Preparing for GDPR: Action Plan Case Study

Suzy Taylor
Information, Records and Projects Manager / Data Protection Officer
Chair Information & Records Management Society (North Region)
Our Action Plan

- Began Jan 2017 looking to finish by March 2018
- 7 Basic Strands
- Initiated by ‘Information Management Steering Group’ and delegated to ‘Information Compliance Group’ to ensure implementation
- Less work because of existing records and information management processes and policies
- Risk assessed approach, target risk areas first
7 Strands

- Training and Awareness
- Privacy Notices
- Information Security Review
- Contracts Review
- Data Sharing Agreements Review
- Customer Processes Review
- Governance Measures
Training & Awareness

- Started first – ongoing
- Briefings for senior management
- New online training course covering DP & IS, refresher for all staff
Privacy Notices

- First action for the Information Compliance Group, representing departments that collect data from individuals
- Identify points of collection and ensure adequate Privacy Notices are supplied

! Risk Area – Complaint of GDPR breach (Articles 6 & 13)
Information Security Review

- Head of ICT led on any and all improvements which might reasonably be made to improve the protection of personal data:
  - Two factor authentication
  - Physical security
  - USB Sticks
  - Virus protection
  - Block websites
  - Use of hosted facilities

! Risk Area – Data Breaches & Security (Articles 32-34)
Contracts Review

- Began August 2017
- Procurement process
  - Identify data processors and ensure they are contracted
- Funding Contracts
- Sub-contracted parties

- Risk Area – Third Party Data Breaches
- Risk Area – Controller/Processor (Articles 24-31)
Data Sharing Agreements Review

- Began August 2017
- Review arrangements in place and compile a list of data sharing agreements

! Risk Area – Data Breaches

! Risk Area – Controller/Processor (Articles 24-31)
Customer Processes Review

- Scheduled for Dec 2017
- Largely covered during identification of areas to be covered by Privacy Notices
- Will cover in depth Jan-Mar 2018

Risk Area – Complaint of GDPR breach (Articles 6 & 13)
Governance Measures

- Began Jan 2017, ongoing
- Full review of policies and procedures to ensure we can provide mandatory information to ICO or to any Controller for whom we are a Data Processor
  - Register of Processing Activity
  - Review Data Disposal capability of our proprietary databases
  - Breach Notification
  - Guidance on Privacy Notices
  - Guidance on Impact Assessments
  - Revised Subject Access procedure to incorporate other information requests
  - Special Category Data?
Due to complete May 2018?

- ICO readiness
- Transparency
- Communication
- Having a plan