Information Compliance

Data Breach Policy and Procedures

December 2019

Document properties

Authority

Chief Information Officer

Sponsor

Chief Information Officer

Responsible Officer

Data Protection Officer

Version history

This is version 1 of this policy.

1 Introduction

Appropriate handling of personal data breaches is one element of ensuring adequate security of personal data.

Training and support regarding the appropriate handling of personal data is provided to all employees.

This document explains what a personal data breach is, and describes the actions to be taken when a breach is discovered.

2 Executive summary and key points

2.1 Legislative background

The requirement to protect personal data from unauthorised or accidental disclosure rests in the sixth data protection principle. Other aspects of data protection law require reporting of incidents to the supervisory authority and keeping a record of all data breaches.

2.2 Personal data breaches

Data breaches may affect *confidentiality*, *integrity* or *availability* of personal data.

Individuals affected by a data breach may experience actual harm, emotional distress, physical or material damage, or inconvenience.

2.3 Reporting a data breach

All data breaches must be reported to the Data Protection Officer. Depending on factors such as the number of records or individuals affected, or the type of data involved, the Data Protection Officer may be required to report the breach to the Information Commissioner's Office and the individuals affected.

2.4 Containment and recovery

A cybersecurity-based breach is likely to be of some duration, and it is important to contain the breach to as few affected individuals as possible.

An email breach, on the other hand, is more likely to require recovery, by requesting the individual to whom the email was erroneously sent, to delete it.

2.5 Consequences of a data breach

Besides the effects of a data breach on individuals, there are consequences for the University. These may be reputational damage, lawsuits by affected individuals, or action by the Information Commissioner's Office. The latter may be administrative, judicial or monetary.

2.6 Avoiding a data breach

Measures which can be taken to try to avoid personal data breaches include training or technology solutions, such as encryption.

However, most data breaches can be avoided if employees take care when sending emails, adhere to a clean desk policy, and ensure manual personal data is locked up when not in use.

2.7 References

A list of useful links to more information about personal data breaches, and data protection generally, may be found in section 9.

3 Legislative background

The sixth data protection principle states that:

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Even with appropriate security measures and training of employees, data breaches can and do occur. Procedures for dealing with data breaches are also part of those organisational measures.

Data protection law also stipulates the time limit for notifying the supervisory authority (in our case, the Information Commissioner's Office (ICO)) and, where appropriate, the individuals affected by the data breach.

In addition, the law requires us to document all data breaches, even if we are not required to report them to the ICO.

4 Personal data breaches

A breach of security which leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data is a *personal data breach*. It makes no difference if the breach was deliberate or accidental; it is still a data breach.

A data breach may affect any or all of the qualities of confidentiality, integrity or availability of personal data.

4.1 Types of data breaches

4.1.1 Breaches of confidentiality

Examples of breaches of confidentiality are access to personal data by an unauthorised third party, or sending personal data to the incorrect recipient.

The loss or theft of a device (computer/laptop/flash drive, etc.) may also lead to a breach of confidentiality if the device is not encrypted or otherwise protected from unauthorised access.

4.1.2 Breaches of integrity

Data integrity is the maintenance of, and the assurance of the accuracy and consistency of data over its entire life-cycle.

Breaches of this type may be caused by deliberate or accidental action or inaction by a controller or processor, or alteration of personal data without permission.

4.1.3 Breaches of availability

> *Availability* refers to the ability to access data when and where needed, even when disruptions occur.

This kind of breach is often the result of a cybersecurity incident, such as a ransomware attack. In this kind of attack, the data on the device or server has been encrypted and payment demanded for its de-encryption. A Distributed Denial of Service (DDOS) attack may also affect data availability.

Other common causes of data availability breaches are theft of a device on which personal data are stored, or the destruction of personal data, whether accidentally or intentionally.

4.2 Effects of data breaches

Depending on the severity of the breach, any one or more of the consequences listed below may occur to the detriment of the individual(s) whose data have been breached:

- Loss of control over personal data
- Limitation of rights
- Discrimination
- Identity theft or fraud
- Financial loss

- Damage to reputation
- Loss of confidentiality of personal data protected by professional secrecy
- Other economic or social disadvantage

A data breach may also cause emotional distress, physical or material damage, or inconvenience to an affected individual.

