Data Breach Reporting Process

Responsibility of:
Approval date:
Review date:
Approved by:

Contents

1. Document Control

1.1. Amendment History

Version	Date	Author	Amendment
0.1	2018-02-14	Graham Hill	First complete draft
1.0	2018-03-20	Graham Hill	Submission to GDPR group
1,1	2018-05-01	Graham Hill	Updated to reflect new guidance from Working Party 29

1.2. Distribution List

This document has been distributed to, and the following should be included in the distribution of any amendments:

- GDPR Group

2. Introduction

The General Data Protection Regulation (GDPR) sets out in Article 33 the requirements for notifying the supervisory authority of a personal data breach, and in Article 34 the requirements for communicating a data breach to affected data subjects. The relevant supervisory authority for the University is the Information Commissioner's Office (ICO).

Failure to meet these requirements puts the University at risk of sanctions, including issuing a warning or reprimand, issuing a compliance order, or issuing fines of up to €10,000,000 or 2% of our annual worldwide turnover.

3. Definitions

Personal data is defined as "any information relating to an identified or identifiable natural person". This means information that is about a specific person who can be identified, either from the data or by combining the data with other information.

A breach of personal data is any security incident that results in personal data being accidentally or unlawfully:

- Destroyed.
- Lost.
- Altered.
- Disclosed to an unauthorised person.
- Accessed by an unauthorised person.

It is important to note that this definition covers not just the usual concern of a loss of confidentiality, but also a loss of integrity or availability. It is possible for there to be a temporary loss of availability. For example, if an unplanned power outage prevents access to the Student Records System for an hour this is a loss of availability, and hence a breach.

4. Responsibilities

All members of UWL staff must report all suspected or possible breaches immediately they learn of them.

The Information Security Manager (ISM) is responsible for maintaining the internal breach register.

The Data Protection Officer (DPO) is responsible for taking the decision to notify the ICO and the data subjects.

All data processors used by the University are responsible for reporting breaches without unnecessary delay. Contracts with data processors should include terms to this effect.

5. Identification of a breach

5.1. Discovery of a possible breach

A possible breach may be discovered in a number of ways:

- By a UWL member of staff, contractor, alumnus, or student.
- By automatic operation of breach detection tools.
- By report from a data processor employed by the University.
- By report from a third party.

Regardless of the means of discovery, the first UWL member of staff to learn about a possible breach must report it immediately.

6.2 Reporting the breach

Reports should be made to the ISM in the first instance. If they are unavailable, the report should be made to the DPO. If neither of these members of staff are available the report should be made to the Chief Information Officer or failing that a member of VCE.

6.3 Confirming the breach

Once a possible breach has been discovered, the University may not immediately have a reasonable degree of certainty that an actual breach has occurred. In this case we are allowed a *short* period of investigation to establish what has taken place.

Once the University has a reasonable degree of certainty that a breach has occurred then:

- We must record and assess the breach. See section 6 below.
- The clock starts on the 72 hour deadline for notifying the ICO.

6. Evaluation of a breach

6.1. Recording the breach

We must record the details of all breaches in the internal breach register. The register will be maintained by the ISM. The register should include:

- what happened
- what data was affected
- what individuals were affected
- what caused the breach
- the effects and consequences
- what we plan to do to mitigate these effects and consequences
- a timeline of the breach, including when we first became aware of the incident and when we determined that it was a breach
- our decisions regarding notification

6.2. Assessing the risk

We must make an assessment of the level of risk posed to the data subjects by the breach. The assessment should consider:

- The type of breach.
- The type of personal data.
- The sensitivity of the personal data.
- The volume of the personal data.
- The number of affected individuals.
- The nature of the processing.
- The ease of identifying individuals. For example, where data was encrypted or pseudonymised, the risk is reduced.
- The severity of consequences for the individuals.
- The permanence of consequences for the individuals.
- Any special characteristics of the individuals. For example, are they children, or vulnerable persons?
- Where there is a breach of confidentiality, the intentions of the persons who have accessed the data.

The assessment should conclude that the beach is either:

- **Unlikely to result in a risk** to the rights and freedoms of natural persons.
- **Likely to result in a risk** to the rights and freedoms of natural persons.
- **Likely to result in a high risk** to the rights and freedoms of natural persons.

The assessment's conclusions should be approved by the DPO.

7. Notification

The assessment of the likely risk determines what notifications are required.

- If the assessment is "**unlikely to result in a risk**" then no notifications are required.
- If the assessment is "**likely to result in a risk**" then notification should be made to the ICO.
- If the assessment is "**likely to result in a high risk**" then notification should be made to both the ICO and the affected data subjects.

Note that the ICO has the power to require us to notify data subjects if they disagree with the assessment of the risk.

7.1. Timing of notifications

Where notification to the ICO or the data subjects is required, it should happen "without undue delay".

In addition, notification to the ICO should happen within 72 hours of our becoming reasonably certain that a breach has occurred. See section 0 above. If we take longer than 72 hours to notify the ICO, we must provide reasons for the delay.

It is acceptable to submit a partial notification to meet the 72 hour deadline and update it later. Such a partial notification should be clear that it is partial, include information about the potential scope of the breach and its consequences, and describe our plans to deal with the breach.

7.2. Use of data processors

If we are the controller of a processing activity, but are using a data processor to do the work, we still have the same responsibilities.

As in section 6.3 above, if a data processor becomes aware of a possible breach they are allowed a short period of investigation to confirm. Once they become reasonably certain that a breach has occurred, they are required by the GDPR to notify us without undue delay.

