IRMS Ireland Seminar
Thursday, 23 November 2017
45 Merrion Square, Dublin

Sponsored by

Thanks also to our speakers and the Irish Architectural Archive
10:00–10.05  Welcome and Introductions

10.05–10.50 Digital Records Management: a risky business
Heather Jack, HJBS Ltd & John McDonough, Director National Archives

10.50-11.20 Records Management and GDPR
Jennifer McGrath, Records Management Unit, Houses of the Oireachtas Service

11.20-11.30 Break

11.30-12.00 GDPR risks and Readiness
Craig Dade, Information Management Services, Crown Records Management

12.00-12.30 Data Protection Audits: A presentation on the 2017 ICO Audit of NI Health Care Trusts
Claire Graham, Head of Information Governance, Southern HealthCare Trust
12.30-13.30  Lunch and networking opportunity

13.30-14.00  GDPR The Journey so Far
Jenny Lynn, Information Management Unit, Department of Finance (NI)

13.30-14.00  GDPR: What you need to know
Deirdre Allison & Gillian Acheson, Belfast Health and Social Care Trust

14.00-14.30  Going it alone: GDPR sources for the Practitioner
Claire Graham, Head of Information Governance, Southern HealthCare Trust

14.30-15.00  News from the IRMS executive/sourcing the training you need to be GDPR-ready
Fiona Kearney, Secretary IRMS

15.00-15.30  AGM for IRMS members

We are very grateful to our sponsors Crown Records Management
Digital Records Management: a risky business

John McDonough, Director National Archives
Heather Jack, HJBS Ltd
The General Data Protection Regulation (GDPR) and Records Management

Jennifer McGrath, Houses of the Oireachtas Service
The General Data Protection Regulation (GDPR) and Records Management
Houses of the Oireachtas
Records Management Unit

Information Governance – joined up approach
Records Management Unit

- Strategic Objectives - Protection Compliance and Control

- Four staff members - Records officer, FOI officer, Information assistant

- Establishment 2016 - FOI and Records Management since 2012, Data protection since 2016
Data protection 'monster' looms

The Irish Examiner
12 August 2017, 470 words, English, © Irish Examiner, 2017, Thomas Crosby Media, TCN

Awareness around a new European law on the protection of personal data is increasing, but its implications for Irish firms requires a “massive push”, according to technology experts.

The new general data protection regulation, or GDPR, which comes into place in May next year, means private and public companies will have to take more care than ever over the ways they store and protect the data of citizens in the EU.

It is designed to harmonise data privacy laws across Europe and to protect citizens’ data privacy.

Unlike an EU directive, which can be implemented over a certain time, the regulation becomes law from May 2018, meaning penalties can be imposed from the very first day.

It applies to organisations in the EU but also to any foreign firms doing business inside the bloc.

If companies fail to comply with the regulation, they can be fined up to 4% of annual global turnover, or €20m.

Chief executive of Cork-based Smarterc, Ronan Murphy, said the law was a “monster” in the scope of the regulations, saying that a massive push was needed to make as many organisations as possible aware before the May deadline.

“First off, GDPR is a good thing as it is to protect all of our data and aims at preventing breaches. There is a lot of scaremongering about the new regulation, which needn’t be the case,” he said.

“However, that doesn’t mean it shouldn’t be taken very, very seriously indeed. We are way, way behind still unfortunately but thankfully, there does seem to be growing awareness,” he added.

According to cyber security experts, under the new regulation, Irish firms will have to comply with up to 90 principles relating to data protection.

Mr Murphy added: “What it boils down to is that data protection officers will be able to ask how data is stored, protected, kept and used on customers, consumers, employees, etc. It will affect companies, government agencies, private public partnerships, universities,” he said.

He said he would advise firms to carry out a readiness assessment to see how prepared they were for the new law.

“While the law is implemented on day one and fines can be imposed on non-compliant firms, I would imagine firms taking steps to comply would be looked more favourably upon even if not fully-compliant,”
Overhaul of the Data Protection legislation

- **Consent** - Rules on consent to change, significant implications for public bodies

- **Subject access requests** - Right to a quicker response with no fee

- **Review** all processing of personal data to ensure there is a legal basis – Public bodies can no longer rely on legitimate interest or consent and must consider the need for specific amendments to primary legislation governing their own activities

- **Conduct a Data Inventory** - detail processing purpose, categories of data held, who data is shared with and retention schedules— replaces the register

- **Conduct Privacy Impact Assessments** for new systems/initiatives which process personal data and integrate privacy by design

- **Changes to responsibilities of data processors**
Bigger than the Records Management Unit
Getting Started GDPR in the Oireachtas

- Briefing to Secretary General
- Support from Senior Management
- Awareness raising to ensure business units know what to expect
"Before you go any further, let me reiterate that I, for one, see nothing wrong with killing the messenger."
Cross Functional GDPR Working Group

- **ICT** – Security and new systems
- **Procurement** – Contracts /SLAs
- **RMU** – Records management & Retention
- **Legal** – legal requirements, policies and guidance with DPO, legal research (L&RS)
- **DPO** – Coordination and roll out
- **HR and Members Services** – manage personal data
Audit

Identify all categories of data processed across the Houses of the Oireachtas Service

- Excel form with 6 columns
- Is the processing lawful?
- List categories of data
- Drop down menus – Purposes for processing
- Articles 6 & 9 e.g. Consent, Legal obligation
- Additional information, copies of forms
Next steps

- Review lawfulness of processing returns
- Application for DPIA
- Review contracts, notices and policies
- Working Group – circulate data inventory templates and guidance
- Continue to raise awareness
- Compile Data Inventories
- Circulate DPIA template
Next Steps - Data Inventory

• **WHY** Description of why the personal data is being held/processed—what is the purpose you are holding it for

• **WHO** Whose personal data

• **WHAT** Categories of personal data and the legal basis for processing, set out where it came from

• **WHEN** Retention, when obtained, when updated/erased

• **WHERE** Where is it held, who receives it, transfers, Security
### Example of a personal data inventory

