# Personal Data Breach – Procedural Guidelines

## Template Version Control

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Author</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>August 2019</td>
<td>TCD DPO</td>
<td></td>
</tr>
</tbody>
</table>
Contents

Template Version Control ................................................................................................................... 1
Introduction ........................................................................................................................................ 3
Scope ................................................................................................................................................... 3
What is a data breach?........................................................................................................................ 4
Procedure for reporting personal data breaches................................................................................. 5
Procedure for managing personal data breaches ..................................................................................... 6
Step 1: Identification & initial assessment of the incident ............................................................. 6
Step 2: Containment & recovery ..................................................................................................... 6
Step 3: Risk assessment................................................................................................................... 7
Step 4: Notification.......................................................................................................................... 8
Step 5: Evaluation & response ........................................................................................................ 9
Guidance ............................................................................................................................................. 9
Appendix 1 – Data Breach Response Flowchart................................................................................ 10
Appendix 2 - Personal Data Breach Report Form ............................................................................. 11
Section 1: Notification of data breach .......................................................................................... 11
Section 2: Assessment of Severity ................................................................................................. 12
Section 3: Action taken .................................................................................................................... 13
Introduction

Trinity College Dublin (‘Trinity College’ / the ‘University’) is required under data protection legislation to keep personal data safe and secure and to respond promptly and appropriately in the event of a breach of security relating to personal data (hereinafter ‘data breach’).

The purpose of these Procedural Guidelines (the ‘Guidelines’) is to provide a framework for reporting and managing breaches involving personal data controlled and processed by the University.

The Guidelines supplement the Trinity Data Protection Policy which affirms the University’s commitment to protect the privacy rights of individuals in accordance with data protection legislation, namely the EU General Data Protection Regulation (‘GDPR’) and Data Protection Act 2018.

It is imperative for all Trinity College staff and students to immediately report any potential or suspected data breach to the Data Protection Officer (DPO) by phone or email – contact details are listed below.

If unsure whether an incident is a data breach or not please refer to the guidance set out within this document and consult with the DPO.

Scope

The Guidelines apply to all processors of Trinity College-controlled personal data, including:

- Any individual who is employed by Trinity College or is engaged by Trinity College who has access to University-controlled or processed personal data in the course of their employment or engagement for administrative, research and / or any other purpose;

- Any student of Trinity College who has access to University-controlled or processed personal data in the course of their studies for administrative, research and / or any other purpose; or

- Individuals who are not directly employed by Trinity College, but who are employed by contractors (or subcontractors) and who have access to University-controlled or processed personal data in the course of their duties for the University.

These Guidelines apply to:

- All personal data processed by Trinity College in any format (including electronic and paper records), whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically, or accessed remotely;

- Personal data held on all Trinity College IT systems managed centrally by IT Services, and locally by individual Schools / Departments / Offices / Institutes or Centres;

- Any other IT systems, including email and Cloud-based platforms on which University-controlled or processed personal data is processed.
What is a data breach?

Under GDPR, a data breach is defined as 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. This definition extends to breaches which result from malicious conduct, lack of appropriate security controls, system or human failure, or error.

Data breaches may occur in a variety of contexts. For example:

- Loss or theft of data, including equipment on which data is stored (e.g. laptop, smartphone, tablet USB key etc.) or paper records
- Inappropriate access controls allowing unauthorised use of information (e.g. uploading personal data to an unsecured web domain, using unsecure passwords)
- Equipment failure
- Confidential information left unlocked in accessible areas (e.g. leaving IT equipment unattended when logged into a user account)
- Disclosing confidential data to unauthorised individuals
- Collection of personal data by unauthorised individuals
- Human error / accidental disclosure of data (e.g. emails containing personal or sensitive personal data sent to the wrong recipient)
- Hacking, viruses or other security attacks on IT equipment, systems or networks
- Breaches of physical security (e.g. forcing of doors / windows / filing cabinets)

Whether an incident giving rise to the suspected data breach involves personal data must be determined on a case-by-case basis. If an incident does not involve personal data, it is not a data breach per the GDPR definition. Furthermore, not all data incidents involving personal data will be data breaches. For example:

- The personal data is securely encrypted or anonymised such to make the personal data unintelligible; and/or
- There is a full, up-to-date back-up of the personal data (in cases of accidental destruction).

If there is any doubt as to whether a data breach has occurred, the DPO should be consulted immediately.