The possible consequences of a data breach can be found in section 7.

5 Reporting a data breach

5.1 Data Protection Officer

All data breaches must be reported to the Data Protection team, regardless of how trivial the breach may appear.

Anyone discovering a suspected data breach, or realising they have caused a data breach, should fill in the *Data breach report* form as soon as possible.

If you are unsure if what occurred is a data breach, you should still report it. If the Data Protection Officer (DPO) has to report the breach to the ICO, it must be done *within 72 hours of discovery of the breach*.

The DPO is required to record all data breaches, whether or not they need to be reported to the ICO. Information recorded must include:

- the facts related to the breach
- its effects
- remedial action
- steps taken to reduce the risk of a similar breach taking place
- justification for not reporting the breach to the ICO

5.2 Information Commissioner's Office

Not all data breaches need to be reported to the ICO. The DPO must assess each breach for potential adverse effects on the individual(s) whose data have been breached. If there is a risk to individuals' rights and freedoms, then the ICO must be notified of the breach.

Factors which will be considered when assessing this risk include:

- The type of breach
- The number of individuals affected
- The nature of the data breached, e.g. bank details, special category personal data
- Whether the information in already publicly available
- Whether the data were encrypted
- Whether a recent backup of the data exists
- How easy it will be for individuals to be identified
- The severity of consequences for individuals

It is the responsibility of the DPO, or the Cyber and Information Security Manager (CISM), where the breach has occurred as a result of a cybersecurity incident.

5.3 Individuals

If a breach is likely to result in a *high* risk to the rights and freedoms of individuals, then those affected by the breach must be informed.

When informing individuals of a breach, we need to provide:

- The nature of the breach, in clear and plain language
- The name and details of the DPO or other contact point where more information can be obtained
- A description of the likely consequences of the breach
- A description of the measures which have, or are proposed to be, taken to deal with the breach, and any measures taken to mitigate the possible effects.

The main reason for notifying individuals of a breach is to enable them to take steps to protect themselves from the effects.

When the decision has been taken to notify the affected individuals, this should be done as soon as possible.

6 Containment and recovery

When a breach is ongoing, every effort must be made to contain the breach. Containment is most likely to be necessary in cases where a breach is caused by a cybersecurity incident, such as phishing.

Recovery takes place after the breach event has ended. This phase includes learning lessons from the breach and putting measures in place to try to avoid any similar breaches occurring in the future.

In the case of simple email breaches (where an email containing personal data has been sent to the wrong individual), recovery will most often consist of requesting that the person or people who received the email in error, delete the email.

Please note that, if an email breach occurs and all the addresses on the email are University addresses, *recalling* the email will not usually work.

Containment and recovery measures should be organised by the DPO/CISM.

Please remember to notify the DPO of the breach *before* trying to recover from it.

7 Consequences of a data breach

Every personal data breach has consequences, to the individual who caused the breach and to the University.

7.1 Individuals

The DPO will always check to see if an individual who has caused a breach is current with their data protection training. If not, the DPO will recommend that the individual complete appropriate training.

Line managers will be notified when one of their direct reports commits a data breach.

Employees who act in breach of this policy repeatedly, or where the data breach is catastrophic, may be subject to disciplinary proceedings if warranted.

7.2 The University

There are a number of possible effects upon the University should we have a reportable data breach.

7.2.1 Reputational damage

Large data breaches are usually reported in national and international media outlets. Such reporting could have an adverse effect on our ability to attract students, and our many academic partners and suppliers could be less likely to want to engage with us.

Actions by the ICO, as described below, will also be publicised.

7.2.2 Actions by the ICO

7.2.2.1 Undertakings

The ICO could issue an undertaking to the University. This is a document which indicates who the controller is, describes the data breach, indicates what representations have been made to the ICO by the controller during the investigation, and specifies what actions the controller must complete to avoid similar breaches. Some or all of the actions may specify a date by which the action must be completed.

All undertakings are followed up, normally within three months. The original undertakings, and the follow-ups, are published on the ICO's website.

7.2.2.2 Enforcement notices

The ICO may choose to issue an enforcement notice in response to a data breach. On occasion, an undertaking may be reissued as an enforcement notice if the controller has not taken the specified actions within the specified time frame. Most often, enforcement notices are issued when the breach is especially serious or has been repeated.