<table>
<thead>
<tr>
<th><strong>Type</strong></th>
<th><strong>Source</strong></th>
<th><strong>Legal basis</strong></th>
<th><strong>WHEN</strong></th>
<th><strong>WHERE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Individual</td>
<td>Contract</td>
<td>Originally</td>
<td>Staff records retained for 6 yrs after termination unless ongoing litigation</td>
</tr>
<tr>
<td>Address</td>
<td>Individual</td>
<td>Contract</td>
<td>Updated</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Contact details</td>
<td>Individual</td>
<td>Third party</td>
<td>Retention period</td>
<td>Manual records - HR department/leadsheet held on closed server located IOM</td>
</tr>
<tr>
<td>Health details</td>
<td>Individual</td>
<td>Third party</td>
<td></td>
<td>CRB Code of Practice</td>
</tr>
<tr>
<td>CV</td>
<td>Individual</td>
<td>Third party</td>
<td></td>
<td>CRB Code of Practice</td>
</tr>
<tr>
<td>References</td>
<td>Individual</td>
<td>Third party</td>
<td></td>
<td>CRB Code of Practice</td>
</tr>
<tr>
<td>CRB check</td>
<td>Individual</td>
<td>Third party</td>
<td></td>
<td>CRB Code of Practice</td>
</tr>
<tr>
<td>Passport details</td>
<td>Individual</td>
<td>Third party</td>
<td></td>
<td>CRB Code of Practice</td>
</tr>
<tr>
<td>Work permit</td>
<td>Individual</td>
<td>Third party</td>
<td></td>
<td>CRB Code of Practice</td>
</tr>
<tr>
<td>Appraisals</td>
<td>Individual</td>
<td>Legitimate interests - staff management</td>
<td>As required</td>
<td>Staff records retained for 6 yrs after termination unless ongoing litigation</td>
</tr>
<tr>
<td>Annual leave</td>
<td>Individual</td>
<td>Legitimate interests - staff management</td>
<td>Regularly</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Disciplinary</td>
<td>Individual</td>
<td>Legitimate interests - staff management</td>
<td>As required</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Tax/NI</td>
<td>Individual</td>
<td>Contract</td>
<td>As required</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Bank account</td>
<td>Individual</td>
<td>Contract</td>
<td>As required</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Pension details</td>
<td>Individual</td>
<td>Contract</td>
<td>As required</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Name</td>
<td>Third party</td>
<td>Vital interests</td>
<td>As required</td>
<td>Employment/limitation law</td>
</tr>
<tr>
<td>Contact details</td>
<td>Third party</td>
<td>Vital interests</td>
<td>As required</td>
<td>Employment/limitation law</td>
</tr>
</tbody>
</table>

**STAFF ADMIN**

**DIRECT MARKETING**

**Existing Customers**

- Name: Individual
- Address: Individual
- Email: Consent of individual
- Mobile: First contact
- Phone: Data Protection Act

**Former Customers**

- Name: Individual
- Address: Individual
- Email: Consent of individual
- Mobile: First contact
- Phone: Data Protection Act

**Potential Customers**

- Name: Third party
- Email: Consent of individual
- Mobile/internet: Not sure - Find Out
- Phone: Data Protection Act

**Isle of Man Information Commissioner – GDPR Toolkit Part 1, V1.1, May 2019**

**Page 17 of 17**
Case study 9 of 2006: An Garda Síochána: Failure respond to an access request on time

Finally, I considered that the Gardaí should develop a clear policy on data retention and apply for the necessary authorisation to dispose of records that are no longer necessary for operational Garda purposes.

Case study 11 of 2011: PAS Access request for old records

We took this opportunity, given the complaint and the issues highlighted by it, to advise the PAS to re-examine its policies in relation to the retention of personal data for longer than was necessary for the purpose/s for which it was obtained. The PAS informed us that it had a Records Retention Policy in place, in accordance with data protection requirements, which sets out the timeframes for the retention and destruction of records. Records such as those that had been examined by my Office on foot of this complaint have a retention period of three years after the determining of the candidate as suitable, or otherwise, for appointment, but in this instance records had been retained by the PAS for over 30 years.

As this case shows, data controllers not only need to have a retention policy in relation to the keeping of personal data, but they must also have an effective mechanism in place to implement that policy. Once an access request is received by a data controller, they must provide the requester with all personal data sought, irrespective of the age of the records, once the data is still in existence. A data retention policy is a vital aspect of good data protection practice in any organisation and is a critical tool in ensuring compliance with the law.
GDPR - An opportunity for the Records Management Unit

2. Disposal

The disposal of an electronic record means its deletion from the shared drive.

**Steps for Disposal**

1. **Prepare**
   - Create a deletion folder in the shared drive.

2. **Match**
   - Match the File Plan folder structure in to the new deletion folder.

3. **Move**
   - Move records for destruction to the deletion folder.

4. **Screen-Grab**
   - Take a screenshot of the records.

5. **Paste**
   - Paste the screenshot into the Records Management Unit (RM Unit) Disposal Form.

6. **Sign**
   - Sign the Disposal Form by your Principal Officer.

7. **Keep**
   - Keep a scanned copy of the Disposal Form in the File Plan in the shared drive.

8. **Copy**
   - Provide a scanned copy to the RM unit.

---

1. Retention

This infographic provides guidance on how to appropriately (1) retain and (2) dispose of electronic records.

**Steps for Retention**

1. **Prepare**
   - Save the appropriate folder in the File Plan and Retention Schedule.

2. **Match**
   - Keep your records by signing the Retention Schedule.

3. **Move**
   - Destroy your records (follow the steps in section 2).

**What is a record?**

A record is any type of record created, sent, received, and maintained by you in the course of your work, which provides evidence of business activities. Records are a vital business resource of the organisation, providing evidence of what you have done or made.

**What is the File Plan and Retention Schedule?**

The File Plan and Retention Schedule provides guidelines on what to keep, what to destroy, and when.

The Records Management Unit (RMU) is the primary user of electronic records. Electronic records are stored in the Record Management Unit (RMU) in accordance with the Records Management Schedule.