**Personal data** is defined under GDPR as any information relating to an identified or identifiable natural person.

**Processing** is defined under GDPR as any operation or set of operations which is performed on personal data or on 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.
Procedure for reporting personal data breaches

Under Article 33 GDPR Trinity must report a data breach, if deemed reportable, to the Data Protection Commission within 72 hours of becoming aware of the breach. This timeframe includes weekends and bank holidays.

Under Article 34 GDPR Trinity must inform affected individuals without undue delay if the data breach is likely to result in a high risk to their privacy.

As such, any data breach must be dealt with immediately and appropriately. If a member of the University becomes aware of an actual, potential or suspected data breach, they must report the incident to their Head of School / Head of Unit immediately. The Head of School / Unit must then immediately report the incident to the DPO.

After reporting the incident, the relevant member of the University must complete the Personal Data Breach Report Form (see Appendix 2 below) and forward it to the DPO as soon as possible. The DPO is responsible for keeping a written record of all potential or suspected data breaches that are notified to him / her (including those that are not notified to the Data Protection Commission or the affected individuals). For this purpose, it is imperative that the Personal Data Breach Report Form is completed satisfactorily. This will enable all the relevant details of the incident to be recorded consistently and communicated on a need-to-know basis to relevant staff so that prompt and appropriate action can be taken to resolve the incident.
Procedure for managing personal data breaches

Upon receiving notification of a data breach, the DPO shall, in conjunction with appropriate members of staff, take the following five steps (in line with best practice) when responding to the incident:

- **Step 1: Identification and initial assessment of the incident**
- **Step 2: Containment & recovery**
- **Step 3: Risk assessment**
- **Step 4: Notification**
- **Step 5: Evaluation & response**

**Step 1: Identification & initial assessment of the incident**

If any member of the University considers that a data breach has, or might have, occurred, they must report the incident immediately and complete the Personal Data Breach Report form. The Personal Data Breach Report Form will assist the DPO in conducting an initial assessment of the incident.

This assessment will take into account:

- Whether a data breach has taken place
- The nature of the personal data involved in the breach (i.e. whether sensitive or confidential personal data is involved)
- 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
- Any steps that may be taken to contain the breach

Following this initial assessment of the incident, the DPO may, according to the severity of the incident, consult with the Secretary to the College and decide if it is necessary to appoint a group of relevant University stakeholders (e.g. IT Services, Human Resources, Academic Registry) to assist with the investigation and containment process.

**Step 2: Containment & recovery**

In the event of a data breach, immediate and appropriate steps must be taken to limit the extent of the breach.

The DPO, in consultation with relevant staff, will:
Establish who within Trinity needs to be made aware of the breach (e.g. IT Services, Communications Office) and inform them of their expected role in containing the breach (e.g. isolating a compromised section of the network)

Establish whether there is anything that can be done to recover any losses and limit the damage caused by the breach

Where appropriate, inform the Gardaí (e.g. in cases involving criminal activity)

Step 3: Risk assessment

The DPO, in conjunction with relevant staff, will use the information provided in the Personal Data Breach Report Form to fulfil the requirement to assess the potential adverse consequences for individuals, including how likely such adverse consequences are to materialise and how serious or substantial they are likely to be.

This assessment should, in particular, consider the likelihood of risks taking place and the severity of such risks is to be categorised as no risk / risk / high risk in accordance with the detailed criteria below:

(a) **Type of breach:** A data breach may include any unauthorised or accidental disclosure, loss, destruction, damage or any other form of unauthorised, accidental or unlawful access to, collection, use, recording, storing or distributing of personal data. What type of data breach has or may have occurred? Does the breach consist of a breach of confidentiality relating to personal data? Is there a temporary or permanent lack of availability or access to personal data and if temporary, how long will it be before it is restored?

(b) **Nature of personal data:** Is the relevant personal data sensitive in nature? The more sensitive the personal data the higher the risk of the data breach. The utility of the relevant information may also indicate a higher risk to the affected individuals.

(c) **Scale and volume of personal data affected:** The higher the volume of the personal data records and the number of individuals potentially affected will usually create a higher risk.

(d) **Ease of identification:** The ease of identifying the relevant individuals based on the personal data will likely increase the risk of identity theft, fraud and reputational damage in particular.

(e) **Security measures:** Are the risks arising from the breach limited as a result of inherent security measures, such as encryption, where the confidentiality of the key is still intact and the data is unintelligible to a third party?

