UNIVERSITY of LIMERICK
OLLSCOIL LUIMNIGH

# University of Limerick
# Data Protection Compliance Regulations
June 2015

## 1. Purpose of Data Protection Compliance Regulations

1.1 The purpose of these Compliance Regulations is to assist University of Limerick employees in adhering to the University's Data Protection Policy and the Data Protection Acts (1988 & 2003). The University's Data Protection Policy (available at www.ul.ie/dataprotection) and these Regulations affirm the University's commitment to protecting the privacy rights of individuals in accordance with the Data Protection legislation. These Compliance Regulations set out a range of areas of work in which data protection issues arise and outline best practice that employees should follow.

## PART 1: Explanation of Terms and Guidance on Data Protection Rules

## 2. Explanation of terms

- **Data**: information in a form that can be processed - includes both electronically held data and paper-based data;
- **Electronic/soft-copy data**: information held in an electronic format e.g. on computer, or information recorded with the intention that it be processed by computer;
- **Hard-copy data**: information that is recorded in paper format and is held as part of a relevant filing system or with the intention that it forms part of such a system;
- **Personal data**: data which relates to a living individual who is identifiable either from the data itself or from the data in conjunction with other information held by the University. This can include one or more factors relating to a person's physical, physiological, mental, economic, cultural or social identity. The Acts also differentiate between 'personal data' and **'**sensitive personal data';
- **'Sensitive personal data** relates to a person's racial or ethnic origin; political opinions; religious or philosophical beliefs; physical and mental health; sexual life; criminal convictions; the alleged commission of an offence and trade union membership. The Data Protection Acts require that additional conditions be met for the processing of such data.
- **Data Subject**: an individual to whom personal data relates;

- **Data Controller**: a body that processes information about living people. The data controller must be in a position to control the contents and use of personal data and has overall responsibility for the privacy and security of that data at all times;
- **Data Processor**: a body that processes personal data on behalf of a data controller;
- **Processing**: the performing of any operation / set of operations on data, comprising:
  - obtaining, assembling, organising and storing data,
  - using, consulting and retrieving data,
  - altering, erasing and destroying data,
  - disclosing data.

## 3. Role of Data Protection Commissioner

3.1 The Data Protection Commissioner oversees compliance with the terms of the legislation. The Commissioner has a wide range of enforcement powers, including investigation of University records and record-keeping practices. Should the University be found guilty of an offence it can be fined up to €100,000 and/or may be ordered to delete data.

## 4. The University's Obligations under Data Protection

4.1 As stated in the University's Data Protection Policy, there are eight rules under data protection, which govern the processing of personal data. When processing personal data, whether in paper or electronic form, the following must apply at all times:

- Obtain and process the personal data fairly;
- Keep only for one or more specified, explicit & lawful purpose(s);
- Use and disclose only in ways compatible with the purpose(s) for which it was initially provided;
- Keep safe and secure;
- Keep accurate, complete and up-to-date;
- Ensure that it is adequate, relevant and not excessive;
- Retain for no longer than is necessary for the specified purpose(s);
- Provide a copy of his/her personal data to an individual, on request.

### 4.2 Obtain and process the data fairly:

- Personal data is obtained fairly if the data subject is aware of:
  - the purpose(s) for which the University collects the data;
  - the categories of person/organisation to whom the data may be disclosed;
  - that some questions in forms may be optional;
  - the right of access to their data and their right of rectification of their data;
- Consent for the processing of personal data should be obtained from the data subject;
- **It is essential to obtain explicit consent for the processing of sensitive personal data by way of signature, opt-in box etc.**

**4.3 Keep only for specified and lawful purpose(s);**

- Personal data already collected for a specific purpose may not be used for further processing if the secondary purpose is not compatible with the original purpose.

**4.4 Use and disclose only in ways compatible with the purposes for which it was initially given;**

- Personal data should only be accessed in order to complete official functions of the University;
- Personal data should only be disclosed to work colleagues where the data is required to fulfil an official function of the University;
- Personal data must be kept confidentially and must never be discussed with/disclosed to any unauthorised third party, either internal or external to the University without the prior consent of the data subject, except where there is a statutory obligation to do so (e.g. if required for the purpose of preventing, detecting or investigating offences, required urgently to prevent damage to health or serious loss/damage to property, required under law etc.);
- Personal data relating to a data subject must not be disclosed to any third party, even if they identify themselves as a parent, current/potential employer, professional body, sponsor, etc. Such disclosures must only be with the consent of the individual concerned. This includes requests for contact details (e.g. address, mobile phone number) or even a request to confirm a person's attendance at the University;
- Where individuals (the data subjects) wish to discuss personal data relevant to themselves, the employee must confirm one or more facts that should be known only to the data subjects such as their date of birth, student number, mother's maiden name etc prior to any disclosure.

