Introduction to Personal Data Protection Law

for DCU Staff

March 2018

DCU Data Protection Office

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Risk & Compliance Office

- A sub-unit of the Office of the Chief Operations Officer

- Responsible for:
  - Facilitating the University's Risk Management Process
  - Management of the University's Policies
  - Secretarial duties related to the Capital Expenditure Programme
  - Assistance with investigations by the Office of the Ombudsman

  - & finally, provision of Data Protection training to staff

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Aims of this presentation

1) Explain the reasons for this training
2) Cover the basic definitions
3) Set out the 7 principles of data protection
4) Data Subject Rights & Data Controller Obligations
5) Set out DCU's approach to assist staff with data protection
6) Increase staff awareness of data protection generally

Introduction only ****it is only the tip of the iceberg!****

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Housekeeping

- Duration of session = 1 Hour +
- Q & A – at any point
- Slides will be circulated
- Attendance Sheet (please sign)

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Examples recent of Data Protection issues in the media

- *******Cambridge Analytica*******
- Department of Social Welfare Data Loss
- GDPR – *'Up to €20 million in fines!'*

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Data Protection (DP) in a nutshell

- Everyone has a fundamental right to privacy
- EU & Irish legislation sets out how this is to be achieved
- Where individuals give their data to DCU, then DCU must protect it
- Enforcement of the law is overseen by the Office the Data Protection Commissioner

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Why must we protect Personal Data?

****It's a legal requirement**** (so no opt-out)

- Promotes good information handling practices
- Protects DCU's reputation (and your own)
- Individuals are increasingly aware of their data rights
- Investigations / audits may be carried out by the DPC
- Litigation / fines if you get it wrong

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Data Protection Legislation

Current Irish Legislation (to be replaced)

- Data Protection Acts of 1988 & 2003 which is based on EU regulations from 1980 & 1995

New EU Regulation - GDPR May 2018

- Elaborates on the existing Data Protection principles
- Becomes effective in May 2018 (so now is the transition phase)
- Penalties of up to €20m or 4% of turnover

Biggest Risk = Individuals may now take legal actions directly

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

What is Personal Data?

Personal data is ‘any information relating to an identified or identifiable natural person’.

e.g. Registry’s student records, HR’s documents relating to staff, Payroll Office records, Campus Company customers, research participants files, medical files, CCTV, emails, online identifiers, genetic data etc.

- Definition is deliberately very broad.
- Refers to living individuals, not legal entities.
- Data can in either an automated or manual format.
- Data must be held in a ‘Relevant Filing System’ to qualify as Persona Data.

****** Data Protection is not the same as Freedom of Information ******

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

What is ‘Special’ or ‘Sensitive’ Data?

A category of data which must not be processed unless allowed for under certain specific exemptions, most usually where explicit consent is obtained. It refers to a person’s:

- Race / ethnicity
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data / Biometric data
- Health data
- Sexual Life / Health / Orientation

Oddly, what category is missing?

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Data Subject

The individual / natural person who is the subject of the personal data e.g. students, staff, research participants, customers, public etc.

Data Controller

The natural or legal person (e.g. body / organisation etc.) who determines the purposes and means of processing of the personal data (e.g. DCU but not its employees).

Data Processor

The natural of legal person who processes data on behalf of a Data Controller.

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

What is ‘Processing’

Processing means performing any operation on personal data, whether or not by automated means, including:

- Collecting / recording
- Organising / structuring
- Storage (Fr. Ted’s Excuse!)
- Altering
- Retrieval / disclosing
- Transmitting / transferring
- Erasure / destruction

Pretty much everything

7 Principles of Data Protection

1. Transparency

State who you are and to what purpose the data being collected will be used for.

'Privacy Notice' or 'Plain Language Statement'
e.g. DCU is the Data Controller and data collected will be used in connection with the provision of services to you. It will also be shared with the HEA, Revenue, Social Welfare, other Data Processors etc.

2. Purpose Limitation

Only process data for the particular purpose for which it was originally collected i.e. it must only be used for a specified purpose.

Case Study- Gym Receptionist

Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

7 Principles of Data Protection cont.

3. Data Minimisation

Data collection is to be limited to only what is adequate, necessary and relevant to the purpose for which it was collected.

4. Accuracy

Data must be accurate, and where necessary, kept up to date. Inaccurate data should be erased or rectified.

