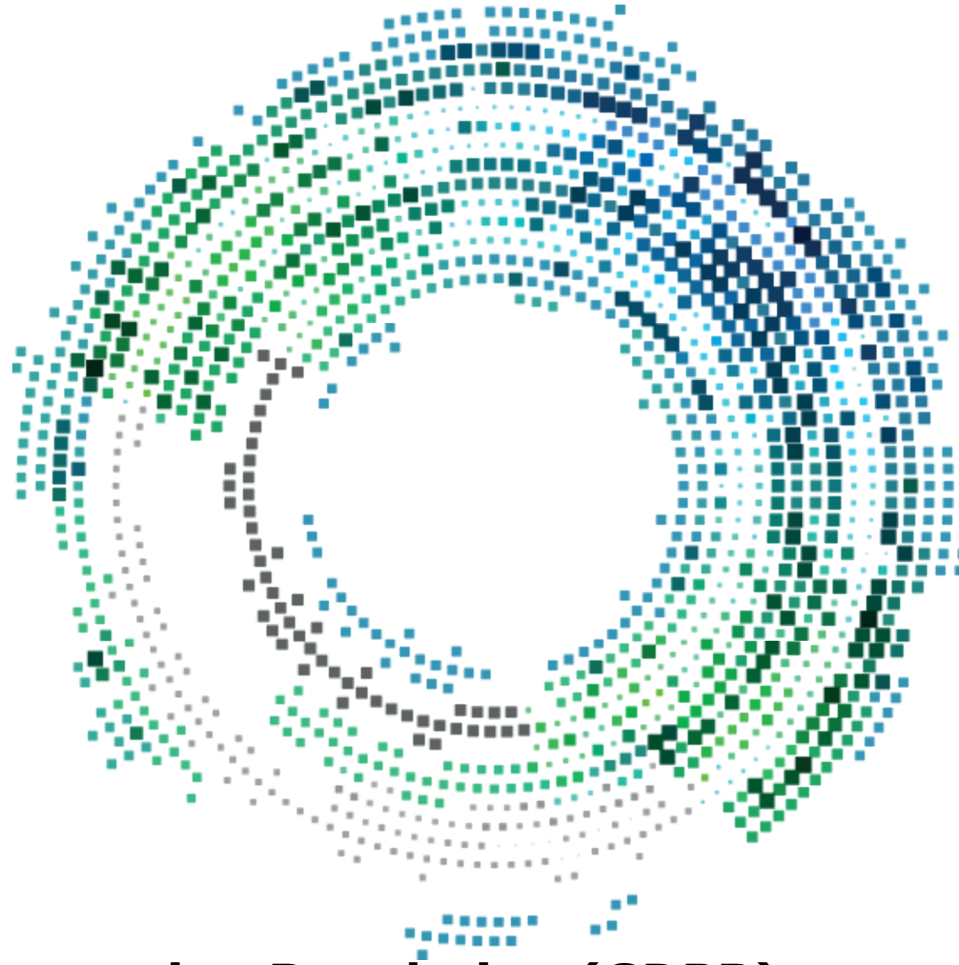
[icaew.com/aaf](http://icaew.com/aaf)

# *Introduction*



- Audio problems?
- ensure your volume is turned on
  - if you experience poor sound quality you may benefit from refreshing your page

**Deloitte.**



## **General Data Protection Regulation (GDPR), Audit and Assurance**

Richard Gillin, Emiel Spoor

23 April 2018

## Massive Equifax data breach hits 143 million

© 8 September 2017 | Technology

f t d e Share



It has been marked as the worst data breach in US history. Attackers stole half the US population's Social Security numbers from Equifax this spring, but the company only notified people in September.