The Records Management Unit is responsible for managing records to ensure that records are appropriately disposed of. Check the Records Management Schedule for guidance on electronic records that should be retained or destroyed.
GDPR and Records

**Access**
Article 15 - Quicker response needed for SARS under GDPR

**Security**
Article 32 - Reduce risk of compromising the availability, authenticity, integrity and confidentiality of stored data

**Retention**
Article 30 - set out how long records will be kept
Article 13(2)(a) / Article 15(1)(d) - Notify data subjects

**Accountability Principle**
Article 5(2) and Article 30(1)(f) - Keep records of processing activities
An opportunity for Records Managers

- **Staffing** – DPO requirement (Article 37)
- **Management** - Need for records to be managed properly throughout their life cycles – Security, Access, Retention, Disposition
- **Risk Mitigation** – Comprehensive procedures, prevent storage risks, insecure disposal, indefinite retention

The EU General Data Protection Regulation has put records management back on the business agenda

Records management is once again back on the business agenda, driven by the new European Union General Data Protection Regulation (GDPR), which comes into effect in under two years from now. Through the GDPR, the European Commission intends to strengthen and unify data protection for individuals within the EU. This new directive represents a substantial leap in
Thank you
GDPR Risk and Readiness
Craig Dade, Information Management Services
Crown Records Management
Craig Dade
BDM of Information Management Services
Crown Worldwide
Wednesday, 22 November 2017

The power of memory
Who is Crown?
World Mobility
Relocations
Fine Art
Records Management
Workplace Relocation
Wine Cellars

Privately held company
Established in 1965

- 56 Languages
- 54 Countries
- 266 Facilities
- 56 Nationalities
- 4,926 Employees
- $721m Revenue
- Owned properties $634m
- 10,000 Clients
- Clients over 883,000 m²

The power of memory

CROWN
RECORDS MANAGEMENT
A refreshing outlook on records management

Document Storage and Management
Complete confidence with immediate accessibility

Long-term Digital Preservation
Ensuring your digital assets are accessible and protected

Information Governance Services
Maximise the value of your information

Information Audit
Know where your information is

Information Consulting Services
Protecting and using data more effectively

Media Management
Reliable media storage to reduce risk

Active File Management
Make your paper documents work harder

Scanning
Unlock your information

Secure Destruction
Effective secure shredding solutions
It's going to have a... BIG IMPACT ON EVERY BUSINESS..
Phase 1
Data Protection Risk profile
High Level Risk Profile of Organisation

• Based upon following captured during assessment exercise
  • Type of Personal Data Processed
  • Volume of Personal Data Processed
  • Size of organisation
  • Complexity of data processing and supporting systems
  • Complexity of organisation
## Risk Assessment Table

<table>
<thead>
<tr>
<th>Ratings</th>
<th>Volumes</th>
<th>Zero</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of data subjects</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Volume of data collected</td>
<td></td>
<td>Zero</td>
<td>Limited</td>
<td>General</td>
<td>Extensive</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Core Data</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Organisational Data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Size of Company</td>
<td></td>
<td>Small</td>
<td>Medium</td>
<td>Large</td>
<td>X Large</td>
</tr>
<tr>
<td>Complexity</td>
<td></td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Complexity of Processes</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Complexity of Systems</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Complexity of Locations</td>
<td></td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>Physical Data</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Data</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Comparative Risk Assessment

Organisation Risk

Data Risk

Process Risk

Company X

[CELLRANGE]
Phase 2
GDPR Readiness

The power of memory
## GDPR - 12 Key Principles and 31 Sub-principles

<table>
<thead>
<tr>
<th>#</th>
<th>PRINCIPLE</th>
<th>ASPECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Awareness</td>
<td>Change in the Law</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accountability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Management Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Staff Training and Corporate Culture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Privacy Program</td>
</tr>
<tr>
<td>2</td>
<td>Information Held</td>
<td>Information Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process mapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third parties transfers, including</td>
</tr>
<tr>
<td></td>
<td></td>
<td>overseas</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contracts</td>
</tr>
<tr>
<td>3</td>
<td>Data Quality</td>
<td>Accuracy and Completeness</td>
</tr>
<tr>
<td>4</td>
<td>Individuals Rights</td>
<td>Privacy Notices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subject Access Requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rectification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Erasure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Restrict Processing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Portability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Objections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automated Decision Making and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Profiling</td>
</tr>
<tr>
<td>5</td>
<td>Legal Basis for</td>
<td>Nature of Personal Data established</td>
</tr>
<tr>
<td></td>
<td>processing Personal</td>
<td>and minimisation</td>
</tr>
<tr>
<td></td>
<td>Data</td>
<td>Reason for processing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pseudonymisation and Anonymization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disposition</td>
</tr>
<tr>
<td>6</td>
<td>Consent</td>
<td>Consent</td>
</tr>
<tr>
<td>7</td>
<td>Children</td>
<td>Consent for Children</td>
</tr>
<tr>
<td>8</td>
<td>Data Breaches</td>
<td>Incident Response Plan (IRP)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including Breach notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>procedure</td>
</tr>
<tr>
<td>9</td>
<td>Data Protection</td>
<td>Data Protection Impact Assessment</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td>(DPIA) and Privacy Impact Assessment</td>
</tr>
<tr>
<td></td>
<td>Assessments (DPIA)</td>
<td>(DPIA) and Privacy Impact Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(PIA)</td>
</tr>
<tr>
<td>10</td>
<td>Data Protection</td>
<td>Data Protection Officers (DPO)</td>
</tr>
<tr>
<td></td>
<td>Officers</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>International</td>
<td>International</td>
</tr>
<tr>
<td>12</td>
<td>Privacy by Design</td>
<td>Data Protection by Design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security of Personal Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption</td>
</tr>
<tr>
<td>#</td>
<td>PRINCIPLE</td>
<td>ASPECT</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Awareness</td>
<td>Change in the Law</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
<td>Has a C-level Executive been made responsible for Data Protection?</td>
</tr>
<tr>
<td></td>
<td>Senior Management Support</td>
<td>Are your senior management supportive of the GDPR initiative?</td>
</tr>
<tr>
<td></td>
<td>Staff Training and</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Corporate Culture</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Privacy Program</td>
<td>Does your organisation have a Privacy Program in place?</td>
</tr>
<tr>
<td>2</td>
<td>Information Held</td>
<td>Information Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process mapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Third parties transfers,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including overseas</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contracts</td>
</tr>
<tr>
<td>3</td>
<td>Data Quality</td>
<td>Accuracy and Completeness</td>
</tr>
<tr>
<td>4</td>
<td>Individuals Rights</td>
<td>Privacy Notices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subject Access Requests</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rectification</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Erasure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Restrict Processing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data Portability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Objections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Automated Decision Making and Profiling</td>
</tr>
<tr>
<td>#</td>
<td>PRINCIPLE</td>
<td>ASPECT</td>
</tr>
<tr>
<td>---</td>
<td>-----------</td>
<td>--------</td>
</tr>
<tr>
<td>5</td>
<td>Legal Basis for processing Personal Data</td>
<td>Nature of Personal Data established and minimisation</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>Reason for processing</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Pseudonymisation and Anonymization</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>Disposition</td>
</tr>
<tr>
<td>6</td>
<td>Consent</td>
<td>Consent</td>
</tr>
<tr>
<td>7</td>
<td>Children</td>
<td>Consent for Children</td>
</tr>
<tr>
<td>8</td>
<td>Data Breaches</td>
<td>Incident Response Plan (IRP) including Breach notification procedure</td>
</tr>
<tr>
<td>9</td>
<td>Data Protection Impact Assessments (DPIA) and Privacy Impact Assessments (PIA)</td>
<td>Data Protection Impact Assessment (DPIA) and Privacy Impact Assessment (PIA)</td>
</tr>
<tr>
<td>10</td>
<td>Data Protection Officers</td>
<td>Data Protection Officers (DPO)</td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>International</td>
<td>International</td>
</tr>
<tr>
<td>12</td>
<td>Privacy by Design</td>
<td>Data Protection by Design</td>
</tr>
<tr>
<td>12</td>
<td>Security of Personal Data</td>
<td>Security of Personal Data</td>
</tr>
<tr>
<td>12</td>
<td>Encryption</td>
<td>Is Personal Data data encrypted?</td>
</tr>
</tbody>
</table>
## Assessment and Target

