GENERAL DATA PROTECTION REGULATION (GDPR)

Information session for Protocol Committee Thursday 25th September 2017 - 8am.

What is GDPR all about?

- General Data Protection Regulation (EU) 2016/679 ("GDPR")
- Adopted April 2016
- Comes into force **25 May 2018**
  - Emphasises transparency, security and accountability of data controllers.
  - New rights and strengthening of rights for citizens
  - New elements and significant enhancements

SCOPE

- Applies to;
  - the processing of personal data by automated means
  - The processing of personal data which forms part of a filing system
- What is personal data?
  - Means any information relating to an identified or identifiable natural person
  - Greater security requirements for “special categories” of personal data

Reminder about the Current law -

- Legal responsibilities of a Data Controller
- **Must ...**
  - **Obtain** and process the information fairly
  - **Keep** it only for one or more specified and lawful purposes
  - **Process** it only in ways compatible with the purposes for which it was given to you initially
  - Keep it **safe and secure**
  - Keep it **accurate and up-to-date**
  - Ensure that it is **adequate, relevant and not excessive**
  - Retain it **no longer than is necessary** for the specified purpose or purposes
  - **Give a copy of his/her personal data** to any individual, on request.

What's new in GDPR

1. DPO – Data Protection Officer
2. Accountability
   - Record of processing activities
   - Data processing agreements
   - Transparency – privacy statements
   - Privacy Impact Assessments
   - Privacy by design and by default
3. New rights for citizens and new information requirements
4. Greater obligations re security measures
5. Consequences – remedies, liability and penalties
   - Enhanced powers of Data Protection Commissioner
   - Administrative fines / notices / directions
   - Rights of citizens to make complaints
   - Right to damages for citizens
6. New requirements re data access requests
7. New notification requirements re personal data breachs

1. Data Protection Officer

- Mandatory for public authorities – Terence O'Keefe newly appointed
- ***Independent*** answerable to highest management level
- DCC obliged to provide adequate resources to the DPO
- Functions;
  - Inform and advise controller, processers, employees who carry out processing re regulation
  - Monitor compliance with regulation, with controllers DP policies, including assignment of responsibilities, awareness- raising, and training of staff and audits.
  - Provide advice re data protection impact assessment
  - Co-operate and consult with data protection commissioners office
  - Point of contact for DPC and data access requests

2. Accountability

- Privacy by design and by default
- Council must document privacy management
- Council must document processing activities
- Must be able to demonstrate how DCC complies with a host of additional obligations
- How to demonstrate compliance
  - Written policies and procedures for all data management processes and for data breach management
  - Privacy statements and information for data subjects that meet all the GDPR requirements
  - Training and awareness for all frontline staff
  - Third party agreements on data sharing
  - ***Privacy impact assessments***

3. New rights for citizens

- New rights to *information* for citizens when providing their details
  - Identity and contact details of the data controller
  - Contact details of the data protection officer
  - Purposes of the processing
  - Legal basis for processing
  - Any third parties or categories of third parties that will be given the data
  - The period for which the data will be stored
  - Existence of various rights in relation to the data including rights of access erasure and right to lodge a complaint with the Data Protection Commissioner….

New Rights for Citizens - continued

- Rights to transparency
  - Communications must be intelligible and easily accessible, in clear and plain language
- Right of access to personal data
- Right to rectification
- Right to erasure / to be forgotten
- New - Right to restrict of processing
- New - Right to data portability
- New - Right to object.... (direct marketing and profiling)

4. Security Measures

- Must be; - processed in a manner that ensures appropriate security of 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)
- What does processing mean?
  - Means any operation or set of operations which is performed on personal data or sets of personal data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5. Consequences - Remedies liability and penalties

- Enhanced rights for citizens
  - Every data subject has a right to complain to DPC
  - Right to compensation
  - Entitled to judicial remedies

- Enhanced and increased powers for the Data Protection commissioner.
  - Entitled to conduct investigations
  - Issues notices and directions
  - Apply administrative fines Up to €10,000,000 / €20,000,000 2%/4% worldwide turnover
  - Reputational damage to DCC

6. Data Access Requests

- New requirements regarding data access requests
  - Provision of information and communications to data subject – must be concise, transparent and in easily accessible form, clear and plain language
  - Right to obtain from the controller confirmation as to whether or not his or her personal is being processed
  - If it is being processed; - Citizens will have the right to access to that personal data **and** the following information
    - Purposes for which data is held
    - categories of personal data
    - Third parties or categories of third parties receiving
    - Storage period
    - Rights to request restriction, erasure, right to restrict/object to processing
    - Right to lodge a complaint
  - Request must be met - Without "undue delay" in any event within **1 month** . Can extend - 2 months, where *necessary*, must explain!
  - Free of charge!

7. **New** requirement to notify when there is a data breach

- What is 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.
- Must notify the DPC when there is a personal data breach
  - Unless data breach is unlikely to result in a risk to rights
  - without due delay" – within 72 hours.
- Must notify the person themselves in certain circumstances
  - High risk to rights and freedoms.

