IRMS Conference 2018

How to achieve GDPR compliance

Is it just Records Management with extras?

Is there a link between GDPR and RM?
What does GDPR compliance require?

- What do you have?
- Where is it?
- What are you using it for?
- Do you have a legal basis for processing?
- How long do you retain it?
Do these map to RM principles?

- Asset register
- Process map
- Retention schedule

What does not map

- Legal basis for processing
Where to get advice:

‘BS 10012: 2017 Data protection – Specification for a personal information management system’

First published 2009, updated for GDPR 2017
Contents

- Understanding the organisation and its context
- Leadership, policy, roles / responsibilities
- Data inventory and data flow
- Legal basis for processing
- Privacy impact assessment / treatment
Contents

• Privacy by design / default
• Support and documentation
• Key appointments
• Training and awareness
• Privacy notices and consent
Contents

• Children’s information
• Data sharing and matching
• Data accuracy and minimisation
• Retention and disposal
• Security and breach management
IRMS Conference 2018

Contents

• International transfers
• Rights of individuals
• Performance evaluation / improvement
International privacy

International privacy

Project in ISO/IEC/JTC 1/SC 27

- Direct link to Information security
- Adds PII management controls
- Use as a checklist
International privacy

Scope

• International
• Data controllers
• Data processors
• Joint controller / processor
International privacy

Current contents

- PIMS specific requirements (ISO/IEC 27001)
- PIMS specific guidance (ISO/IEC 27002)
- Additional guidance for PII controllers
- Additional guidance for PII processors
- Annex A Controls for PII controllers
- Annex B Controls for PII processors
International privacy

Future

- Certification
- Compliance scheme
- Trust marks
- Worldwide adoption

Who knows????
Thank You
Any Questions?
Contacts

Alan Shipman
Phone: 01923-450527
a.shipman@group5.co.uk
www.group5.co.uk