The GDPR and NIS Directive: Risk-based security measures and incident notification requirements

Adrian Ross LLB (Hons), MBA
GRC Consultant
IT Governance Ltd
4 May 2017
Introduction

- Adrian Ross
- GRC consultant
  - Infrastructure services
  - Business process re-engineering
  - Business intelligence
  - Business architecture
  - Intellectual property
  - Legal compliance
  - Data protection and information security
  - Enterprise risk management
IT Governance Ltd: GRC one-stop shop

IT governance, risk and compliance

Cyber resilience
- Information security and ISO 27001
- Penetration testing
- Data protection
- Incident response management

Governance and risk management
- IT governance
- Service management
- Project management

Consultancy and certification
- Security testing
- Training and qualifications
- Software tools
- Toolkits and publications

All verticals, all sectors, all organisational sizes
Agenda

- An overview of the regulatory landscape
- Subject matter, material and territorial scope
- Remedies, liabilities and penalties
- Personal data breaches under the GDPR
- The NIS Directive
- Operators of essential services
- Digital service providers
- GDPR vs NIS Directive
Two main types of legal instrument:

- **Directives**
  - Require individual implementation in each member state
  - Implemented by the creation of national laws approved by the parliaments of each member state
  - Directive on security of network and information systems (Directive (EU) 2016/1148)

- **Regulations**
  - Immediately applicable in each member state
  - Requires no local laws to implement
  - General Data Protection Regulation (Regulation (EU) 2016/679)
The General Data Protection Regulation (GDPR)
Article 99: Entry into force and application

“This Regulation shall be binding in its entirety and directly applicable in all Member States.”

KEY DATES

- On 8 April 2016, the European Council adopted the Regulation.
- On 14 April 2016, the European Parliament adopted the Regulation.
- On 4 May 2016, the official text of the Regulation was published in the EU Official Journal in all the official languages.
- The Regulation entered into force on 24 May 2016, and will apply from 25 May 2018.

Articles 1 – 3: Who, and where?

Natural person = a living individual

- Natural persons have rights associated with:
  - The protection of personal data
  - The protection of the processing personal data
  - The unrestricted movement of personal data within the EU

- In material scope:
  - Personal data that is processed wholly or partly by automated means;
  - Personal data that is part of a filing system, or intended to be.
  - The Regulation applies to controllers and processors in the EU irrespective of where processing takes place.

The GDPR applies to controllers not in the EU.
Remedies and liabilities

- Natural Persons have rights
  - Judicial remedy where their rights have been infringed as a result of the processing of personal data.
    - In the courts of the Member State where the controller or processor has an establishment.
    - In the courts of the Member State where the data subject habitually resides.
  - Any person who has suffered material, or non-material, damage shall have the right to receive compensation from the controller or processor.
  - Controller involved in processing shall be liable for damage caused by processing.
Penalties

Administrative fines

- In each case will be effective, proportionate, and dissuasive
  - taking into account technical and organisational measures implemented;

- €10,000,000 or, in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year.

- €20,000,000 or, in case of an undertaking, 4% total worldwide annual turnover in the preceding financial year.
Data breaches in the UK

January to March 2016 – 448 new cases

- Data breaches by sector
  - Health (184)
  - Local government (43)
  - Education (36)
  - General business (36)
  - Finance, insurance and credit (25)
  - Legal (25)
  - Charitable and voluntary (23)
  - Justice (18)
  - Land or property services (17)
  - Other (41)

Source: UK Information Commissioner’s Office
Key facts about cyber breaches

Number of data breaches detected in 2016

- Overall: 24%
- Among micro firms: 17%
- Among small firms: 33%
- Among medium firms: 51%
- Among large firms: 65%

Median number of breaches per company

- Micro/small: 1
- Medium: 2
- Large: 5

Costs associated with the most disruptive breaches

- Large organisations: Mean - £50k, Highest - £3m
- Small organisations: Mean - £5k, Highest - £100k

