Data Protection
Procedural Guidelines for Personal Data Security Breaches

Introduction

The University of Notre Dame (USA) ("Notre Dame") and its offices within the European Union are 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 security breach. It is vital to take prompt action on foot of any such actual, potential or suspected security breach to avoid the risk of harm to individuals, damage to operational business and financial, legal and reputational costs to Notre Dame.

The purpose of these guidelines is to supplement the UND Data Protection Policy by providing a framework for reporting and managing security breaches involving personal or sensitive personal data. These guidelines may be used by all members of the Notre Dame community in a combined effort to minimize the damage done by personal data security breaches.

1. **What Is A Personal Data Security Breach?**

A personal data security breach is any incident which gives rise to a risk of unauthorized disclosure, loss, destruction or alteration of personal data held by Notre Dame.

Personal data security breaches may occur in a variety of contexts, such as:

- Loss or theft of data, equipment on which data is stored (e.g. a memory stick) 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 information 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)

If there is any doubt as to whether a personal data security breach has occurred, Notre Dame should be consulted immediately.

These guidelines apply to all personal data created or received by Notre Dame in any format, including data that is accessed remotely. Personal data 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 UND.

2. Procedure For Reporting Personal Data Security Breaches

Any personal data security breach must be dealt with immediately and appropriately.

If a member of Notre Dame becomes aware of an actual, potential or suspected breach of data security, they must report the incident to Notre Dame immediately via oithelp@nd.edu .

3. Procedure For Managing Personal Data Security Breaches

Upon receiving notification of a personal data security breach, Notre Dame shall, in conjunction with any appropriate members of staff, take the following steps (in line with best practice[1]) when responding to the breach.

Step 1: Identification & initial assessment of the incident

If any member of Notre Dame considers that a data security breach has, or might have, occurred, they must report this breach immediately to Notre Dame via oithelp@nd.edu .

Notre Dame will conduct an initial assessment of the incident. This assessment will take into account:

- Whether a personal data security breach has taken place
- The nature of the personal data involved in the breach (i.e. whether sensitive 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, Notre Dame may, according to the severity of the incident, consult within the Office of Information Technology and decide if it is necessary to appoint a group of relevant Notre Dame stakeholders (e.g. IT Services, Human Resources) to assist with the investigation and containment process.

[1] https://gdpr-info.eu/

Step 2: Containment & Recovery

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

Notre Dame, in consultation with relevant staff, will:

- Establish who within the local office and Notre Dame 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 appropriate legal authorities, e.g. in cases involving criminal activity.

Step 3: Risk Assessment

Notre Dame, in conjunction with relevant staff, will use the information provided in the Personal Data Security Breach Report form to fulfil the requirement to consider 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.

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

Step 4: Notification

In accordance with the General Data Protection Regulation[2], all incidents in which personal data has been put at risk must be reported to the appropriate Legal Supervisory Authority's office (LSA) within working 72 hours (3 days) of Notre Dame becoming aware of the incident.

Incidents do not have to be reported to the LSA's Office when:

- The full extent and consequences of the incident have been reported without delay directly to the affected data subject(s) **and**
- The incident affects no more than 100 data subjects **and**
- The incident does not affect sensitive personal data or personal data of a financial nature.

All contact with the LSA's Office should be made through Notre Dame.

The decision to report a breach to the LSA's Office will ultimately be made by Notre Dame, in consultation with the Office of Information Technology and Office of General Counsel. If a decision is made not to report a breach, a brief summary record of the incident with an

[2] https://gdpr-info.eu/

explanation of the basis for not informing the LSA's Office will be retained by Notre Dame and the local office.

Step 5: Evaluation & Response

In the aftermath of a personal data security breach, a review of the incident may 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.

Further Information

Further information can be obtained via the websites for applicable legal supervisory authorities offices.

Ireland Supervisory Authority Office: https://www.dataprotection.ie/