<table>
<thead>
<tr>
<th>Principle</th>
<th>Element</th>
<th>Current Level</th>
<th>Minimum State Phase 1</th>
<th>Desired State May 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Awareness</strong></td>
<td>Change in the Law</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Accountability</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Senior Management Support</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Staff Training and Corporate Culture</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Privacy Program</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Information Held</strong></td>
<td>Information Audit</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Process mapping</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Third parties transfers, including overseas</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Contracts</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Data Quality</strong></td>
<td>Accuracy and Completeness</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Individuals Rights</strong></td>
<td>Privacy Notices</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Subject Access Requests</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Rectification</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Erasure</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Restrict Processing</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Data Portability</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Objections</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Automated Decision Making and Profiling</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Legal Basis for processing personal data</strong></td>
<td>Nature of Personal Data established and minimisation</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Reason for processing</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Pseudonymisation and Anonymization</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Disposition</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Consent</strong></td>
<td>Consent</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td><strong>Children</strong></td>
<td>Consent for Children</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Data Breaches</strong></td>
<td>Incident Response Plan (IRP) including Breach notification procedure</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td><strong>Data Protection Impact Assessments (DPIA) and Privacy Impact Assessments (PIA)</strong></td>
<td>Data Protection Impact Assessment (DPIA) and Privacy Impact Assessment (PIA)</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Data Protection Officers</strong></td>
<td>Data Protection Officers (DPO)</td>
<td>0</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>International</strong></td>
<td>International</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td><strong>Privacy by Design</strong></td>
<td>Data Protection by Design</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Security of Personal Data</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Encryption</td>
<td>2</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>
## Action Plan

<table>
<thead>
<tr>
<th>#</th>
<th>PRINCIPLE</th>
<th>ASPECT</th>
<th>Current level</th>
<th>Phase 1 target</th>
<th>May 2018 target</th>
<th>Actions for Phase 1</th>
<th>Actions Phase 1 to May 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Information Held</td>
<td>Information Audit</td>
<td>1 2 3</td>
<td></td>
<td></td>
<td>There are two approaches the business could take to complete the information audit. 1. Follow the phased approach outlined in this action plan whereby an audit is completed for key business systems first then for all business systems. 2. Complete a full audit for all business systems at once. It is up to the business to determine what approach they will follow. Complete a comprehensive information audit of all key business systems for all parts of the business. Document what Personal Data is held, where it comes from and who it is shared. Complete a risk assessment for information captured in the audit. Identify high level risks and implement mitigating actions. Create a procedure so that if any changes are made to how Personal Data is stored and whom it shared with, the information audit can be updated.</td>
<td>Complete a comprehensive information audit of all business systems across the entire organisation. Include where Personal Data is stored in paper format. Document what Personal Data is held, where it comes from and who it is shared and capture detailed information about how Personal Data is stored and used. Complete a full risk assessment for all information captured in the audit. Identify all risks and implement mitigating actions. Ensure policies and procedures are in place to ensure Personal Data is stored and processed in line with Data Protection Regulations. Create a policy which states that if Personal Data is found to be inaccurate, the business has to tell any organisations they have shared the information with. Create an audit schedule to regularly update the information. Develop plans so that there is resource available to complete audits within the set timeframes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>#</th>
<th>PRINCIPLE</th>
<th>ASPECT</th>
<th>Current level</th>
<th>Phase 1 target</th>
<th>May 2018 target</th>
<th>Actions for Phase 1</th>
<th>Actions Phase 1 to May 2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Process mapping</td>
<td></td>
<td>1 2 3</td>
<td></td>
<td></td>
<td>There are two approaches the business could take to complete the process mapping. 1. Follow the phased approach outlined in this action plan whereby the process mapping is completed for key business processes first then for all business processes. 2. Complete a full audit for all business processes at once. It is up to the business to determine what approach they will follow. Using the existing process maps in department handbooks to map out and fully document details about the key business processes that use Personal Data. Identify any gaps in the process maps and create or update the information. Create policies and procedures for creating process maps so that information captured is consistent across the organisation. Identify the types of Personal Data used in the processes and categorise them accordingly. Complete a risk assessment for processes involving Personal Data. Identify high level risks and implement mitigating actions. Create a procedure so that if any changes are made to how Personal Data is used in a business process, the information can be updated. Continue to review process maps annually.</td>
<td>Map out and document details about the all business processes that use Personal Data. Identify the types of Personal Data used in the processes and categorise them accordingly. Complete a risk assessment for processes involving Personal Data. Identify all risks and implement mitigating actions. Where sensitive Personal Data is used, implement appropriate technical and organisational methods to protect the information. Create an audit schedule to regularly update the information. Develop plans so that there is resource available to complete audits within the set timeframes.</td>
</tr>
</tbody>
</table>
Example Summary of Findings
Summary

• Consultants from Crown IMS have carried out a Risk and Readiness Assessment of Company X and produced a roadmap to compliance

• Based on the information gathered at the initial assessment workshop on XXXX it is confirmed that Company X:
  • **Does have to meet the GDPR in full** due to the size of the organisation and the type of data being processed
  • **Does have a level of risk** around meeting obligations under the GDPR
  • **Should be able to achieve a high level of compliance** by the time the GDPR comes into effect due to the size and scope of personal data held

• For each of the 31 GDPR sub-principles, a two phase action plan has been created
  • Immediately required activity and activity required before the regulation comes into force
  • Actions have been limited in those areas where the impact and risk level of the GDPR is relatively low
Company X Action Plan Summary

- Awareness
  - Finalise then execute Action Plan
  - Develop and implement a Privacy Program

- Information Held
  - Information Audit
  - Process Mapping
  - Document Data Flows
  - Contract Review

- Data Quality
  - No Actions

- Individuals’ Rights
  - Policies and Procedures for Individual Rights

- Legal Basis for Processing
  - Establish nature and ensure minimisation
  - Identify and document legal basis
  - Retention Schedule and Disposition Policy

- Consent
  - Policies and Procedures

- Children
  - No actions

- Data Breaches
  - Policy review and update
  - Reporting and notification criteria

- Impact Assessments
  - Develop Policies and Procedures
  - Develop PIAs based on risk areas identified

- DPO
  - Determine if requirement applicable

- International
  - No initial actions

- Privacy by Design
  - Confirm Policies and Procedures
  - Develop and maintain technical privacy infrastructure
Summary of Initial Activity

• **Update Company X action plan**
  - Initial Crown IMS work has produced a action plan which can be used as a baseline plan for future activity

• **As a priority, carry out a detailed audit** to identify personal data in use across the business - a key part of GDPR compliance is documenting:
  - Types of personal data and where it is located
  - Commercial reason for holding or using the data and the legal basis for processing
  - Limitations on use of the data and evidence of consent and transparency
  - Movement and transfer of data
  - Security of systems

• **Carry out a risk assessment** to identify what is required in terms of technology and organisational measures to ensure compliance
Data Protection Audit

• A Data Protection Audit involves a business engagement to perform a deep dive on the areas as covered in the initial two hour review but at a much more detailed level, specifically:

  • Types of personal data – by category, volume of personal data, scale of subjects and type of data used in processing, where it comes from and how it is collected, purpose it is collected, legal basis for processing, other purpose it is used for, limitation of use

  • Access to data and systems - how data and information is kept up to date and accurate, security of data, consent of data subjects, notice / information provided to data subjects

  • Additional areas - third party transfers, cross border transfers, disposition or retention, ability to meet Subject Access Requests and other data subject rights, how new processes are implemented (Privacy By Design)

• System owners are engaged to allow us to understand where the data is stored, what technical controls are in place and how GDPR requirements are (or could be) met

• Key deliverable will be a “Personal Data Map and Flow” with a risk rating assigned to all components – providing Company X with a detailed understanding of all major risks surrounding the processing of personal data
Full Data Audit

• A Full Data Audit is broader than a Data Protection Audit in that **all information types are tracked** not just personal data.
  • The **business engagement** will focus on information types, location of data and paper business records, information owners, volumes of data, retention and disposition, current and future access requirements, systems used
  • A **risk rating** would be applied to all data using a “harm matrix” to assess the impact on the business in the event of compromised CIA (confidentiality, integrity, availability) of the data
  • The analysis will identify broader risks such as those around data use and efficiency as opposed to specific issues around data protection compliance

• **System owners** would be engaged to understand where data is stored, how systems are integrated or linked and how they manage security, access controls and deletion

• **File analytics tools** will be used to assess levels of data duplication and ROT (redundant, outdated and trivial) data

• **Deliverables** will be a fully documented information environment, data map and risk assessment
Sample Post-Audit Activity

• Commence a **review of privacy notices** to understand how they may have to change

• Look at what **data portability** might require as this is an individual right that will definitely need to be met by Company X and will need to be documented

• Undertake a **contract review with all suppliers** to understand the current level of data protection provision within supplier contracts
  • Once data movement and transfer has been documented, it will then be possible to identify which ones will need to be updated and with what clauses - general data protection or specific clauses relating to what is being processed and any limitations

• A more complicated **technical database mapping exercise** will also need to be carried out which may include documenting the data fields held in each structured system
  • There are limited core systems of this type at Company X
Sample Technology Solutions

• Completion of “Discovery Phase” activities will allow Company X to finalise a costed programme of remedial and improvement work and associated technology that will be required for GDPR compliance.