Cambridge Analytica

- Personal data of 87m Facebook users compromised
- Use of personal data and analytics by political campaigns, parties, social media companies and other commercial actors
- Allegedly influenced the outcome of the 2016 US presidential elections and Brexit referendum
- ICO investigates 30 companies, including Facebook

## Google loses landmark 'right to be forgotten' case

Businessman wins legal action to force removal of search results about past conviction



▲ The judge rejected a similar claim brought by a second businessman. Photograph: Dado Ruvic/Reuters

# GDPR

## *Basics*

- GDPR has been **in force** for almost 2 years now and will be **enforceable** from 25 May 2018
  - The ICO says that there will be **no further grace period**
- The scope has broadened to include **any data** related to an identifiable individual
  - Under DPA the focus was on Sensitive Personal Information
- GDPR applies to all (global) organisations that collect, use, store and transfer personal data in the EU or about individuals in the EU
- Sanctions include substantial monetary fines and a stop order
- Data Controllers must provide **Privacy Notices** to explain what personal data they process, why, how, for what lawful reason, with what supply chain, how long for and explain the data subject's rights
- Data Controllers have to evidence compliance with the principles of GDPR
- Data Processors have obligations and liabilities related to their own processing

Note that **non-compliance is more easily detected**  
by the Data Protection Officer and data subjects

# How do we achieve GDPR compliance?

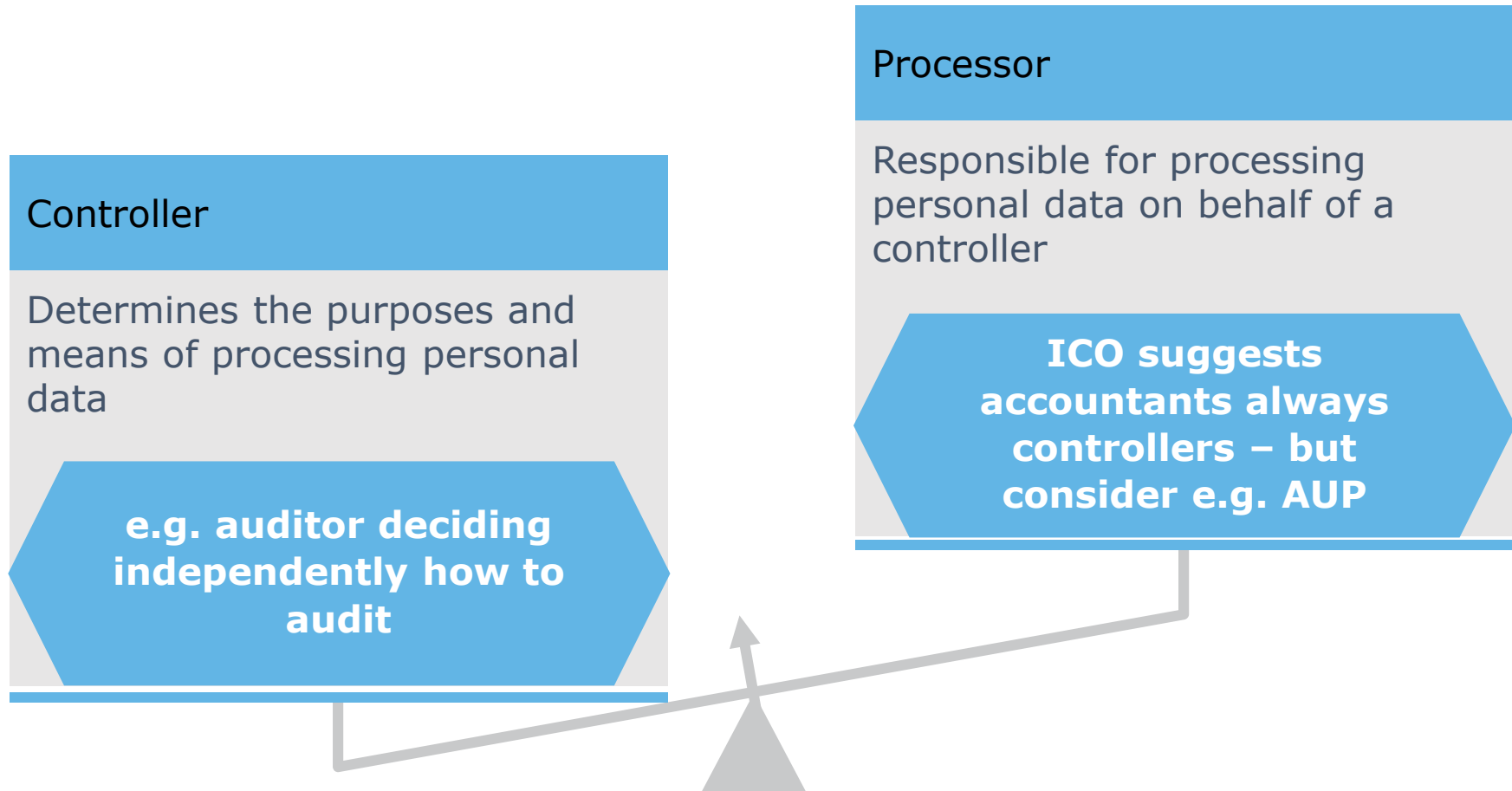
*Evidencing compliance with GDPR principles,  
focussing on the risk to the data subject and their rights*

