The EU GDPR

What Is It & Why Should I Care?

Brian Honan
“Why do you rob banks?”

“Because that's where the money is.”

Willie Sutton
“Why do you hack companies?”

“Because that's where the Data is.”

CyberWillie Sutton
What is GDPR?

- The EU General Data Protection Regulation (GDPR) is the update to the EU Data Protection Directive
- Came into Force 24th May 2016
- Will Apply Across All 28 EU Member States

25th May 2018
What is GDPR?

- Updates the EU Data Protection Directive with a Strong Focus on Individual’s Privacy Rights
- Harmonises the Data Protection Regime Across All 28 EU Member States
- Significant (and Fines) Obligations on Organisations Holding Personal Data
What is GDPR?

- Personal Data

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;’
EU GDPR Applies to EU Member States

Also part of the EU (not shown):
--Canary Islands (Spain)
--Madeira (Portugal)
--Azores (Portugal)
--Many (but not all) French overseas territories

EUROPEAN UNION
- Current member
- Official candidate
- Recognized as a potential candidate

(As of June 2016)
EU GDPR Also Applies Globally
What it Means to The Individual

- Stricter rules for obtaining consent as a legal basis for processing. Consent can be withdrawn at any time.
- Right to clear information relating to the scope, purpose and retention of personal data.
- Right to rectify inaccurate data.
- Subject access requests - right to obtain a copy of their personal data.
- Right to be forgotten and have personal data erased.
- Data portability – right to move personal data to another provider.
- Automated processing – right not to be subject to an automated decision.
- Right to make a compensation claim for damages suffered.
What it Means to Organisations?

- **Conduct a privacy risk assessment of how all personal data is collected, used, stored, and accessed throughout the organisation.**
- **Demonstrate accountability and compliance to the GDPR by maintaining documentary evidence of all data processing activities.**
- **Where personal data is transferred outside of the EU? You must demonstrate the adequacy of the safeguards in place.**
- **A full audit of supply chain is required. Verify that adequate data protection safeguards are in place with suppliers who process personal data.**
- **Data Security - keep personal data secure through appropriate technical and organisational measures.**
- **Data Breaches – report data breaches to the regulator within 72 hours.**
- **Consider the data protection role within the organisation.**
- **Demonstrate that privacy by design is built into technical solutions and organisational practices.**
What it Means to Organisations?

- Fines of up to €20 million or 4% of global turnover
- Compensation claims for damages suffered
- Possible prison sentences for deliberately breaching the GDPR
- Reputational damage to The Irish Times brand and loss of consumer trust
Mandatory Breach Notifications

- If Personal Data Breach
  
  “likely to result in a risk to the rights and freedoms of individuals”

- Notify The Supervisory Authority Within **72 Hours** of Becoming Aware of Breach

- If High Risk Breach Likely To Affect Rights and Freedoms of Individuals
  
  “You Must Notify Those Concerned Directly”
Mandatory Breach Notifications

➢ The Nature of the Personal Data Breach Including:
  ➢ Categories and Approximate Number of Individuals Impacted;
  ➢ Categories and Approximate Number of Personal Data Records Concerned;
➢ Contact Details of the Data Protection Officer or Other Contact Point;
➢ Description of Likely consequences of the Personal Data Breach;
➢ Description of Measures Taken, or Will be Taken to;
  ➢ Deal with the Breach
  ➢ Measures (if appropriate) Taken to Mitigate any Possible Adverse Effects.
Appoint A Data Protection Officer

- Mandatory For
  - A Public Authority (with some exceptions);
  - Companies with;
    - Large Scale Systematic Monitoring of Individuals,
    - Large Scale Processing of Special Categories of Data
    - Large Scale Processing of Data Relating to Criminal Convictions and Offence

- Data Protection Officer Must
  - Report to the Highest Management Level of Organisation
  - Operates independently
  - Is not Dismissed or Penalised for Performing their Task.
  - Have Adequate Resources are Provided
Significant Fines

- Supervisory Authority Can Fine;
  - Up to €20,000,000 (or 4% of total annual global turnover, whichever is greater) for the most serious infringements
  - Failing to notify a breach when required to do so can result in a significant fine up to 10 million Euros or 2 per cent of your global turnover
    - On Top of Fine for the Breach itself

- An Individual(s) Can
  - Complain to Supervisory Authority
  - Right To Compensation
  - Potential for Group Actions
Identify Key Data Assets
Risk Management Strategies:
- Avoid
- Reduce
- Transfer
Establish Policies
Security Awareness Training
Monitor & Respond
Use Existing Frameworks

- ISO/IEC/27002:2013 Guidance
- Not all controls for GDPR in ISO 27001
  - Subject Access Requests
  - The Right to be Forgotten
  - Data Portability
- But can be included in your ISMS
ISO 27001 ROADSHOW // INFOSEC VS GDPR

4TH OCTOBER - 16TH NOVEMBER 2017