• Following the detailed audit and risk assessment, technology options could include:
  • Creation of a secure content repository
  • File analytics to discover dark data and analyse content
  • Scanners and document capture sub-systems
  • Implementation of a document and records management system to manage work product and ongoing retention and disposition
  • Policy management system
  • Contract management system
  • Consent management system
  • Encryption and / or pseudonymisation
  • Security incident and event management (SIEM)
Benefits

• Opportunity to drive organisational change, taking the lead in your business area
• Effective privacy management provides assurance to clients and staff alike
• Better trained, knowledgeable staff can help deliver an improved service, retaining and increasing customer base
• Achievement of compliance means there should less to lose and harder to access data in the event of a breach
• Potential cost benefit through reduced storage, selection of appropriate suppliers and better contract management
• Competitive advantage when tendering for business
• Readiness assessment is first step in compliance with Article 24(1) (evidencing that processing is carried out in accordance with the Regulation)
• Mitigation against reputational damage and financial penalties!
For more information about GDPR please visit www.crownrms.com/gdpr

Craig Dade – BDM of Information Management
cdade@crownww.com

+44 (0)20 8443 6016
sales.uk@crownrms.com
Data Protection Audits: A presentation on the 2017 ICO Audit of NI Health Care Trusts

Claire Graham, Head of Information Governance
Southern Healthcare Trust
Background – Data Protection compliance in the Health Sector

• ICO (regulatory body in UK) was given new powers to audit NHS for DP compliance in 2015

• Data Protection/IG Training HSC Northern Ireland
  – Compliance with Controls Assurance Standard
  – Data Protection is mandatory for all HSC Trusts. Regional review of content of module
  – Readiness for GDPR implementation

• Findings from NHS (UK) ICO (trends)
Preparation for the Review
April-June 2017

• Initial contact from ICO on background of review
• Draft staff survey questions (36) to Trusts
• Live link to revised survey to be circulated to all staff
• Results of survey to be assessed by ICO & inform scope of review
• Questions based on responses to survey (above) issued to IG Manager/SIRO/Training staff
• On-site visit to Trust
• Interview with named personnel
Preparation for the Review
Communication to staff

• Memo to Directors for cascade
• ‘SIRO says’ reminder of training
• Global email
• Desktop message: guidance and awareness
• Southern i
• Liaison with ICT re provision of live link
• Invitation to SIRO, Training Manager, Assistant Director Informatics, Head of IG and IG Manager
• Provide questions to above personnel
• Arrange visit by ICO auditors - agenda
Scope of the Review

• Management Structure & Accountability
  - Documentation (GDPR)

• Training Programme: mandatory/induction
  – Monitoring & Reporting of DP training
  – Compliance figures
  – Follow up – non attendance (PDP), sanctions
  – Refresher training

View content of training and sample resources
Interview staff
Survey questionnaire (all staff)

• Is training mandatory?
• Is training targeted to roles of staff?
• How soon after recruitment is training taken?
• How often is refresher training undertaken?
• How is training monitored and reported?
• What external scrutiny is in place?
• Are policies up to date?
• Are there sanctions for non compliance?
Questions for IG & Training staff – on site visit

- **Management structure & accountability - evidence**
  - Minutes, reports, policy, strategy, training reports, PDP, assurance to DoH (CAS)
  - Job descriptions, Terms of reference, qualifications of IG staff,

- **Training programme – format - evidence**
  - Face to face – targeted e.g. social work, SIRO & IAO
  - On line – IG e learning module reminders sent by email prior to expiry date
  - Workbooks – leaflets, guidance
  - Other – compliance mini audits rolling programme (internal visits & questionnaire)

- **Access to Training Materials - evidence**
  - Link to mandatory IG e-learning module for HSC staff
  - IG/DPA checklist is included in department training

- **How do you ensure all staff including bank, students, volunteers and temporary are trained?**
  - Student complete social work induction, targeted training for addiction, safeguarding
  - Bank, temporary and volunteer staff complete e-learning before undertaking work

- **Specify any staff groups not covered by training programme and explain why?**
  - Transport staff, porters and domiciliary care staff receive leaflets – lack of access to PCs

- **How is training recorded on individual records? evidence**
  - KSF/PDP, ELD central database, recorded manually at targeted sessions by Head of Service

- **Provide detail of specific DP training for specialised roles and functions - evidence**
  - Personal Data Guardian/IAOs/social workers

- **Provide qualifications of Information Governance Manager who approves content?**
Charts of Survey Findings in Trust

Which methods are used to communicate new and updated IG policies or messages to you? (Please select all that apply)

Free text responses included:
- “e-learning and emails”.
- “Training sessions”.
- “I have never had any communication”.

- Bulletin / Global emails: 74%
- Intranet: 66%
- Team meetings: 78%
- Screensavers: 31%
- Posters / leaflets: 56%
- Email from manager: 33%
- Newsletters: 66%
Chart of Survey Findings in Trust

Have you completed any training covering IG / Data Protection issues?

- Yes: 94%
- No: 3%
- Don't Know: 3%
Chart of Survey Findings in Trust

What would happen if you did not complete IG / DP training on time?

- 87% Reminder sent
- 43% Line manager informed
- 21% HR or L&D informed
- 3% Disciplinary action
- 3% Nothing
- 5% Other
- 3% Other

- “Training department send out reminders”.
- “This would be flagged up by my manager at my PDP meeting”.
- “Line manager is updated at regular supervisory meetings in terms of training to be undertaken”.
- “Part of appraisal so would be addressed appropriately then”.

Do you have sufficient time to complete IG training?

- “I make time, usually before my appraisal is due”.
- “Regular workload pressure can prevent data protection training being completed in a timely fashion”.
- “I have to complete this training in my own time often staying after my work day is finished to complete same”.
- “Workload does not allow protected time for training – always completed in own time”.
- “Difficulty finding protected time to complete at work and don’t feel it should be done at home”.

Chart of Survey Findings in Trust

84% Yes
16% No
Recommendations

• Compliance remain below ICO target
• Large number of bank staff are not compliant with their IG training, representing a key risk
• Staff have reported that protected time for training is not always offered
• Need to ensure managers allow staff time to complete training module
Follow Up

• ICO training target of 95% clarified
• Compliance figures therefore remain below the recommended ICO target at % 71%
• Develop Action Plan
Issues raised

• What do you see as a barrier to training?
• What is the follow up processes for staff who do not complete training? Are these effective?
• Are the figures escalated to any group?
• Is there a gap between staff starting work and receiving DP induction?
• What awareness mechanisms of policy and procedures are provided?
LUNCH
12.30-13.30
12.30-13.30  Lunch and networking opportunity

13.30-14.00  GDPR The Journey So Far
  Jenny Lynn, Information Management Unit, Department of Finance (NI)

14.00-14.30  GDPR: What you need to know
  Deirdre Allison & Gillian Acheson, Belfast Health and Social Care Trust

14.30-15.00  Going it alone: GDPR sources for the Practitioner
  Claire Graham, Head of Information Governance, Southern HealthCare Trust

15.00-15.30  News from the IRMS executive/sourcing the training you need to be GDPR-ready
  Fiona Kearney, Secretary IRMS

15.45-16.15  AGM for IRMS members

We are very grateful to our sponsors Crown Records Management
GDPR – The Journey So Far

Jenny Lynn, Information Management Unit, Department of Finance (NI)
GDPR
The Journey So Far

JENNY LYNN
DATA PROTECTION AND RECORDS MANAGEMENT
DEPARTMENT OF FINANCE (NI)
DoF Structure

- Information Management Unit
  - Develop policies and guidance; provide updates for SIRO; communicate via BAIMs

- Business Area Information Managers
  - Local GDPR ‘expert’; support IAOs

- Information Asset Owners
  - Branch implementation; ensure staff compliance

- Senior Information Risk Owner
  - Reports to DB

- Departmental Board
  - Endorse and implement business area compliance
We already have in place:

- DoF Data Protection & Records Management Policies
- Staff Handbooks
- Branch Data Handling Procedures
- Data Breach Management Plan
- Data Incident Register
- Data Sharing Guidance/Register
- Information Asset Register
- e-Learning
- 6 monthly branch compliance checklist exercise
## GDPR implementation in DoF

<table>
<thead>
<tr>
<th>Objective</th>
<th>Action</th>
<th>Responsible Owner</th>
<th>Target Date</th>
<th>RAG Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. To lead GDPR compliance from a senior level (top down approach)</td>
<td>a) Appoint a Data Protection Officer, as required by Article 37 of the GDPR</td>
<td>Permanent Secretary</td>
<td>TBC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b) Inform staff of mandatory requirement to conduct privacy impact assessments (PIAs)</td>
<td>Permanent Secretary</td>
<td>13 June 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>c) Ensure each business area has an effective network of Information Asset Owners (IAOs) in place</td>
<td>DB members</td>
<td>By end Sept 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>d) Ensure IAOs understand and accept their responsibilities under GDPR</td>
<td>DB members</td>
<td>By end Sept 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e) Ensure each business area has a dedicated, proficient Business Area Information Manager (BAIM) in place, suitably resourced to take forward GDPR</td>
<td>DB members</td>
<td>By end Sept 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>f) Put in place a process within business areas to mandate the requirement for (PIAs) in all projects/plans/proposals involving use of personal data</td>
<td>DB members</td>
<td>By end Sept 2017</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>g) Ensure mandatory use of PIAs forms part of internal audit programme</td>
<td>DB members/Head of Internal Audit</td>
<td>By end Dec 2017</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Implementation Plan - Areas of Compliance

- Senior level visibility
- Accountability and privacy by design
- Awareness
- Policies and guidance
- Training
- Holdings of personal data
- Data breach reporting
- IT security
- Sharing personal data
Senior level visibility

- Departmental Board priority
- Strong, effective IAO network in place
- Suitably resourced BAIM for each business area
- Regular GDPR updates to Departmental Board
- Appointment of Data Protection Officer
Accountability

- Tailored business area action plans in place
- Document legal basis for processing
- Mandatory use of data protection impact assessments
- Data minimisation
- Data protection built into business planning process
- Internal audit programme
- Retain evidence
Policies and guidance

- Review of DoF policies and guidance to reflect GDPR requirements
  - Information assets
  - Conducting privacy impact assessments
  - Developing privacy notices
- Review of branch data handling procedures – IAOs
  - Clear
  - Concise
  - Comprehensible
  - Consider your audience
- Regularly circulate to staff
- Keep evidence!
Awareness

- Regular DB updates
- Seminar for IAOs
- Staff Brief articles
- Information Managers’ Forum
- Business area updates – BAIMs
- Staff updates - IAOs
Training

- Review of mandatory training courses
  - Responsible for Information – Cabinet Office
  - Managing Information Effectively
- Roll-out in April/May 2018
- Ensure staff completion - IAOs
- Consider branch specific training – I.
- Data Protection Staff Handbook
Holdings of personal data

- Identify holdings
- Legal basis for processing
- Information asset register
- Communicate via privacy notice
- Conduct a DPIA for any new uses
- DoF Information Asset Register Guidance
Communicating privacy information

- Clearly communicate
  - Our identity
  - How we use personal data
  - Lawful basis for processing
  - Retention period
  - Right to complain
- DoF group taking this forward
- Consult your BAIM
- Developing Privacy Notices - Departmental Guidance
Data protection impact assessments

- Address risks at an early stage
- Became mandatory in DoF in July 2017
- Legislative requirement under GDPR
- Guidance available:
  - Screening exercise
  - Report template
  - Checklist
- Conducting a DPIA – Departmental Guidance
Managing data incidents

- GDPR requirement to notify ICO of certain breaches
- Data breach management plan
- Investigation process
  - Report incidents promptly
  - Containment and recovery
  - Assessment of risks
  - Consider notification
  - Evaluation and response
- Full IAO involvement required
- DoF Data Breach Management Plan
Our Key Messages to Senior Managers

- Be accountable
- Lead by example
- Involve your staff in the process
- Keep evidence
- Know your legal basis
- Adopt a privacy by design approach
- Report data incidents
Thank you!