- Find out what you are processing
- Assess the risks to the individual, include third parties
- Determine appropriate technical and organisational mitigations
- Ask data subjects their opinion about necessity and proportionality of the processing
- Use Data Governance and exercise Data Protection by Design and by Default
  - Don't forget about Data Subject Rights
- Produce Record of Processing Activities, Data Protection Impact Assessment and Privacy Notice, as appropriate
- Gather documented evidence of GDPR compliance before processing
- Ensure contractual support for GDPR compliance and monitor compliance
- Implement incident management and breach notification procedures

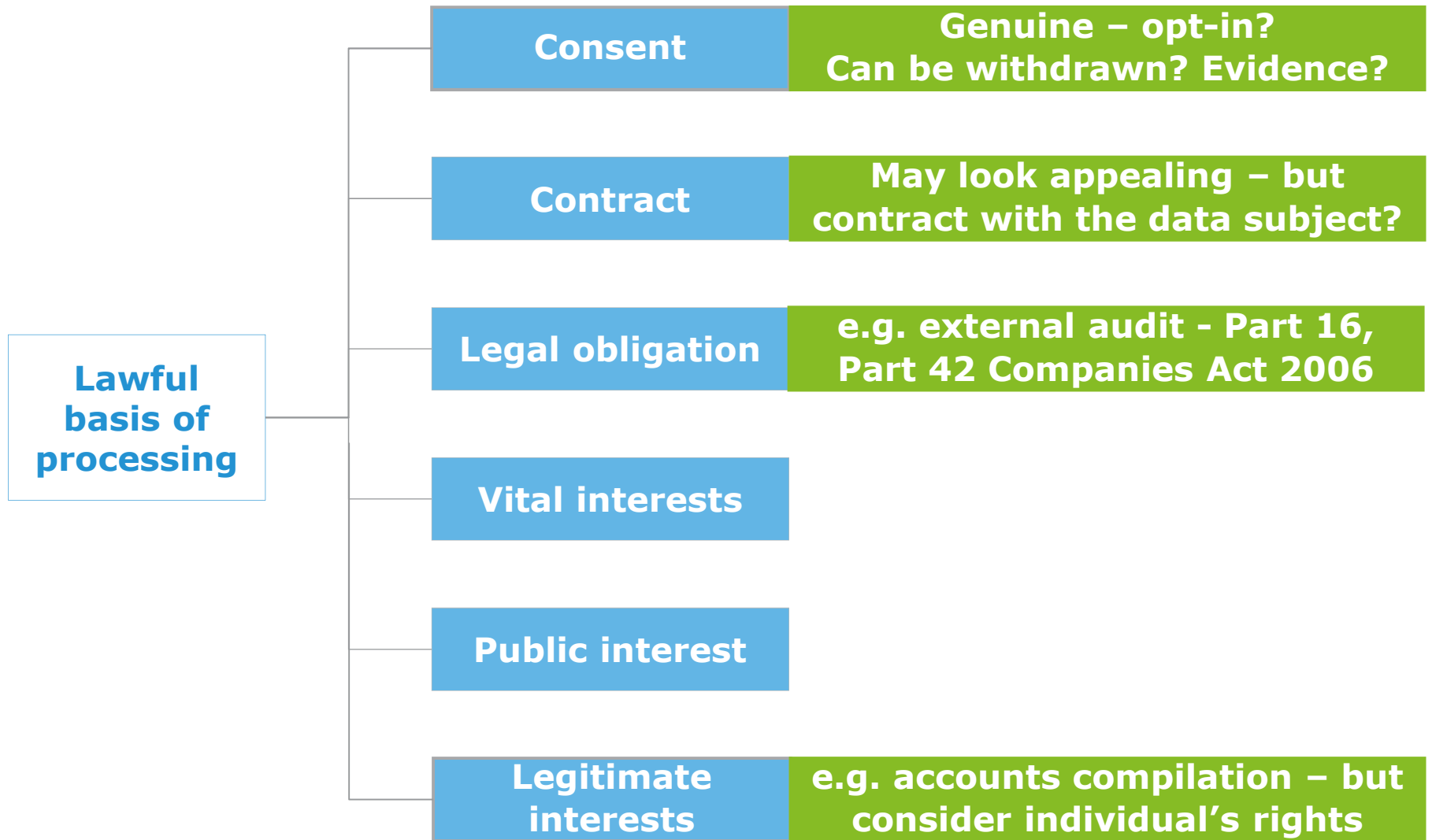


# **GDPR and audit and assurance**

# Controller vs Processor



# Lawful basis of processing



## Special category data



- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic/biometric data
- Health/sex life/sexual orientation

Lawful basis not enough –  
may need more e.g. explicit  
consent, public interest

# Engagement letters

## Controller-Controller

- GDPR strictly silent but consider:
  - Previous text might be out of date
  - May want to clarify you really are a controller
  - General client expectations – many are writing to all suppliers with processor language



## Controller-Processor

- Article 28 has a prescriptive list of content including:
  - Use of sub-processors – now must be agreed
  - Non-EEA transfers
  - Delete/return data at end of contract
  - Make available information re compliance (“right to audit”)
  - Notify breaches etc.

# Privacy notices



- Article 13 – from the data subject vs Article 14 – from someone else

*Article 14 likely for an audit where a client gives you data about their employees, customers and suppliers*