5. Storage Limitation

Data is not to be held for any longer than the original purpose for which it was collected.

7 Principles of Data Protection cont.

6. Integrity & Confidentiality

Technical & organisational security measures are to be implemented to keep the data safe & secure e.g. staff training, access rights, PDSS, Data Protection Agreements etc.

Case Study – Researcher's email data leak

7. Accountability

Data Controllers must be able to demonstrate compliance with each of their obligations under GDPR.

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Legal bases for processing

When processing data at least of the following legal bases must apply:

1) By the consent of the individual (explicit if its 'special' data). It must be specific, freely given, and informed. It can also be withdrawn.

2) In fulfilment of a contract with the data subject.

3) Where there is a legal obligation on the Controller (e.g. payroll taxes).

4) Legitimate interest of the Data Controller - (not available to Public Authorities e.g. DCU)

5) For the 'Vital Interests' of the individual (e.g. in an emergency).

6) In Public Interest (e.g. possibly research?).

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Data Subjects Rights

1) Right of access to their own data
2) Right to data portability (where technically possible)
3) Right of erasure (but not an absolute right)
4) Right to rectification if incorrect
5) Right to object to processing (where legitimate interest is the legal basis being used)

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

DCU's Obligations

1) Appoint a 'Data Protection Officer'- Deputy COO

2) Keep records (process logs, data categories, DPIA's, log of data breaches etc.)

3) There is to be mandatory reporting of data breaches within 72 hours

4) Restrict data transfers outside of the EU (very much an evolving area)

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

GDPR – New Concepts

1) DPIAs - Data Protection Impact Assessment

2) Privacy by Design – factor in controls at the design stage for a new process

3) Privacy by Default – any data processing must have data protection as a priority

4) Fines / Compensation rights are enhanced

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

DCU's approach to Personal Data Protection

- Policies & Guides
  - Data Protection Policy
  - Data classification Policy
  - Data Handling Guidelines
  - Data Breach Code of Practice
  - Contact with 3rd Parties Policy

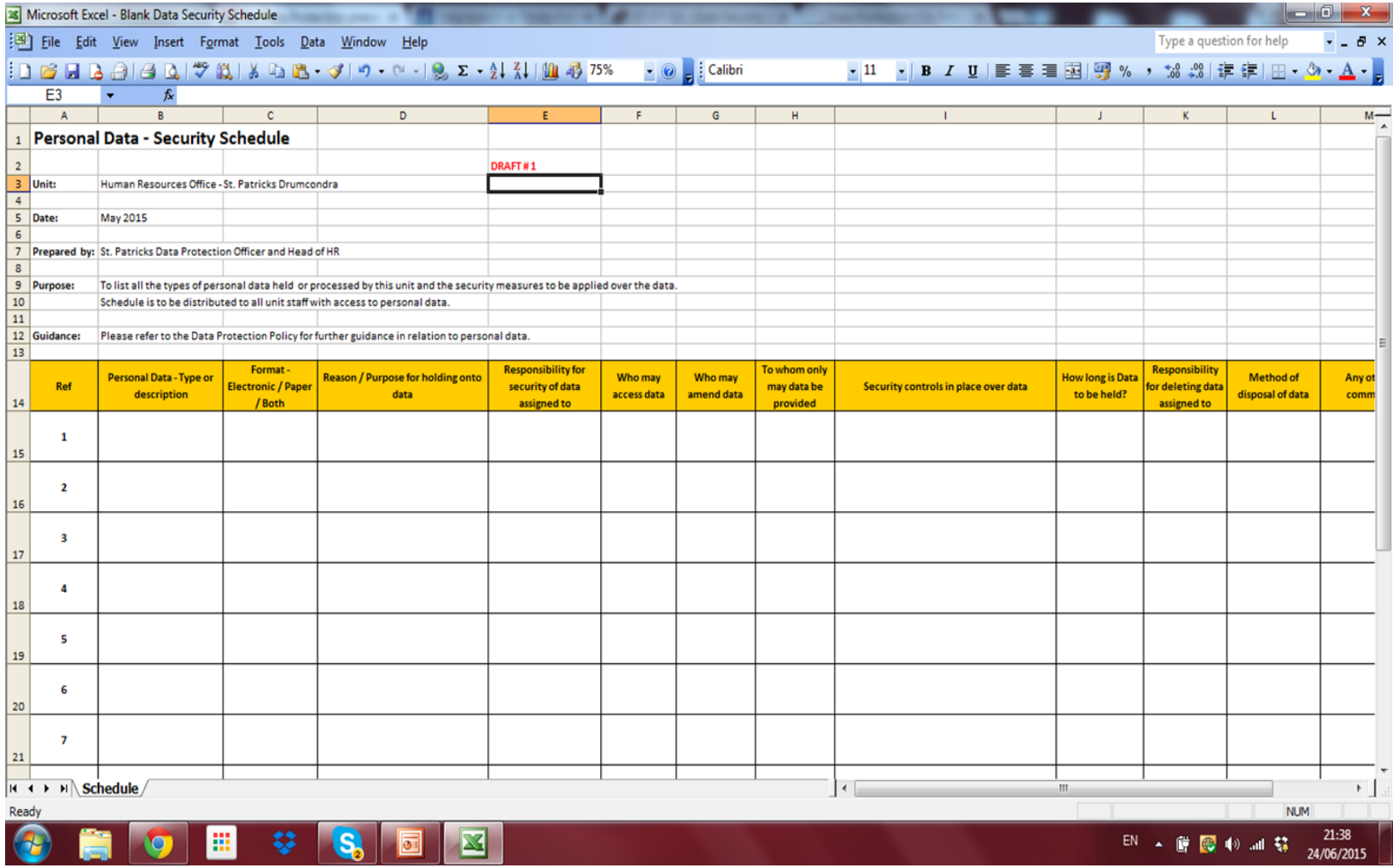
- Data Protection Officer & Unit Data Champions
  - Advice on all DP related issues e.g. transferring our data to other parties (data processing agreements), staff training and management of data breaches.