(f) **Containment measures:** Have any containment measures been implemented which mean that the data breach is unlikely to present a risk to the individuals affected?

(g) **Other factors:** Other relevant factors in assessing the risk to individuals is whether those individuals affected by the data breach have any special characteristics (for example children or vulnerable adults).
Severity of risk: Based on the above criteria and any other relevant factors, the DPO should assess the severity of the risk in terms of the potential consequences to the individuals affected by the data breach.

(i) Likelihood of the risk(s) materialising: Once the data breach has occurred, the DPO must objectively assess the likelihood of the potential risks actually materialising and this should form part of the risk assessment.

An assessment of the risks for the University, including strategic and operational, legal, financial and reputational risks may also be prepared.

Step 4: Notification

Data Protection Commission: Under Article 33 GDPR Trinity College must report a data breach, if deemed reportable, to the Data Protection Commission within 72 hours of becoming aware of the breach. This timeframe includes weekends and bank holidays.

If the relevant details surrounding the data breach are not clear within the initial 72 hour notification period, an initial notification should be made to the Data Protection Commission. Subsequent notifications can be made to the Data Protection Commission in phases. Consideration as to whether a communication to affected individuals is required should be addressed when notifying the Data Protection Commission.

All contact with the Data Protection Commission should be made through the DPO.

The decision to report a breach to the Data Protection Commission will ultimately be made by the Secretary to the College, in consultation with the DPO and relevant University staff. If a decision is made to not report a breach, a summary record of the incident with an explanation of the basis for not informing the Data Protection Commission will be retained by the DPO.

Affected individuals: Under Article 34 GDPR Trinity College must inform affected individuals without undue delay, if the data breach is likely to result in a high risk to their privacy.

Where the DPO assesses that there is a high risk to rights and freedoms of individuals as a result of the data breach, then the existence of the data breach should be communicated to the affected individuals without undue delay.

Any such communication should inform the affected individuals on relevant measures that they can take to reduce the risks to them and any negative consequences arising from the data breach. The DPO should determine the most appropriate and effective means of communicating the data breach to the affected individuals, if necessary engaging the assistance of communications advisors.

Notification should have a clear purpose, e.g. to enable individuals who may have been affected to take steps to protect themselves (e.g. by cancelling a credit card or changing a password), to allow regulatory bodies to perform their functions, provide advice and deal with complaints, etc.

In each case, the notification should include as a minimum:

- a description of the nature of the breach;
- a description of the likely consequences of the breach;
- how and when the breach occurred;
- what data was involved;
- a description of the measures taken or proposed to be taken by the University to address the breach;
- the name and contact details of the DPO and other contact points.

**Other parties:** Trinity should consider, and seek advice as appropriate, as to whether there are any other relevant notification requirements are required (such as to the Gardaí, insurers, external legal advisers etc.).

**Step 5: Evaluation & response**

Certain data breaches will require further detailed investigation after the initial investigation period, which may involve external IT, legal and other support, as appropriate to ascertain the full extent of the data breach, its causes, likely consequences and in order to effectively contain the breach. The effect of the data breach must be monitored and the risks re-evaluated throughout this period. It may be necessary to agree a phased notification program with the Data Protection Commission in these instances.

In the aftermath of a data breach, a post-incident review of the incident should take place to ensure that the steps taken during the incident were appropriate and effective, and to identify any areas that may be improved in future, such as updating policies and procedures or addressing systematic issues if they arise, in order to reduce the recurrence of similar data breaches and to ensure that appropriate technical and organisational security measures are put in place.

**Guidance**

For further information and advice about what to do in the event of a suspected data breach please contact:

Data Protection Officer
Office of the College Secretary
Trinity College
Dublin 2

Email: dataprotection@tcd.ie
Tel: +353 (0)1 896 1892

Comprehensive information on data breach notification is available from the Data Protection Commission.
Appendix 1 – Data Breach Response Flowchart

A. Flowchart showing notification requirements

Controller detects/is made aware of a security incident and establishes if personal data breach has occurred.

The controller becomes “aware” of a personal data breach and assesses risk to individuals.

Is the breach likely to result in a risk to individuals’ rights and freedoms?

No

No requirement to notify supervisory authority or individuals.

Yes

Notify competent supervisory authority.

If the breach affects individuals in more than one Member State, notify the lead supervisory authority.

Is the breach likely to result in a high risk to individuals’ rights and freedoms?