IPSOS Mori: 2016 Cyber Security Breaches Survey
## Types of breach occurrence

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any breach or attack</td>
<td></td>
</tr>
<tr>
<td>Single breach or attack that caused most disruption to the business</td>
<td></td>
</tr>
<tr>
<td>Viruses, spyware or malware</td>
<td>54%</td>
</tr>
<tr>
<td>Others impersonating organisation in emails or online</td>
<td>13%</td>
</tr>
<tr>
<td>Denial-of-service attacks</td>
<td>15%</td>
</tr>
<tr>
<td>Access to computers, networks or services without permission (i.e. hacking)</td>
<td>6%</td>
</tr>
<tr>
<td>Money stolen electronically</td>
<td>13%</td>
</tr>
<tr>
<td>Breaches from personally-owned devices</td>
<td>8%</td>
</tr>
<tr>
<td>Personal information stolen</td>
<td>8%</td>
</tr>
<tr>
<td>Breaches from externally-hosted web services</td>
<td>1%</td>
</tr>
<tr>
<td>Unlicensed or stolen software downloaded</td>
<td>8%</td>
</tr>
<tr>
<td>Money stolen via fraud emails or websites</td>
<td>2%</td>
</tr>
<tr>
<td>Software damaged or stolen</td>
<td>5%</td>
</tr>
<tr>
<td>Breaches on social media</td>
<td>3%</td>
</tr>
<tr>
<td>Intellectual property theft</td>
<td>1%</td>
</tr>
</tbody>
</table>

* IPSOS Mori: 2016 Cyber Security Breaches Survey
Article 32: Security of processing

• A requirement for data controllers and data processors to implement a level of security appropriate to the risk, including:
  - pseudonymisation and encryption of personal data
  - ensure the ongoing confidentiality, integrity and availability of systems
  - a process for regularly testing, assessing and evaluating the effectiveness of security measures
  - security measures taken need to comply with the concept of privacy by design
A 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Data processor**
- Notify data controller without delay
- No exemptions
- All data breaches have to be reported
- European Data Protection Board (EDPB) to issue clarification with regard to ‘undue delay’

**Data controller**
- Notify supervisory authority no later than 72 hours
- Unnecessary in certain circumstances
- Description of the nature of the breach
- No requirement to notify if no risk to rights and freedoms of natural persons
- Failure to report within 72 hours requires explanation
Article 34: Personal data breaches

Obligation for data controller to communicate a personal data breach to data subjects

- Communication to the data subject without undue delay if high risk
- Communication in clear, plain language
- Supervisory authority may compel communication with data subject

Exemptions:

- if appropriate technical and organisational measures taken
- if high risk to data subject will not materialise
- if communication with data subject would involve disproportionate effort
Independent supervisory authorities

• Member states must create independent supervisory authorities and resource them appropriately
  - Tasks:
    ◦ Monitor and enforce
    ◦ Communicate
    ◦ Promote awareness
  - Powers:
    ◦ To investigate, correct, advise, enforce

• Leading supervisory authority for multi-state controllers
Cyber security assurance

- GDPR requirement – data controllers must implement “appropriate technical and organisational measures to ensure and to be able to demonstrate that the processing is performed in accordance with this Regulation.”
  - Must include appropriate data protection policies
  - Organisations may use adherence to approved codes of conduct or management system certifications “as an element by which to demonstrate compliance with their obligations”
  - ICO and BSI are both developing new GDPR-focused standards
- ISO 27001 already meets the “appropriate technical and organisational measures” requirement
- BS 10012 developed specifically for the GDPR
  - It provides assurance to the board that data security is being managed in accordance with the regulation
  - It helps manage ALL information assets and all information security within the organisation – protecting against ALL threats
Network and Information Directive (NIS)
“Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with this Directive.”

KEY DATES

- On 6 July 2016, the Directive was adopted by the European Parliament.
- On 19 July 2016, the official text of the Directive was published in the EU Official Journal in all the official languages.

Network and Information Security Directive

2013 Cybersecurity Strategy

• The NIS Directive is the first comprehensive piece of EU legislation relating to the 2013 EU Cybersecurity Strategy.

• Its objective is to achieve a high common level of security of network and information systems across the EU through improved cyber security capabilities at a national level and increased EU-level cooperation.

• Processing of personal data to comply with Directive 95/46/EC
Article 1: Subject matter and Scope

- A high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.
  - Obligations on member states to adopt a national strategy for security of network and information systems
  - Creates a Cooperation Group in order to support and facilitate strategic cooperation and the exchange of information among member states
  - Creates a computer security incident response teams network (‘CSIRTs network’) in order to contribute to the development of trust and confidence between member states
  - Establishes security and notification requirements for operators of essential services and for digital service providers
  - Lays down obligations for member states to designate national competent authorities, single points of contact and CSIRTs with tasks related to the security of network and information systems.
Operators of essential services and digital service providers

- **Operators of essential services**
  - Operators of critical infrastructures in industry sectors such as energy, transport, banking, financial market infrastructure, health, water, and digital infrastructure including Internet exchange points, domain name system service providers etc.
  - Public or private entities set out in Annex II of the Directive.