**4.5 Keep safe and secure;**

- Use and storage of personal data in electronic format must be subject to stringent controls (e.g. use of password protection, timed log-out of systems, encryption of PC folders and portable devices, regular backup, use of anonymisation software etc);
- Authorised users of personal data must ensure that personal data they have access to as part of their duties is kept securely at all times and is protected from inadvertent disclosure, loss, destruction, alteration or corruption;
- Personal data must not be stored or transported on unencrypted laptops, USB devices or other portable devices and every effort must be made to ensure the security of the encrypted devices (e.g. do not store a laptop in your car or allow unauthorised individuals to view computer screens displaying sensitive information);
- Any personal data requiring electronic transfer must be password protected or encrypted;

- When upgrading/changing a PC, always ensure the contents of the hard drive of your old PC are irrevocably deleted by an authorised ITD employee;
- Screens, printouts, documents, and files showing personal data must not be accessible to unauthorised persons;
- Personal data held in paper format must be stored securely in cabinets in locked rooms;
- Subject to the schedules set out in the University's Records Management & Retention Policy (www.ul.ie/recordsmanagement), personal data held must be destroyed by confidential shredding/secure deletion when the retention period has expired.

**4.6 Keep accurate and up-to-date;**

- Administrative procedures should include review and local audit facilities so that personal data is accurate, complete and kept up-to-date.

**4.7 Ensure that it is adequate, relevant and not excessive;**

- The personal data held by the University should be adequate to enable the University achieve its purposes, and no more. Personal data must not be collected or held on a 'just in case' basis.

**4.8 Retain for no longer than is necessary for the specified purpose/purposes;**

- Personal data should be held for the periods specified in the University's Records Management & Retention Policy (www.ul.ie/recordsmanagement). The retention and confidential destruction of personal data must be carried out in accordance with that policy.

**4.9 Provide a copy of his/her personal data to an individual, on request.**

- The Acts provide for the right of access by the data subject to his/her personal data. Where an access request is received, it should be directed to the Information & Compliance Officer in the Corporate Secretary's Office **within a maximum of three days of receipt of the request** in order to enable the University comply with the entitlements of the requester within the timeframes specified in the Acts.

## PART 2: Best Practice Guidance for Key Areas of Work where Data Protection Issues arise

*(not an exclusive list)*

## 5. Use of Third Party Agents (Data Processors) by the University

5.1 There are times when, rather than discharge a service itself, the University may be required to outsource the supply of a service to an external supplier. Data Protection is relevant where service providers have access to the personal data of individual students, employees and other customers.

5.2 If the service involves the processing of personal data on behalf of the University, then in accordance with the Data Protection Acts, **there must be a written contract** between the University (data controller) and the supplier of the service (data processor).

5.3 The Office of the Data Protection Commissioner advises that this contract should stipulate at least the following:

- the conditions under which personal data may be processed;
- the minimum security measures that the data processors must have in place;
- provision that will enable the data controller to ensure that the data processor is compliant with the security requirements.

5.4 All proposed agreements between the University (data controller) and a third party (data processor) must be developed in conjunction with the Corporate Secretary's Office.

## 6. Transfer of Personal Data outside the European Economic Area (EEA)

6.1 The Data Protection Acts 1988 and 2003 specify conditions that must be met before personal data may be transferred to third countries [that is, countries outside of the European Economic Area (EEA)]. In addition, some third countries have been approved for this purpose by the EU Commission and are known as 'approved countries'.

6.2 Organisations that wish to transfer personal data from Ireland to third countries other than those deemed an 'approved country' must first ensure that the country in question provides an adequate level of data protection. In this regard special conditions must be met before personal data may be transferred.

6.2.1 Specific provisions are in place concerning personal data transfers to service providers in the United States of America who are registered under the 'US-EU Safe Harbour' arrangement.

6.2.2 Where a country is not an 'approved country' nor has the 'Safe Harbour' arrangement, EU-approved 'Model Contracts' which contain data protection safeguards to EU standards or 'Binding Corporate Rules' options may be used.

6.3 All proposed agreements between the University (data controller) and a third party (data processor) which will involve the transfer of personal data outside the EEA must be developed in conjunction with the Corporate Secretary's Office.

## 7. Examination Marks, Publication of Student Pass Lists

7.1 Internal and external examiner comments, whether made on an examination script or in another form that allows them to be held and linked to the original script or to a specific candidate (e.g. an examiner's report) are subject to an access request under the Acts.

