UNIVERSITY of LIMERICK

OLLSCOIL LUIMNIGH

Personal Data Breach Procedure
June 2018

1. Introduction

1.1 The University of Limerick ("the University") is obliged under data protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a personal data breach. The University is required legally to notify the Office of the Data Protection Commissioner ("the ODPC") **within 72 hours** after becoming aware of a breach. The University is also required to notify the data subjects affected where the data breach in question is likely to result in a "high risk" to their rights and freedoms. Accordingly, it is vital to take prompt action on foot of any such actual or suspected breach to avoid the risk of harm to individuals, damage to operational business and financial, legal and reputational costs to the University. Where there is any doubt as to whether a data breach has occurred or not, the matter must be referred as a priority to the University's Data Protection Officer ("DPO") for evaluation. Therefore, data breaches referred to throughout this Procedure relate to actual and suspected data breaches.

1.2 In addition to the foregoing, any individual or organisation acting on the University's instructions should be made aware of their obligation to report any data breaches to the University as soon as they become aware of the breach in order that the University can comply with its obligations under data protection legislation.

1.3 Data Protection legislation/GDPR relate to personal data which is defined as information 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 in, or is likely to come into, the possession of the University. For more information on terminology, please consult the University's Data Protection Policy and Compliance Regulations available at www.ul.ie/dataprotection. The likelihood or severity of a data breach can be greatly reduced by following the University's Compliance Regulations.

1.4 This Procedure supplements the University's Data Protection Policy and Compliance Regulations by providing a framework for reporting and managing breaches involving personal data.

1.5 This Procedure applies to all staff of the University regarding all personal data created or received by the University in any format, including personal data that is accessed remotely.

2. What is a data breach?

2.1 A data breach is any incident which gives rise to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of/access to personal data processed by the University.

2.2 Data breaches may occur in a variety of contexts, such as loss or theft of data, inappropriate accessing of personal data, disclosures of personal data to unauthorised individuals, to name but a few.

2.3 **If there is any doubt as to whether a data breach has occurred, the Data Protection Officer of the University should be consulted immediately (email: dataprotection@ul.ie).**

3. Procedure for reporting a data breach to the DPO

3.1 Any data breach must be dealt with immediately. When a staff member becomes aware of a breach of data security, he/she must report the incident to the Data Protection Officer at dataprotection@ul.ie immediately.

3.2 After reporting the incident, he/she must complete the Data Breach Report Form and email it to dataprotection@ul.ie as soon as possible and no later than 24 hours after the identification of the breach in order to allow the University to comply with its reporting obligations.

4. DPO Management of Data Breach

4.1 Upon receiving notification of a data breach, the Data Protection Officer will, in conjunction with the Corporate Secretary and other appropriate members of University Staff, take the following steps:

4.1.1 Identification & initial assessment of the incident

Information provided in the Data Breach Report Form will assist the DPO in conducting an initial assessment of:

- Whether a personal data breach has taken place;
- The nature of the personal data involved in the breach;
- The cause of the breach;
- The extent of the breach (i.e. the number of individuals affected)
- The potential harms to which affected individuals may be exposed and whether the breach can be deemed “high risk” so as to warrant notification to those individuals involved;
- Any steps that may be taken to contain the breach in consultation with the relevant University personnel.

Following this initial assessment of the incident, the Corporate Secretary’s Office will, according to the severity of the incident, brief relevant Senior Management.

4.1.2 Containment & Recovery

Where a data breach occurs, immediate and appropriate steps must be taken to limit the extent of the breach. The DPO, in consultation with relevant University staff, will:

- Establish who within the University needs to be made aware of the breach (e.g. IT Division, Communications Office etc.) so as to ensure they act as required in containing the breach (e.g. isolating a compromised section of the network etc);
- Develop correspondence for issue to affected individuals where required and preparation of notification and/or a report to the ODPC.
- Establish whether there is anything that can be done to recover any losses and limit so far as possible the damage caused by the breach;
- Where appropriate, inform the Gardaí (for e.g. in cases involving criminal activity).
- Inform the University's insurers as appropriate.

4.1.3 Notification

In accordance with the requirements of the Data Protection Acts/GDPR, based on the information contained in the data breach report form, incidents in which personal data has been breached must be reported to the ODPC **within 72 hours of the University becoming aware of the incident**. All contact with the ODPC will be made through the DPO or his/her nominee only.

The University will also be required to notify the data subjects affected where the data breach in question is likely to result in a "high risk" to their rights and freedoms. All contact with those data subjects affected will be made only after consultation and agreement with the DPO or his/her nominee.

4.1.4 Evaluation & Response

Following initial assessment of the information contained in the data breach report form, the DPO will conduct further assessment of the incident as the DPO or his/her nominee deems necessary in consultation with relevant staff members to provide any additional information that may be required by the ODPC and to identify and mitigate any risks emerging from the breach.

In addition, in the aftermath of a data breach, the DPO will conduct a review of the incident with the relevant staff to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas for improvement.

The University through its DPO, will maintain a log of data breaches.

5 Further Information

Further information can be obtained from the University's Data Protection Policy and Compliance Regulations at www.ul.ie/dataprotection or on the Office of the Data Protection Commission website www.dataprotection.ie.

UNIVERSITY of LIMERICK

OLLSCOIL LUIMNIGH

DATA BREACH REPORT FORM

If you discover a data breach, please notify your Head of Department **and** the Data Protection Officer immediately.

Please complete this form and return it to the data protection unit at dataprotection@ul.ie within 24 hours of becoming aware of the breach.

Notification of Personal Data Breach

Name of Person Reporting Incident:	
Contact Details of Person Reporting Incident:	
Date(s) of Breach(s):	
Date Incident was discovered:	
Brief Description of Data Breach e.g. cause, types of personal data breached including dates of breaches:	
Number of Data Subjects affected – if known:	
Brief Description of any action(s) since breach was discovered:	
For Data Protection Unit Use Only	
Report received by:	
Date:	
Actions taken & Dates:	
Date of report to ODPC and follow actions:	