- **Digital service providers**
  - Any legal person that provides a digital service, such as online marketplaces, online search engines, Cloud computing services, app stores etc.
  - Does not apply to micro and small enterprises.
Article 1: Subject matter and scope

- Directive does not apply to all operators of essential services or DSPs
  - Certain sectors are already sufficiently regulated, or may be in the future
  - If this is the case then the NIS Directive has no application
  - Sector-specific regimes must supply equivalent protection
Article 5: Identification of operators of essential services

- Each country designates which essential services are within the scope of the Directive.
  - Member states shall identify the operators of essential services with an establishment on their territory by 9 November 2018;
    - Set criteria for the identification of the operators of essential services:
      - An entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
      - The provision of that service depends on network and information systems; and
      - An incident would have significant disruptive effects on the provision of that service.
  - List of operators of essential services subject to revision every two years.
Network and Information Security Directive

Recital 57: Directive applies to all digital service providers

- Member state rules apply to establishment of DSPs
  - This follows the approach used by ECJ, case law and the GDPR.
- Recital 65: Directive applies to digital service providers outside the EU that offer services within the EU
  - The use of a language or currency that is generally used in one or more Member State may indicate that DSPs outside the EU are offering services within the EU.
  - DSPs outside the EU that offer services within the EU must designate a representative to act on their behalf, including in relation to incident reporting.
  - Representative contact point for competent authorities and CSIRTs.
Operators of essential services must:

- Take appropriate technical and organisational measures to manage the risks to the security of networks and information systems.
- Take steps to prevent and minimise the impact of incidents with a view to ensuring continuity of services.
- Notify the competent authority or the CSIRT without undue delay of incidents having a significant impact on the continuity of the essential services.
- In order to determine the significance of the impact of an incident, the following shall be taken into account:
  - The number of users affected by the disruption of the essential service
  - The duration of the incident
  - The geographical spread with regard to the area affected by the incident.
Network and Information Security Directive

Article 16: Security requirements and incident notification

- Digital service providers must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems.
  - Including the following elements:
    - the security of systems and facilities
    - incident handling
    - business continuity management
    - monitoring, auditing and testing
    - compliance with international standards.
- The Commission can further specify the elements above but the member state cannot impose any further security or notification requirements on the digital service provider.
- Digital service providers must take steps to prevent and minimise the impact of incidents affecting the security of their network and information systems on the services offered within the Union, with a view to ensuring the continuity of those services.
• Must ensure that Digital service providers must ensure they notify the competent authority or the CSIRT without undue delay of any incident having a substantial impact on the provision of a service within the Union.

• When determining whether the impact of an incident is substantial, the following parameters in particular shall be taken into account:
  - the number of users affected by the incident, in particular users relying on the service for the provision of their own service
  - the duration of the incident
  - the geographical spread with regard to the area affected by the incident
  - the extent of the disruption of the functioning of the service
  - the extent of the impact on economic and societal activities
Intention is to have a high level of harmonisation across the member states.
- Subject to variation by member state through method of adoption.
- In France, many of the requirements are already set out in the Military Planning Act.
- In Germany, the IT Security Act covers many of the requirements of the NIS Directive.
- Other member states like the UK do not currently have detailed cyber security laws.
- Possibility of many different sector-based competent authorities.
- Implementation by the combination of new laws and amendment of existing laws.
- This approach is contrary to harmonisation.
The GDPR

- Intention is the harmonisation of data protection across the member states
- GDPR derogations allow variation between member states
- Mandatory appointment of DPOs in certain circumstances
- Mandatory breach reporting in certain circumstances
- Prior consultation where there is a high risk to data subjects
- Data processors now brought into scope
- Controllers have to demonstrate accountability
- Introduction of administrative fines
IT Governance: GDPR one-stop shop

Self-help materials

A Pocket Guide
www.itgovernance.co.uk/shop/Product/eu-gdpr-a-pocket-guide

Implementation manual
www.itgovernance.co.uk/shop/Product/eu-general-data-protection-regulation-gdpr-an-implementation-and-compliance-guide

Documentation Toolkit
www.itgovernance.co.uk/shop/Product/eu-general-data-protection-regulation-gdpr-documentation-toolkit

Compliance Gap Assessment Tool
www.itgovernance.co.uk/shop/Product/eu-gdpr-compliance-gap-assessment-tool
Training courses

1-Day accredited Foundation course (classroom, online, distance learning)
www.itgovernance.co.uk/shop/Product/certified-eu-general-data-protection-regulation-foundation-gdpr-training-course

4-Day accredited Practitioner course (classroom, online, distance learning)
www.itgovernance.co.uk/shop/Product/certified-eu-general-data-protection-regulation-practitioner-gdpr-training-course

1-Day Data Protection Impact Assessment (DPIA) Workshop (classroom)
www.itgovernance.co.uk/shop/Product/data-protection-impact-assessment-dpia-workshop
Questions?

aross@itgovernance.co.uk
0845 070 1750
http://www.itgovernance.co.uk