7.2 The publication of student pass lists on departmental noticeboards is regarded as acceptable by the Office of the Data Protection Commissioner, provided that results are displayed using a student ID number rather than student name, and that no further personal data is presented.

## 8. Personal Data for Research

8.1 Research data comprises all recorded descriptive, numerical, physical or visual material collected and used in the conduct of research, irrespective of medium (e.g. paper or electronic records, physical samples etc.).

8.2 Research data may be of a personal or non-personal nature - research data of a personal nature must be collected and processed in accordance with the Data Protection Acts 1988 & 2003, the University's Data Protection Policy and its Research Ethics Governance Operational Guidelines.

8.3 Whenever possible, personal data should be rendered anonymous. If personal data is collected anonymously or is irrevocably anonymised it is not subject to the requirements of the Data Protection Acts or the University's Data Protection Policy.

### 8.4 Responsibility for the Management of Research Data of a Personal Nature

8.4.1 While the University has overall responsibility for ensuring compliance with the Data Protection legislation, the principal investigator[1]/ supervisor[2] has operational responsibility for ensuring compliance when research data of a personal nature is being collected and processed. This includes ensuring the collection of informed consent and the application of controls to maintain data security, limitation of access, storage, retention and timely and appropriate deletion.

[1] **Principal Investigator:** An employee of the University who has primary responsibility for the design, implementation, completion and management of a research project.

[2] **Supervisor:** An employee of the University who is assigned to a postgraduate research candidate at the time of their commencement of a postgraduate research project. The supervisor has responsibilities relating to the postgraduate's academic and research activities as described in Section 5 of the University of Limerick's Handbook of Academic Regulations and Procedures (Research Postgraduate Academic Regulations).

8.4.2 Where personal data must be collected in order to conduct research, the principal investigator/supervisor is responsible for ensuring:

- that research participants are fully informed of all aspects of the research project in advance of providing any personal data (e.g. the way(s) in which the data will be used, storage, retention time etc), and that appropriate consent for specified use(s) of their personal data is obtained;
- that such personal data is used in accordance with the consent obtained;
- that personal data is accessible to only those researchers who are authorised to undertake the research.

8.4.3 As a standard approach it is important that consent be sought from research participants should there be secondary uses planned for the material/data e.g. future research studies. Any queries in this regard should be referred to dataprotection@ul.ie.

8.4.4 These regulations apply to all University researchers who are conducting research either on or off the University Campus.

## 9. Employment/Student References

9.1 Employment/Student references received by the University may be subject to an access request or FOI request and confidentiality vis-a-vis the individual to whom the reference relates cannot be guaranteed.

## 10. Use of Filming for Teaching Purposes etc.

10.1 Students of certain programmes at the University may use webcams/recording devices (e.g. for teaching purposes). In such circumstances, consent should be obtained from individuals in advance of the commencement of recording; or an appropriate warning sign should be posted clearly within the area covered by the webcam/device. Care is required in order to prevent the unauthorised transfer of images of individuals (deemed personal data). In addition, recordings should only be retained for as long as is necessary after the purpose for undertaking recording has been fulfilled.

## 11. Use of Closed Circuit Television (CCTV)

11.1 Monitored CCTV cameras are installed at various locations on the University of Limerick Campus and record footage with associated date and time.

11.2 The purposes for which the University's CCTV system is installed on Campus, related retention time and details on access to and disclosure of its CCTV footage are as set out in the University's 'Closed Circuit Television (CCTV) System Operating Procedures'.

## 12. Responsibilities of data subjects

12.1 Employees, students and other data subjects are responsible for:

- ensuring that any information they provide to the University is accurate and up to date;
- informing the University of any changes of information that they have provided, such as changes of address etc.

## 13. Breaches of the University Data Protection Policy & Compliance Regulations

13.1 Breaches of the terms and conditions of these Regulations and the University's Data Protection Policy (available at www.ul.ie/dataprotection) could result in major reputational and financial damage to the University and may result in Statute No. 4 of the University of Limerick: 'Employee Disciplinary Matters & Termination of Employment' being invoked.

## 14. Further information

14.1 These Regulations set out key areas of work at the University where data protection issues may arise and outline best practice in dealing with them. However, it is not envisaged that these Regulations contain an exhaustive list of all areas of work to which Data Protection principles apply and employees should contact the Corporate Secretary's Office (Information & Compliance Officer, Ext: 4393, email: dataprotection@ul.ie) to obtain clarification where necessary.

14.2 Extensive information is also available from the Data Protection Commissioner's website, www.dataprotection.ie, or from the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois.

## 15. Review

15.1 These Compliance Regulations will be reviewed regularly in light of any legislative changes.