- ISS Services e.g. encryption of devices, emails etc.

- Provision of a tailored & unit specific Personal Data Security Schedule (i.e. the PDSS)

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

PDSS - Example



Microsoft Excel - Blank Data Security Schedule

Personal Data - Security Schedule

DRAFT #1

Unit:	Human Resources Office - St. Patricks Drumcondra
Date:	May 2015
Prepared by:	St. Patricks Data Protection Officer and Head of HR
Purpose:	To list all the types of personal data held or processed by this unit and the security measures to be applied over the data. Schedule is to be distributed to all unit staff with access to personal data.
Guidance:	Please refer to the Data Protection Policy for further guidance in relation to personal data.

Ref	Personal Data - Type or description	Format - Electronic / Paper / Both	Reason / Purpose for holding onto data	Responsibility for security of data assigned to	Who may access data	Who may amend data	To whom only may data be provided	Security controls in place over data	How long is Data to be held?	Responsibility for deleting data assigned to	Method of disposal of data	Any ot comm
1												
2												
3												
4												
5												
6												
7												

Schedule

Ready

Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Staff Awareness

- Be aware of the types of personal data handled by you and your unit.
- Know your Unit's Data Protection Champion
- Where your unit uses an external party for data processing it must have an agreement in place.
- Apply controls as set out in the unit's PDSS.
- Incoming GDPR: Where new activities, new modes of operations, or projects are planned ensure that the data protection risks inherent in these are managed & addressed at the planning stage.

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Staff Awareness cont.

- Avoid data breaches – (e.g. control access to the data, CC emails where appropriate, encrypt laptops / USB keys).
- Use only approved Google Drives for data storage (not Dropbox).
- Encrypt documents containing personal data prior to emailing them.
- Etc. etc

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Additional Guidance

- Contact DCU Data Protection Officer (COO's Office)

- Helpful websites:
  1) DCU Data Protection webpage - https://www.dcu.ie/ocoo/data-protection.shtml#overlay-context=ocoo/committee-structures.shtml
  2) ISS Encryption Webpage - https://www.dcu.ie/iss/Securing-University-Data.shtml
  3) DCU Central Policies Webpage http://www4.dcu.ie/policies/index.shtml
  4) Irish Data Protection Commissioner https://www.dataprotection.ie/docs/Home/4.htm

DCU
Ollscoil Chathair Bhaile Átha Cliath
Dublin City University

Conclusion – What we have covered

1) Basic data protection definitions

2) 7 Principles of data protection

3) Data rights and obligations

4) Your responsibilities as members of staff

DCU
Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University

Thanks

Noel Prior

Risk & Compliance Officer

noel.prior@dcu.ie

Ext: 8706

Ollscoil Chathair
Bhaile Átha Cliath
Dublin City University