An enforcement notice sets out the legislative framework, the background of the case, the steps which must be taken by the controller (with completion dates), and the consequences of failing to comply with the enforcement notice.

All enforcement notices are published on the ICO's website.

7.2.3 Monetary penalties

The ICO may decide to issue a monetary penalty to the University in consequence of a serious data breach.

7.2.3.1 Standard maximum fine

A fine of up to €10,000,000, or up to 2% of the University's total worldwide annual turnover, whichever is higher, may be issued for failure to:

- comply with an enforcement notice
- to comply with the requirements for offering information society services to a child
- practice data protection by design and default
- comply with the requirements of the GDPR in relation to joint controllers, or processors
- maintain a record of processing activities
- cooperate with the ICO
- implement appropriate technical and organisation measures to ensure the security of personal data
- notify a data breach to the ICO
- notify individuals when their data have been subject to a data breach
- complete data protection impact assessments as required
- consult the ICO prior to implementing a high-risk processing activity
- designate a Data Protection Officer

7.2.3.2 Higher maximum fine

A fine of up to €20,000,000, or 4% of the University's total annual worldwide turnover, whichever is higher, may be issued for failure to:

- comply with the principles
- ensure there is a lawful basis for processing personal data
- comply with the requirements for obtaining consent
- ensure there is a lawful basis for processing special category personal data
- comply with individuals' rights with respect to their personal data
- comply with the requirements for transferring personal data to a third country or international organisation
- comply with an order by the ICO to limit processing of personal data, or an order to suspend the transfer of personal data to a third country or international organisation
- provide access to University premises to the ICO when required

7.2.4 Court action

The ICO can bring an organisation to court if that organisation fails to comply with an enforcement notice.

Any individual who considers his/her rights have been infringed by a controller can seek a judicial remedy against that controller. Individuals can also sue a controller (or data processor) for compensation for damages caused by a data breach.

8 Avoiding a data breach

8.1 Training

Every employee needs to be trained in data protection and information security. There is an online module for each of these, which should be completed *every year* for refresher training. These are available on the Staff Development webpages (https://intra.brunel.ac.uk/s/StaffDev/Modules/Modules.aspx).

Workshops are also available for data protection training. Any employee who has access to staff or student data, including academic staff, should attend at least one workshop while they are employed by the University.

Information security workshops may be scheduled on request to the CISM.

8.2 Information technology solutions

These include

- encryption of documents and laptops
- use of Virtual Private Network (VPN) to access files and folders when off-campus (when using a PC or laptop)
- use of OneDrive to access files and documents (works on any device, including tablets and mobile phones)
- strong passwords
- classification of documents and emails

More information about these can be found on the Cyber 365 page (https://intra.brunel.ac.uk/s/cc/security/Pages/default.aspx#).

8.3 Other solutions

- Attention to detail: this is important whenever one is handling personal data
- Proper email handling – this includes
    - Check the addressees on emails before pressing Send – don't try to guess the individual's email name
    - Use the proper classification
    - If sending an email to many people, especially if any of them have non-Brunel email addresses, use the ***Bcc*** line
    - Emails containing personal data should be sent to the *minimum* number of addressees
    - **Think** before forwarding an entire email thread – do the people to whom you are forwarding it really need to see the whole thing?

    - Take an extra 10 seconds to check every field on the email form before sending it
- A clear desk policy can help avoid inadvertent data breaches
- Check the retention schedules – avoid retaining personal data longer than necessary
- Manual personal data should be kept in a locked location (file cabinet, cupboard or desk) when not in use.

9 References

- Data Protection policies and procedures: https://www.brunel.ac.uk/about/administration/information-access/data-protection

- Information and Cyber Security: https://intra.brunel.ac.uk/s/cc/security/Pages/default.aspx#

- Information Commissioner's Office: https://ico.org.uk
- ICO guidance on Personal data breaches: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

- University Retention and Disposal Schedules: https://intra.brunel.ac.uk/s/GILO/records/Pages/Retention-Schedules.aspx

- Data Protection Act 2018: http://www.legislation.gov.uk/ukpga/2018/12/contents

- General Data Protection Regulation: http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN