**Data Breach Notification – Procedural Guidelines**

# 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 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**](https://www.tcd.ie/dataprotection/assets/docs/dataprotectionpolicy/Trinity_College_Dublin_Data_Protection_Policy_16122020.pdf)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.

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the College is required under GDPR to report the breach to the Data Protection Commission **within 72 hours of discovery, even if the risk is not considered as substantial**.

Where appropriate, actions to inform data subjects affected by the breach and reduce risks to their privacy arising from the breach must also be implemented without delay, pursuant to Article 34 GDPR.

These timeframes include weekend and public holidays and failure to comply will result in regulatory sanction and reputational damage for the College.

### As such, it is extremely important that you take immediate action upon learning of a breach or suspected incident involving the loss or disclosure of data and contact the Data Protection Officer at [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie) and Head Of School / Unit without delay. All emails should be marked ‘Urgent’.

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

These Guidelines apply to individuals who process personal data on behalf of Trinity College, 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 including working from home, 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 and software solutions, including Cloud- based platforms, managed centrally by IT Services or 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:

* Disclosing confidential data to unauthorised individuals. For example, accidentally sending an email containing confidential or sensitive data to the wrong recipient or recipients as a result of human error.
* 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).
* Collection of personal data by unauthorised individuals.
* 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 (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’*.

Special categories of personal data are defined under GDPR as:

Personal data revealing racial origin, ethnic origin, political opinions, religious beliefs, philosophical beliefs, trade-union membership, genetic and biometric data which is processed for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life and data concerning a natural person’s sexual orientation

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 a Data Breach

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 the Data Protection Officer at [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie) and to their Head of School / Head of Unit immediately. All emails should be marked ‘Urgent’.

Please familiarise yourself with the [**Data Breach Response Flowchart**](#_Trinity_College_Procedure) (Appendix 1). After reporting the incident, the relevant membe[r of the University must comple](#_bookmark0)te the [**Personal Data Breach Report Form**](#Appendix_2_-_Personal_Data_Breach_Report) (Appendix 2) 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 a Data Breach

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 and type of the personal data involved in the breach, including whether sensitive or confidential personal data has been compromised.
* 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, Financial Services Division, 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, notifying affected individuals).
* 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:

1. **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?

1. **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.
2. **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.
3. **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.
4. **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?
5. **Containment measures:** Have any containment measures been implemented which mean that the data breach is unlikely to present a risk to the individuals affected?
6. **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).
7. **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.
8. **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.
9. **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 then 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 must be made through the DPO.

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 and engaging the assistance of communications advisors if appropriate.

Notification should have a clear purpose, to enable individuals who may have been affected to take appropriate 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. 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; and
* 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, Secretary’s Office, Trinity College, Dublin 2, Ireland.

Email: [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie)

Comprehensive information on Data Breach Notifications is available from the Data Protection Commission [Website.](https://www.dataprotection.ie/sites/default/files/uploads/2019-08/190812%20GDPR%20Breach%20Notification%20Quick%20Guide.pdf)

# **Graphical user interface, text, application Description automatically generated****Appendix 1 - Trinity College Procedure - Data Breach**

**STEP 5**

**DPO agrees appropriate course of action with relevant stakeholders**

**STEP 1**

**Member of staff becomes aware of incident involving breach / suspected breach of personal data**

**STEP 2**

**Incident is immediately reported to DPO and Head of Unit**

**STEP 3**

**Personal Data Breach Report Form filled out and sent to** [**dataprotection@tcd.ie**](mailto:dataprotection@tcd.ie)

**STEP 4**

**Risk Assessment carried out to determine cause, extent and severity of the incident**

GDPR Requirements - Data Breach

**DPO documents the rationale for not notifying affected individuals – Article 33 GDPR**

**Affected individuals to be notified of breach immediately and advised of steps to be taken to mitigate impact of breach**

**– Article 34 GDPR**

**DPO documents the incident and rationale for not reporting to the DPC**

**– Article 33 GDPR**

**No**

**Yes**

**1.**

**Is the breach likely to result in a RISK to individuals’ rights & freedoms?**

**No**

**Yes**

**2.**

**Is the breach likely to result in a HIGH RISK to individuals’ rights & freedoms?**

**Breach Notification to be made by DPO to the DPC within 72 hours of College staff first becoming aware of the breach – Article 33 GDPR**

**Execute remedial actions to be implemented to mitigate similar incidents re-occurring**

**All breaches to be documented – log of all incidents to be retained by DPO – Article 33 GDPR**

# **Appendix 2 - Personal Data Breach Report Form**

**It is extremely important that you take immediate action upon learning of a breach or suspected incident involving the loss or disclosure of data and contact the Data Protection Officer at** [**dataprotection@tcd.ie**](mailto:dataprotection@tcd.ie) **and Head Of School / Unit without delay. All emails should be marked ‘Urgent’.**

|  |  |  |
| --- | --- | --- |
|  | **Section A: Incident Timeline - Complete all sections** | |
| 1. Name of person reporting incident: | |  |
| 1. Date and precise time of the incident: | |  |
| 1. Date and precise time the incident was detected: | |  |
| 1. Date / time of reporting the incident to Data Protection Officer:   Timely reporting is crucial to satisfy the GDPR’s **72 hour deadline**. If you are reporting outside of this timeframe please explain why. | |  |
| 1. Is the incident ongoing? | | Yes / No |
| 1. Date / time that the incident ended: | |  |
| 1. School / Unit where incident occurred: | |  |
| 1. Name of Head of School / Unit: | |  |
| 1. Has the Head of School / Unit been informed? | | Yes / No |

|  |  |  |
| --- | --- | --- |
|  | **Section B: Incident Detail** | |
| Please describe how the incident occurred. Provide as much detail as possible. | | |
| What [personal data](#_bookmark1) was disclosed? | | |
| Were any [special categories of personal data](#_bookmark2) or confidential data involved?  Provide detail. | |  |
| Do you know the number of affected individuals?  Provide detail. | |  |
| Do you know the number of affected records?  Provide detail. | |  |

|  |  |
| --- | --- |
| Were vulnerable individuals affected? |  |
| What measures have been taken in response to the incident? |  |
| Have you secured / retrieved any breached data? |  |
| If not, please outline why you have not secured / retrieved the data. |  |
| What in your view are the potential consequences of the incident for affected individuals? |  |
| How severe is the incident for affected individuals? | Low risk / Medium risk / High risk |
| Have you notified the affected individuals of the incident? |  |
| How many affected individuals have been informed? |  |
| What information was communicated to the affected individuals?  In particular, please indicate if you have related to affected individuals the steps they should take to mitigate any adverse consequences which have been caused or could be caused to them by this incident. |  |

|  |  |  |
| --- | --- | --- |
|  | **Section C: Course of Action as Determined by Data Protection Officer** | |
| Personal data breach? | | Yes / No |
| Risk to data subjects? | | High risk / Medium risk / Low risk |
| Is the incident reportable to the Data Protection Commission? | | Yes / No |
| If notified to Data Protection Commission, provide details, incl. date and time of notification and reference number. | |  |
| Data subjects to be informed? | | Yes / No |
| If notified to data subjects, provide details, incl. dates. | |  |
| If notified to other external regulators / stakeholders, provide details. | |  |
| If reported to Gardaí, provide details, incl. dates. | |  |
| If notified to other internal stakeholders, provide details and dates. | |  |
| What deficiencies in the organisational or technical measures have been identified as a result of this breach? | |  |
| What mitigating factors will be put in place i.e. is there a need for reviewing processes, retraining, etc.: | |  |
| When will these measures be implemented? | |  |
| Other comments / details: | | |