General Data Protection Regulation (GDPR)

Presented by
Lorraine Valentine
Regulatory Compliance & Information Security Specialist
CIF/CPAS

Agenda

- What is GDPR?
- What is Personal/Sensitive Data?
- Important Definitions
- Rights of Individuals under GDPR
- Accountability
- Data Breaches under GDPR
- DPC Powers
- Security Measures
- Recommendations
- Summary
- Further Information

What is GDPR?

- **GDPR Effective from 25th May 2018**
- GDPR will replace the current regime in Ireland; Data Protection Acts 1988 and 2003
- Direct effect in all Member States
- All organisations that process EU citizens data
- Applies to all “data controllers” and “data processors”
- Data Protection Bill – 2018
- Regulator in Ireland – Office of the Data Protection Commissioner

What is Personal Data?

- ***Personal data***- defined very broadly and means any information relating to an identified or identifiable natural person
  - Relates to an individual rather than a corporate entity
  - Individual must be living; information about a deceased individual does not constitute personal data of that individual
  - All information processed electronically
  - Manual records intended to be processed electronically
  - Manual records in a "*relevant filing system*"

What is Personal Data?

- Contact Details including work contact details e.g. work e-mail address
- Employee Data
- PPS Numbers
- Financial Data
- Training Records
- Site access cards
- Photographs
- CCTV Images
- Wearable technology
- Health & Safety records

What is Sensitive Personal Data?

- Personal data as to one or more of the matters listed below;
  - The racial or ethnic origin of the data subject
  - Political opinions
  - Religious or philosophical beliefs
  - Trade Union membership
  - Genetic data
  - Biometric data
  - Physical or mental health or condition
  - Sexual Life

Other Important Definitions

- ***Processing***

- Any use to which personal data are put;

  - Obtaining, retrieving, storing, making available to others within or outside the organisation, printing, destroying

- ***Data Subject***

- An individual who is the subject of personal data, including;

  - Employees, past employees, job applicants, customers, prospective customers

Other Important Definitions

- ***Data Controller***
  - The organisation that determines how personal data will be used.

- ***Data Processor***
  - An organisation that processes personal data on behalf of a Data Controller. Data Processor has increased obligations under GDPR.

Rights of Individuals under GDPR

- **Right to be informed –** individuals are aware of the purpose for processing

- **Right of access –** Individuals can request all data held on them
  - Under GDPR – no fee and 30 days to respond with all information

- **Right of rectification and erasure**
  - A data controller must rectify or erase inaccurate data

- **Right to restrict processing**
  - An individual may request a data controller to cease processing personal data relating to him/her where substantial damage or distress is likely to be caused.

Accountability Principle

- Organisations must be able to demonstrate compliance
- No longer required to register with DPC
- What personal data do you hold?
- Where is it stored?
- Who has access to it?
- Legal basis for processing

Data Breaches under GDPR

- Data controllers and data processors are now subject to a notification regime
- Data Controller must report a breach within 72 hours of becoming aware of the breach
- Processor must notify controller of a breach
- Data controller must maintain an internal breach register

Powers of the Data Protection Commissioner

- Fines under GDPR
  - 4% of annual turnover or up to €20 million
  - Adverse Publicity/Brand damage
  - “Name & Shame” - Biggest driver for compliance so far!

- Audit & Seize
- Substantial powers of entry and inspection as well as the seizure of documents
- Direct organisations to cease processing of data

The Security of Personal Data

““..processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’)…” Article 5 (1) (f)

- **Technical measures**
  - Password protection, firewalls, virus protection software, encryption and building security measures
- **Organisational measures**

  - Training staff, lockable cabinets, clean desk/clear screen policy, shredding manual records, IT expertise when destroying electronic media

E-mail Use and Security

- Beware of attachments in unexpected e-mails.
- Be extremely cautious of clicking on links in emails – if you are not expecting the email DO NOT CLICK and verify with sender via phone
- If a suspicious email is received log a call for IT to investigate but don't forward the email.
- Never transfer company data to your own personal e-mail account i.e. Gmail, Yahoo etc.
- Check if the recipient address is correct before sending an email.
- ALWAYS BE SUSPICIOUS OF E-MAIL!

Security Incidents - Real life example

UK Online retailer left customers' financial details vulnerable to cyber attack

An online building products supplier has been fined £55,000 by the Information Commissioner's Office (ICO) after the firm failed to protect its customers' personal information.

Construction Materials Online Ltd (CMO) was unaware its website contained a coding error which left it vulnerable to attack. Attacker accessed 669 unencrypted cardholder details including names, addresses, account numbers and security codes.

An investigation by the ICO discovered the firm did not have the appropriate technical measures in place to prevent the attack.

GDPR Preparation – Recommendations

- Conduct a data audit
- Conduct a data minimisation exercise – are you asking for information that is not required in order to provide the service?
- Staff awareness – Key
- Implementation/update of policies and procedures
- Implement a record retention schedule
- Secure erasure of data that is no longer required
- Privacy notice
- Review and update contracts with data processors
- Privacy by design
- Privacy Impact Assessments

Summary

The Principles of GDPR

1. Obtain and process the information fairly, lawfully and in a transparent manner
2. Obtain data for one or more specified, explicit and lawful purposes and use and disclose it only in ways compatible with these purposes
3. Ensure that it is adequate, relevant and not excessive for the purpose or purposes
4. Keep it accurate, complete and up to date
5. Do not keep data on a “just in case basis”
6. Keep it safe and secure
7. Controller shall be responsible for and be able to demonstrate compliance

Further Information

- **Ireland**
  - www.dataprotection.ie (Data Protection Commissioner)
- **EU**
  - https://ec.europa.eu/info/law/law-topic/data-protection_en (EU GDPR webpage)
  - WP29 Guidance
- **UK**
  - www.ico.org.uk (UK Regulator)