Data Protection in UCC

What you need to know:
An introduction to the Rules, Policies & Procedures

Presentation to Tyndall National Institute,
Tuesday 16th May 2017
Catriona O’Sullivan, Information Compliance Officer, UCC
What we’ll cover today

1. What is Data Protection?
2. Who does it apply to?
3. Why is it important?
4. UCC’s Data Protection Policy
   • The Data Protection Rules
5. Personal Data Security Breaches
6. New legislative developments (GDPR)
7. Summary & Conclusion
Data Protection is everywhere!

- Governs the way in which we deal with personal information (data)

- Mechanism for safeguarding privacy rights of individuals in relation to the processing of their personal data

- Overseen by Office of the Data Protection Commissioner (upholds rights / enforces obligations)
What is Data Protection?
Personal Data - Definition

**Personal Data:** data relating to *living, identifiable* individuals

“Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is, or is likely to come into, the possession of the data controller”

- Applies to manual *and* electronic data
- Relates to the “Processing” of personal data...
- **Sensitive Personal Data** defined in the Acts...
Sensitive Personal Data

- Physical or mental health
- Racial origin
- Political opinions
- Religious or other beliefs
- Sexual life
- Criminal convictions
- Alleged commission of offence
- Trade Union membership

**Explicit consent required to process sensitive personal data.**
What is Data Protection?

**RIGHTS**
for individuals
(“data subjects”)

- Fair
- Transparent
- Proportionate

- To fairness when giving information
- To get a copy of their own data
- To have wrong information corrected
- To opt out of direct marketing
- To complain to DPC
- New! Right to be forgotten
- New! Data portability

**RESPONSIBILITIES**
for users of personal data
(i.e. YOU!)

- To comply with the rules of DP
To Whom Does Data Protection Apply?

• **Data Subjects** (e.g. staff, students, research subjects, patients, members of the public)

• **Data Controllers** (e.g. UCC, some research centres/projects)

• **Data Processors*** (those who process data on behalf of data controller)

* Data Processors currently do not have many obligations under the existing law BUT they will have many new responsibilities imposed on them by the new law!
Why is it Important?

- People increasingly aware of their rights – expect organisations to protect their personal data
- Investigations/audits by the Office of Data Protection Commissioner
- Can be forced to release / destroy information
- Data security breaches
- Litigation / Fines
- Negative publicity and loss of “consumer” confidence
Negative Publicity

Three Irish hospitals targeted in cyber attack

‘AN ALARMING DEVELOPMENT’
Thousands of Trinity College donors may have been hacked in €1million money laundering scam

The university’s solicitor wrote to people who contributed to the ‘Trinity Foundation’ to warn them
Negative Publicity

Laptop containing children’s personal details stolen from car of HSE staff member

Data breach investigated after Irish Water discloses bank details
MOBILE phone operators 3G Ireland and Meteor as well retailer Carphone Warehouse have admitted breaking data protection regulations by sending unsolicited text messages and "spam" emails to customers... The companies ...faced the possibility of being fined up to €5,000 per offence.”
UCC’s Data Protection Policy

The 8 Data Protection Rules

1. **Obtain & process** the information fairly (consent)
2. **Keep** it for one or more specified and lawful purposes
3. **Use and disclose** only in ways compatible with these purposes
4. Keep it **safe and secure**
5. Keep it **accurate** and **up-to-date**
6. Ensure that it is **adequate, relevant and not excessive**
7. Retain it **no longer than is necessary** for the purpose(s)
8. **Give a copy of his/her personal data** to any individual on request

Under GDPR, we must be able to demonstrate compliance with these principles!
Data Protection Rule 1

Obtain and Process the Data Fairly

This means:

(1) At the time personal data is being collected from data subjects, they must be informed via a “Data Protection Notice”* of the following:

- who is collecting the data (e.g. UCC School of X)
- the purpose(s) for which data shall be processed
- to whom the data will be disclosed (if anyone)
- if data will be transferred outside the EU
- right of access to personal data... AND......→
Data Protection Rule 1

Obtain and Process the Data Fairly

(2) You must have a legal basis for processing personal data. i.e. you must “Legitimise” the processing by obtaining **consent or** relying on one of a number of other conditions:

- Legal obligation
- Contract with individual
- Necessary to protect vital interests
- Necessary for a public function (Justice)
- Necessary for ‘legitimate interests’ of data controller

- **Explicit consent** in writing must be obtained for sensitive personal information
Data Protection Rule 1 (contd.)