- Consider use of website – in particular for Article 14

*Unlikely to have contact details for all data subjects*

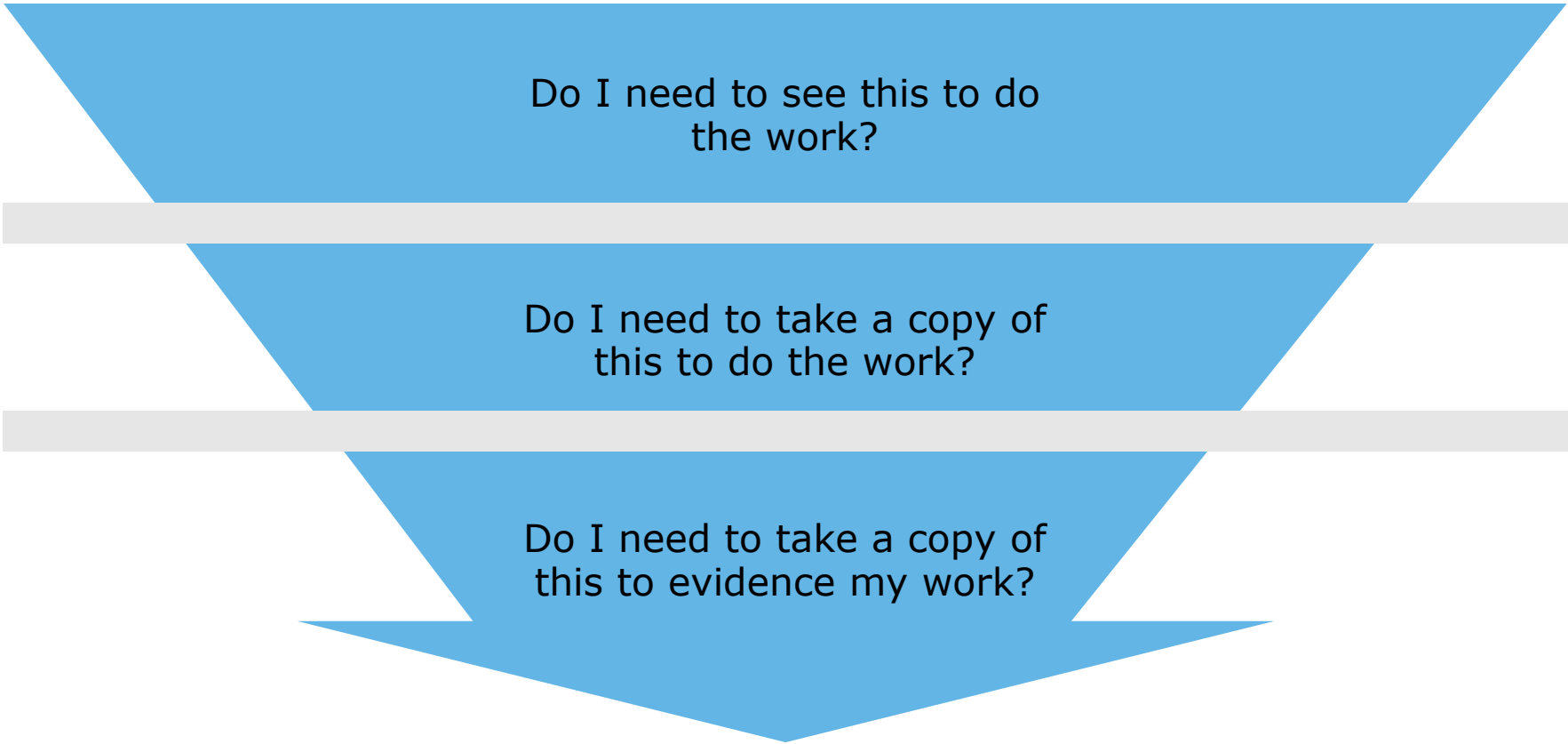
- Consider use of processors (if you're a controller) or sub-processors (if a processor) – and whether data might leave the EEA

*Think about IT providers e.g. your accounting software provider if you've moved to the cloud – and where the data is hosted*



# Privacy by design and privacy by default

## Data minimisation



Do I need to see this to do the work?

Do I need to take a copy of this to do the work?

Do I need to take a copy of this to evidence my work?

# Privacy by design and privacy by default

## Minimisation? Pseudonymisation?

### Example

- We want to test a 4% pension contribution
- Client sends dump from payroll system
- Didn't need name, address, tax code
- Didn't (arguably) need to keep actual figures – but most people would?
- Probably do need payroll number to enable sample to be retested – ISA 230 test – but without names a lot more secure – though not truly anonymous e.g. can work out who the CEO is

Payroll number	Name	Address	Gross pay £	Tax code	E'e pension £
...	...	...	...	...	...
17	Fred	67 High Street	50,000	1150L	2,000
18	Tom	123 ICO Avenue	70,000	30K	2,800
19	Diane	The Mansion	250,000	465K	10,000
...	...	...	...	...	...

Can you send me just the following fields?