Yes

No requirement to notify individuals.

No

Notify affected individuals and, where required, provide information on steps they can take to protect themselves from consequences of the breach.

All breaches recordable under Article 33(5). Breach should be documented and record maintained by the controller.
Appendix 2 - Personal Data Breach Report Form

Please act promptly to report any data breaches. If you discover a data breach, please notify your Head of School / Unit immediately. Heads of School / Unit to complete Section 1 of this form and email it to the DPO immediately.

Section 1: Notification of data breach

<table>
<thead>
<tr>
<th>INCIDENT DETAIL</th>
<th>TO BE COMPLETED BY HEAD OF SCHOOL / UNIT OF PERSON REPORTING INCIDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date incident was discovered:</td>
<td></td>
</tr>
<tr>
<td>Date(s) of incident:</td>
<td></td>
</tr>
<tr>
<td>Place of incident:</td>
<td></td>
</tr>
<tr>
<td>Name of person reporting incident:</td>
<td></td>
</tr>
<tr>
<td>Contact details of person reporting incident (email address, telephone number, Trinity address):</td>
<td></td>
</tr>
<tr>
<td>Description of incident:</td>
<td></td>
</tr>
<tr>
<td>Details of the IT systems, equipment, devices, records involved in the incident:</td>
<td></td>
</tr>
<tr>
<td>Number of data subjects affected, if known:</td>
<td></td>
</tr>
<tr>
<td>Has any personal data been placed at risk? If, so please provide details:</td>
<td></td>
</tr>
<tr>
<td>Brief description of any action taken at the time of discovery:</td>
<td></td>
</tr>
</tbody>
</table>
## Section 2: Assessment of Severity

<table>
<thead>
<tr>
<th>DETAIL OF DATA BREACH</th>
<th>TO BE COMPLETED BY DPO IN CONSULTATION WITH HEAD OF AREA AFFECTED BY THE BREACH</th>
</tr>
</thead>
<tbody>
<tr>
<td>If laptop lost / stolen: how recently was the laptop backed up onto central IT systems?</td>
<td></td>
</tr>
<tr>
<td>Is the information unique? Will its loss have adverse operational, research, financial legal, liability or reputational consequences for the University or third parties?</td>
<td></td>
</tr>
<tr>
<td>Is the data bound by any contractual security arrangements e.g. to research sponsors?</td>
<td></td>
</tr>
</tbody>
</table>

### WHAT IS THE NATURE OF THE SENSITIVITY OF THE DATA?

**PLEASE PROVIDE DETAILS OF ANY TYPES OF INFORMATION THAT FALL INTO ANY OF THE CATEGORIES LISTED BELOW**

1. **High risk personal data - special categories of personal data relating to a person’s**
   - racial or ethnic origin
   - political opinions
   - religious or philosophical beliefs
   - membership of a trade union
   - genetic or biometric data
   - data concerning health
   - data concerning a person’s sex life or sexual orientation

2. **Information that could be used to commit identity fraud such as personal bank account and other financial information and national identifiers, such as Personal Public Service Numbers (PPSNs) and copies of passports and visas**

3. **Personal information relating to vulnerable adults and children**

4. **Detailed profiles of individuals including information about work performance, salaries or personal life that would cause significant damage or distress to that person if disclosed**

5. **Spreadsheets of marks or grades obtained by students, information about individual cases of student discipline or sensitive negotiations which could adversely affect individuals**

6. **Security information that would compromise the safety of individuals if disclosed.**
### Section 3: Action taken

<table>
<thead>
<tr>
<th>SECTION 3: ACTION TAKEN</th>
<th>TO BE COMPLETED BY DPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the incident reportable to the Data Protection Commission?</td>
<td></td>
</tr>
<tr>
<td>If notified to Data Protection Commission, provide details, incl. date and reference number:</td>
<td></td>
</tr>
<tr>
<td>If notified to data subjects, provide details, incl. date:</td>
<td></td>
</tr>
<tr>
<td>If notified to other external, regulator/stakeholder, provide details:</td>
<td></td>
</tr>
<tr>
<td>If reported to Gardai, provide details, incl. dates:</td>
<td></td>
</tr>
<tr>
<td>If notified to other internal stakeholders, provide details and dates:</td>
<td></td>
</tr>
<tr>
<td>Follow up action / Corrective remediation actions required / recommended:</td>
<td></td>
</tr>
</tbody>
</table>