**Obtain and Process the Data Fairly**

Under GDPR, additional info must be communicated to individuals in advance of processing:

- the legal basis you are relying on
- data retention periods
- the right of complaint where unhappy with implementation of these criteria
- whether the data will be subject to automated decision making

**OCLA can assist with drafting of DP Notices if required**

- All websites must have a Privacy & Cookies Statement
Data Protection Rule 2

*Keep personal data only for one or more specified, explicit and lawful purposes*

- Be clear about why you are collecting personal data
- Make sure that data subjects are also clear about the purpose(s) for which you are collecting/holding their data and what they might be contacted about
- Cannot expand purpose without reverting to individual
Data Protection Rule 3

Use and disclose the data only in ways compatible with these purposes

General rule – no disclosure for different purpose

- Ask yourself: would the data subject be surprised to learn that their personal data was being used/disclosed in a particular way?

- In general, personal data should never be shared or disclosed without the data subject’s consent.

- Special attention to be paid to **sensitive** personal data
Data Protection Rule 4

Keep personal data safe and secure

• “Appropriate security measures” (appropriate to the harm that might result and to the nature of the data)
  - May have regard to cost of implementation
  - May have regard to the current state of technology
  - Staff must know and comply with measures
  - Internal review of security measures-part of Internal Audit function

• Extremely important to make sure that all personal data you are responsible for is kept secure and in such a way that it does not permit unauthorised access, intentionally or accidentally.

• Adhere to UCC’s IT policies at all times
Data Protection Rule 5

Keep data accurate, complete and up-to-date

• The longer personal data is held, the more likely it will be inaccurate and out-of-date

• Individuals have the right to have errors rectified

• Staff must ensure that local procedures are in place to ensure high levels of personal data accuracy, including periodic review and audit.
Data Protection Rule 6

Ensure that personal data is adequate, relevant & not excessive

• Must seek and retain only the **minimum** amount of personal data from data subjects which you need to achieve your purpose (which is referred to in the data protection notice)

• Advisable to carry out periodic reviews of data being sought and data already held
Data Protection Rule 7

Retain data for no longer than is necessary

• You must be clear about length of time data will be kept and reason for same. Data should never be kept “just in case”!

  • Decide how long data should be kept for
  
  • Records Management Policy/ Retention Schedules
    (contact University Archivist Catriona Mulcahy (Timmy O’Connor- ex. 2753)

  • SOP re Disposal of redundant personal data

• Under GDPR, we must inform people how long we will keep their data
Data Protection Rule 8

Right of Access

• Individuals are entitled to:
  • A copy of the data you are keeping about him/her
  • Know the identity of those to whom you disclose the data
  • Know the source of the data, unless contrary to public interest
  • Response by the University required within 40 days*
  • All access requests to be directed to Catriona O’Sullivan, Information Compliance Officer

*Under GDPR, this will be reduced to 1 month plus must tell people your data retention periods and the right to have inaccurate data corrected
Additional Rules

• Data Processors
  • Under current law, limited obligations for processors
  • Under new law: many new responsibilities:
    • Statutory obligation to protect personal data by appropriate technical and organisational security measures
    • Statutory obligation to communicate data breaches to data controller’s customers and to cooperate with the controller insofar as it is required to notify DPA/data subject
    • Extensive requirements for data processing/outsourcing agreements (audits, breach notification, security measures, etc).