Can you send me another copy with just what I asked for?

I deleted the columns I didn't need, but careful what you send in future.



# Privacy by design and privacy by default

## More things to consider



### Security

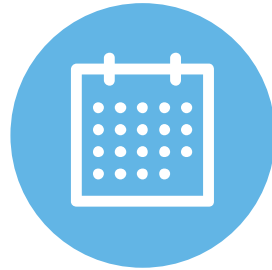
Are your systems up to date?

Who can access which files – hard copy vs soft copy?

Client transfers?

Encrypted where appropriate?

Tested?



### Data retention

How long do I need to keep my data e.g. law, Audit Regulations, ISQC 1, Practice Assurance Standards

Am I keeping multiple copies unnecessarily?



### Data destruction

Am I deleting data I no longer need?

Consider carefully e.g. emails held outside the audit file? Information in online storage?



### Have I trained my people?

Do they know policies and procedures?

Will we remind them to tidy up data?

# Dealing with breaches

---

	Notify the ICO?	Notify the data subjects?
Does a controller need to notify?	Controller to notify within 72 hours unless unlikely to result in risk to rights and freedoms	If a "high risk to the rights and freedoms" communicate without undue delay unless: <ul style="list-style-type: none"><li>- Appropriate technical and organisational measures taken e.g. encryption</li><li>- Subsequent measures to high risks unlikely to materialise</li><li>- Disproportionate effort</li></ul>
Does a processor need to notify?	Processor to notify controller without undue delay	Art 28 requires processor to co-operate – likely to be contractual commitment to tell controller, who may then tell data subject

---



This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

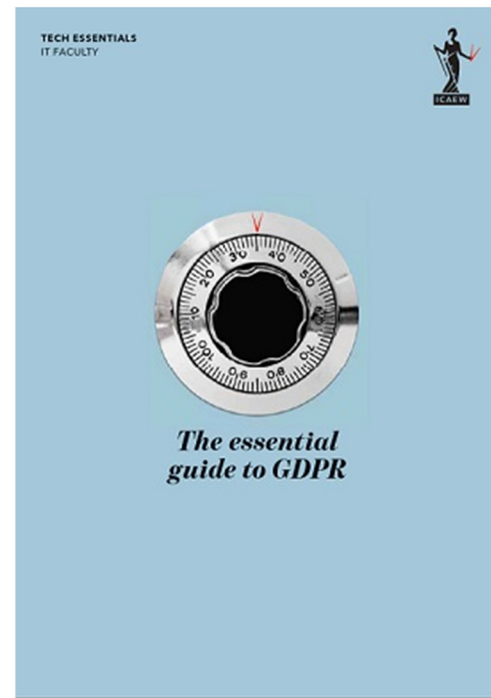
Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 2 New Street Square, London, EC4A 3BZ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more about our global network of member firms.

© 2018 Deloitte LLP. All rights reserved.

# GDPR resources

- [icaew.com/gdpr](https://www.icaew.com/gdpr)
  - FAQs
  - Links
  - Engagement letter templates
  - Essential Guide to GDPR





*Any questions?*

# *Future webinars and events*

- Webinars
  - 3 May – Audit of bank and cash in the light of recent developments
  - 12 June - When audits go wrong.....and right! The importance of being skeptical
- Roadshows
  - Taking place at various locations in April, May and June
  - Focus on the latest developments in audit technology
  - Provide a round up of the latest news

Further information regarding Audit and Assurance Faculty events programme for 2018 can be found at [icaew.com/events](http://icaew.com/events)

# *Thank you for attending*

Please take the time to fill out our short survey

Contact the Audit and Assurance Faculty

 +44 (0)20 7920 8671

 [tdaf@icaew.com](mailto:tdaf@icaew.com)

 [icaew.com/aaf](http://icaew.com/aaf)

ICAEW and the speakers will not be liable for any reliance you place on the information in this presentation.  
You should seek independent advice.