Jenny Lynn

jenny.lynn@finance-ni.gov.uk

Data Protection & Records Management
Department of Finance (NI)
GDPR – What you need to know

Deirdre Allison, Belfast Health and Social Care Trust
Going it alone: GDPR Sources for the Practitioner

Claire Graham, Southern Healthcare Trust
‘Going it alone’

GDPR sources for the Practitioner
Information Commissioners
UK & Ireland

ICO (UK)
• Preparing for the GDPR (2016) 12 steps to take now
• Overview of the GDPR (2016)
• Blog
• Data Friday
• GDPR: helping you prepare (2017) (ppt by S. Wood Deputy Commissioner)

Data Commissioner (Ireland)
• The GDPR and you. Preparing for 2018(2016) 12 steps
• Awareness and Outreach activities
• Overview with relevant GDPR Articles referenced
International

GDPR Coalition established in Feb 17 to raise awareness, based in **Ireland**, voluntary

• Collaborative, not for profit (multinational - small companies)

• Free of charge to download
  – Infographics
  – Blank templates
  – Comprehensive and colourful

[http://gdprcoalition.ie](http://gdprcoalition.ie)
European Sources

- NHS European Office Briefings (overview of key changes)
- Article 29 DP Working Party – DPIA & DPOs guidance
- European Patients Forum The new regulation on the protection of personal data; What does it mean for patients? www.eu-patient.eu
- EU general Data Protection Regulation (EU-GDPR) Table of contents (easy to read text with hyperlinks) http://www.privacy-regulation.eu
- GDPR Quick access to chapters (all articles of GDPR are linked with suitable recitals) https://gdpr-info.eu
European Commission

- Press releases, questions & answers
- Factsheets Q&A e.g. ‘right to be forgotten’
- Proposals on reform –
  - legislative texts, regulation, directive, report
  - current legal framework – Directive 95/46/EC
  - surveys – Eurobarometer, results by country

European Data Protection Supervisor guidelines on data protection in EU financial services regulation 2014
UK Sources

• Information Governance Alliance (IGA) (excellent)
  www.digital.nhs.uk/iga
  – News (monthly)
  – CEO Briefing Note
  – Webinar EU GDPR 3 Aug16 chair S. Lea

• Dept. for Digital, Culture, Media & Sport (7 Aug 17)
  – A New Data Protection Bill: our planned reforms statement of intent.
  – Annex - Summary of derogations in the DP Bill

– Other sources
  – EU GDPR A compliance Guide (Dec 16) (it governance)
  – Data Flow Mapping & EUGDPR (Sep16) (it governance)
  – 11KBW Data Protection Updates ppts & news
  – UKAuthority virtual debate 30 June17GDPR ..Ready or not (good)
Bulletins Issue 200 Nov 2017 – several articles

PDP Journal

• Bevitt, A Stack (2016) 16(6) 13 preparing for the GDPR – advice for employees
• Fulford, N (2016) 16(6) People, processes, technology – a how to guide to data mapping
• Sayers, S (2017)17(6) GDPR demystifying DPIA
• Flannery, N (Deloitte Ire.) (2017)17 (6) Direct marketing & privacy: striking that balance
• Brennan, D. 17(2) GDPR series: personal data – an expanding concept?
• Clark, J. 17(3) GDPR series: building a compliance programme
• Brimstead, K. 17(3)GDPR series: accountability-blueprint for GDPR compliance
• Fulford, N. 17 (3)GDPR series: the new right to data portability
• Woods, G. 17 (3) The right to be forgotten-a decision from the Irish Circuit Court
Legal Firms & Companies

• AIIM Understanding GDPR readiness in 2017 (key findings of survey) www.aiim.org
• Bird & Bird A guide to the GDPR (2016) detailed
• International Reg. Strategy Group example GDPR ready processor terms www.irsg.co.uk contracts
• White & Case LLP (2016) Unlocking the EU GDPR: a practical handbook - chapters may be downloaded free
Websites

- GDPR coalition  [http://gdprcoalition.ie](http://gdprcoalition.ie)
- JISC UK DP mailing list
- PDP compliance news – [www.pdpcompanies.com](http://www.pdpcompanies.com)
- [www.whatdotheyknow.com](http://www.whatdotheyknow.com) – FOI requests & responses
- [www.Hawktalkamberhawk.typepad.com](http://www.Hawktalkamberhawk.typepad.com) (discussion)
- Information Governance Alliance (IGA)  [www.digital.nhs.uk/iga](http://www.digital.nhs.uk/iga)
Related legislation

• Network & Information Systems Directive 2016/1148 (UK Gov Aug17 consultation) cyber security/risk (high level)

• Digital Economy Act 2017 (UK) personal data definition & ICO notification fees
Sourcing the Training you need to be GDPR-ready/ News from the IRMS Executive

Fiona Kearney, Secretary, IRMS
SOURCING THE TRAINING YOU NEED TO BE GDPR-READY

FIONA KEARNEY – AMIRMS
LOOKING AROUND

- Online Search
- Identify the courses
- Evaluate the training providers
- Is there a recognisable name providing the training
MAKING THE RIGHT CHOICE FOR YOU

- What is the right course for you?
- How to choose?
MAKING MY CHOICE

- Location
- Price
- Delivery
- Tutors
DO I WANT TO BE A DPO?

- I’m not sure!
- We have many transferrable skills
- The job market
OTHER RESOURCES

- Data Protection Commissioner Website
- gdprandyou.ie
- ICO
- Data Protection professionals on social media
- International Association of Privacy Professionals
- Digital Rights Ireland
- GDPR Awareness Coalition
THANK YOU

@ fionabkearney

Fiona Kearney
IRMS Update

• Membership Survey – reply by 22 December

• Membership review being conducted

• Creating a content group being led by Emily Overton, Vice-Chair

• Focused editions for the Bulletin in 2018 – GDPR March edition

• 2018 renewals process has been launched
Conference 2018

• Back to the future – last year in Hilton Brighton

• Keynotes – Elizabeth Denham, John Sheridan, Joel Westphal

• Early bird rate until 31/12/17

• Themes Privacy & GDPR, soft skills, technological innovation, leveraging & information value, deployment of solutions
IRMS Member Benefits

- Group events
- Accreditation
- Recognition in our annual awards
- Bulletin & newsletter
- On-line content
- Training discounts
- Conference discounts
- Networking with peers
- Contribution to development in the sector – standards & legislation
IRMS Ireland Group

- Hold events 3 times a year
- Both north & south
- Joint event with ARA, Ireland
- Leading the profession in Ireland, get involved
- Experts in our field
Join IRMS

• Individual £80

• Corporate £350

• Associate £40

• Student - free
Thank you
15.45-16.15
AGM for IRMS members

Meeting afterwards in
The Cellar Bar, Merrion Hotel