Lawfulness of processing – Article 6

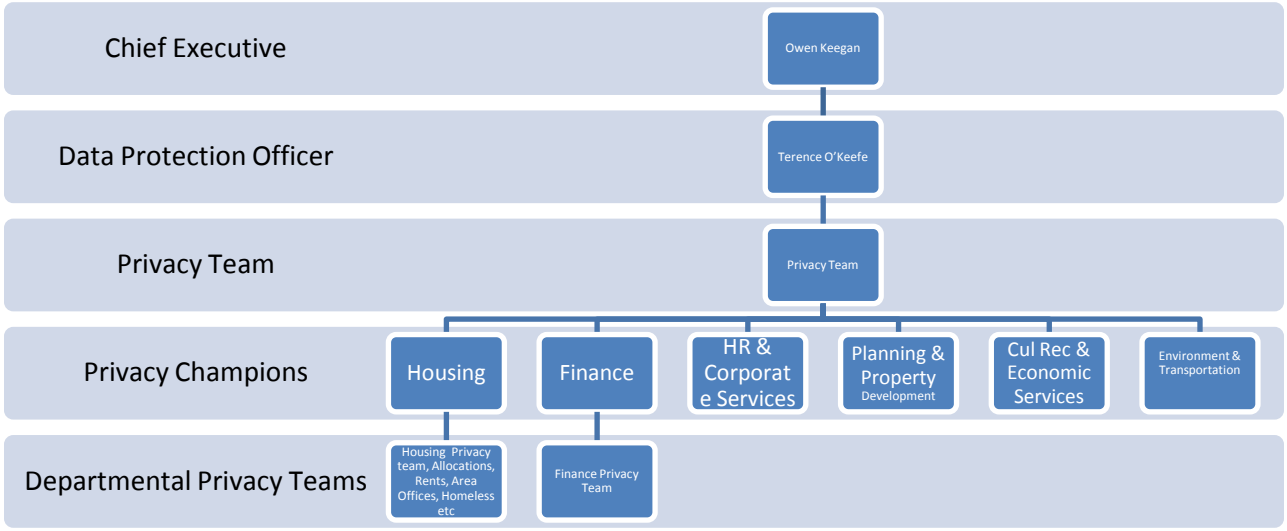
- Only lawful if at least one applies;
  - Consent
  - Contract
  - Legal obligation
  - Necessary to protect vital interest of data subject
  - Necessary for performance of task carried out in the public interest or exercise of official authority (must be a legal basis to rely on this ground)
  - Necessary for purposes of legitimate interest pursued by controller…. (this ground specifically excluded for public authorities)
- Must ensure lawfulness of processing
- Consent **not** a reliable ground where controller is a public authority (Recital 43)

What’s next?

Preparing for GDPR - Executive

- Privacy management teams
- Review and Audit of personal data in the various Departments:
  - Identification and analysis of the collection and processing of data within Departments.
  - Identification of relevant filing systems – list all data sets
  - Map and review of the *data life cycle for each data set.*
    - *Legal basis for holding*
    - *Access – who, what, why*
    - Contracts - Disclosures to third parties
    - Destruction, retention and storage policies
    - Security of data
    - Privacy statements on application forms, websites
- Identify and document the relevant policies and procedures for each data set.
- Governance:
  - DPO and privacy management team
  - Personnel training, awareness training
  - Privacy Impact Assessments
  - Policies and procedures around processing
  - Documentation of processing
  - Data access requests – policies and procedures
  - Data breach procedures
  - Demonstrating Compliance
- Look at third party contracts and data sharing, review all contracts
- Look at all internal housekeeping matters with privacy in mind.

PRIVACY MANAGEMENT STUCTURE



Elected members….

- Issues for consideration…..
  - Privacy management issues
  - Management of data generally
  - Difference between personal data and non-personal data
  - Awareness, awareness, awareness….
- Privacy Impact Assessments
- Liaising with the DPO.

Resources

- Text of the GDPR Regulation -http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf
- Website of the Data Protection Commissioner https://www.dataprotection.ie/docs/GDPR/1623.htm
- EU Guidelines on Data Protection Officers http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

Y C Kelly Assistant Law Agent Dublin City Council yvonne.kelly@dublincity.ie

GDPR Regulation (EU) 2016/679
Nuts and Bolts

- Recitals: 173
- Articles: 1 - 99
- Chapters: 1 – 11
  1. General provisions
  2. Principles
  3. Rights of the Data Subject
  4. Controller and processor
     1. General obligations
     2. Security of personal data
     3. Data protection impact assessment and prior consultation
     4. Data protection officer
     5. Codes of conduct and certification
  5. Transfers of personal data to third countries or international organisations
  6. Independent supervisory authorities
  7. Cooperation and consistency
  8. Remedies and penalties
  9. Provisions relating to specific processing situations
  10. Delegated acts and implementing acts
  11. Final provisions

THANK YOU!

- Yvonne Kelly, Assistant Law Agent, and Audrey O'Hara, Senior Solicitor
- 28th September 2017