• If a service is outsourced to an external supplier, and involves personal data:
  • Must adhere to UCC’s Externally Hosted Personal Data Policy
  • Must be a written contract in place (data processor agreement)
Additional Rules

• Transfers outside European Economic Area
  • Special conditions must be met where the country importing the data does not have EU-approved level of DP law
  • ‘Safe harbor’ no longer applicable – need to look at other ways of transferring data abroad (Model Contract Clauses, Privacy Shield, Certifications…)

• Registration* with Data Protection Commissioner if not covered by educational exemption

*requirement to be abolished under the new GDPR
Personal Data Security Breaches

• What is a Personal Data Security Breach?
• What is a Personal Data Security Breach?
  • E.g.
    • Disclosure of confidential data to unauthorised individuals
    • Loss or theft of data or equipment on which data is stored
    • Hacking, viruses or other security attacks on IT equipment / systems / networks
    • Inappropriate access controls allowing unauthorised use of information
    • Emails containing personal data sent in error to wrong recipient / emails sent to mailing list not using the BCC field
  • Applies to paper and electronic records
  • Consequences? – Financial, Reputational, Legal...
• Follow Personal Data Security Breach Management Procedures... (see next slide)
Personal Data Security Breaches

• Breaches managed by Information Compliance Officer with Deputy Corporate Secretary and Director of IT Services/IT Security Officer

• What to do if you discover a breach (or potential breach)?
  • Don’t delay – act immediately!
  • Report incident to your Head of Dept.
  • Head to report incident to Info. Compliance Officer

This enables University to assess, contain and respond to incident (incl. notifying affected parties and DPC).

Under GDPR: mandatory breach notifications:
- to DPC within 72 hours
- to data subjects ‘without undue delay’.
New Legislative Developments

• New EU Data Protection Regulation – 25 May 2018
• Aim: to harmonise the current data protection laws in place across the EU member states.
• Principles (8 rules) largely the same... But several areas strengthened/added:

  - Consent remains very high standard (must be distinguishable from other matters and in clear plain language)
  - Must be as easy to withdraw consent as it is to give it
  - More flexibility on “legitimate interests” as a lawful ground to process personal data in some circumstances, but must inform people if you are relying on this
  - More information must be given to data subjects (how long data will be kept, right to lodge a complaint to ODPC, source of the data...).
New Legislative Developments (contd.)

- “One Stop Shop” (one supervisory authority for organisations who are based in multiple countries)
- Data portability
- “Right to be forgotten”
- “Privacy by Design”
- Privacy Impact Assessments (mandatory in certain circumstances)
- The law will apply to Data Processors as well as Data Controllers (extensive new requirements to be imposed on contracts – good idea to include clauses in contracts now).

• Sanctions/Fines – 2 levels of fines:
  • up to the greater of 2% of annual worldwide turnover of preceding financial year or €10million for matters re internal record keeping, data processor contracts, DP by design and default;
  • Up to the greater of 4% of annual worldwide turnover of preceding financial year or €20million for matters re breaching DP principles, conditions for consent, data subjects’ rights and international data transfers
SUMMARY: Your responsibilities in relation to personal data

Beginning
Getting the Data

- Inform and get consent (DP Notice/Privacy & Cookies Statement)
- Specify purpose
- Only gather what is required
- Register with DPC?
- Data Processor agreement?

Middle
While you have the data

- Justification to process
- Keep accurate
- Respond to access requests
- Disclose only if compatible or allowable exception

End
 Disposing of data

- Have a retention policy
- Keep secure and dispose of securely
Concluding Remarks

• Data protection is a growing issue

• People are aware of their privacy rights and are demanding ever higher standards

• The laws are becoming ever tighter and the penalties for non-compliance becoming harsher

• The media will expose and embarrass wrong-doers and the DPC has the power to take action against us in the event of non-compliance

• Follow policies and procedures

• Contact OCLA and IT Services for assistance

Privacy is everybody’s business!
FOR FURTHER INFORMATION, CONTACT:

Catriona O’Sullivan
Information Compliance Officer
Office of Corporate & Legal Affairs, UCC
Tel: 021 4903949
Email: foi@ucc.ie
Web: http://ocla.ucc.ie/compliance/index.asp

Thank you for your attention