Note that in such a case the 72 hour clock begins when the University is notified of the breach by the data processor.

7.3. Notification to the ICO

The notification should be made by the Data Protection Officer. The notification should be made without undue delay and within 72 hours of confirmation of the breach. It should include:

- Details of the beach, including the categories and approximate numbers of data subjects and data records involved.
- Contact details for the DPO or some other appropriate contact point.
- The likely consequences of the breach.
- The measures already taken or proposed to address the breach and mitigate possible adverse effects.

As mentioned above, if the notification is made more than 72 hours after we became aware of the breach, we must also provide reasons for the delay.

7.4. Notification to the Data Subject

The notification should be made by the Data Protection Officer.

The notification should be made without undue delay and include:

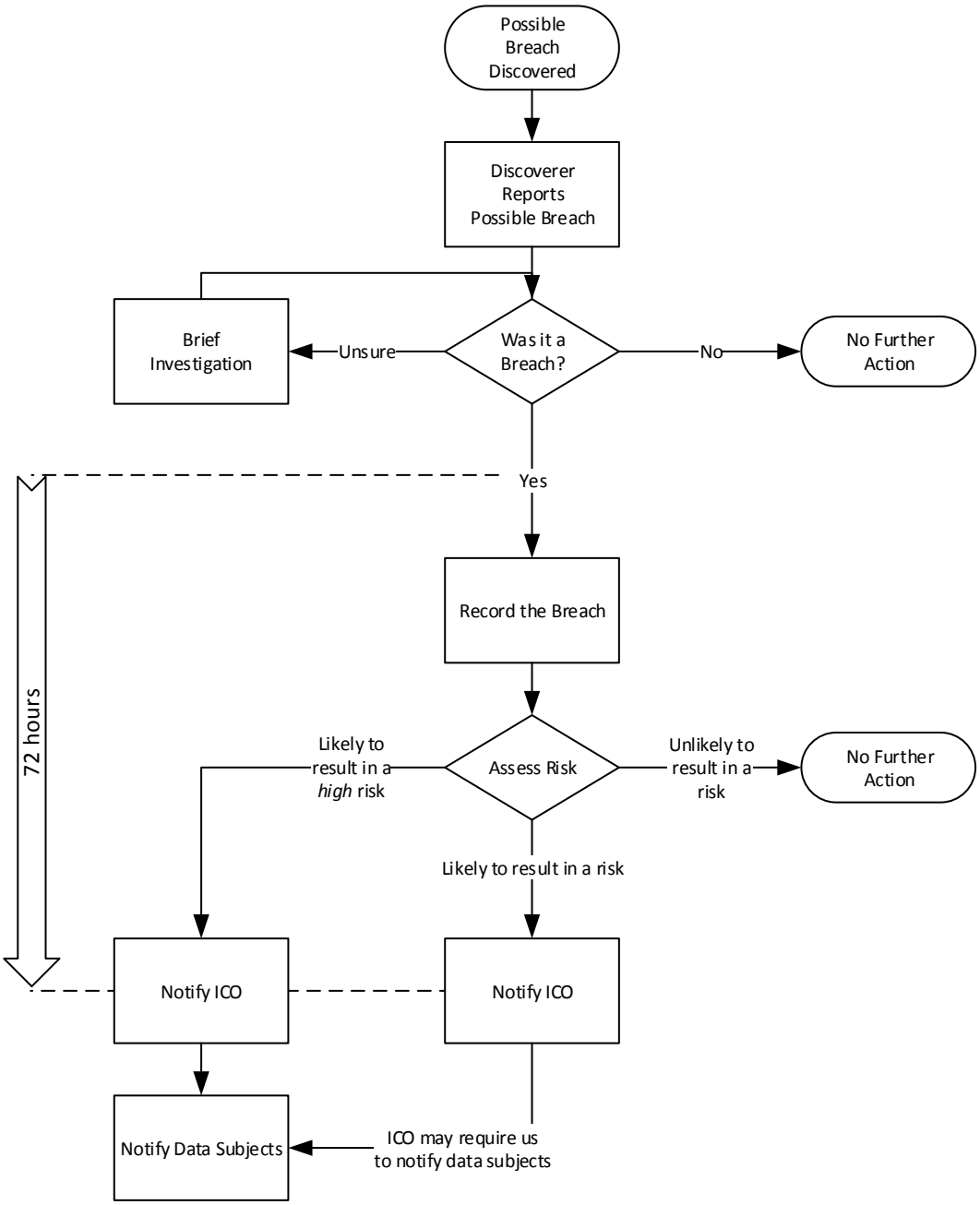
- A description of the breach.
- Contact details for the DPO or some other appropriate contact point.
- A description of the likely consequences for the subject.
- A description of the measures already taken or proposed to address the breach and mitigate its possible effects.

Where appropriate we should also provide advice to the data subjects on steps they can take to protect themselves. The notification should stand alone and not be sent with other information such as in a newsletter. Generally we should choose the communication method or methods we believe will be most effective. If it would be disproportionately difficult to notify each data subject directly then we can do so via a prominent public announcement.

8. For further information

Text of the GDPR	http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
Pre-GDPR guidance from the ICO	https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf
ICO guide to GDPR	https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
ICO news blog	https://iconewsblog.org.uk/2017/09/05/gdpr-setting-the-record-straight-on-data-breach-reporting/
Article 29 Data Protection Working Party guidelines.	http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827

9. Summary


Possible Breach Discovered
Discoverer Reports Possible Breach
Was it a Breach?
Unsure
Brief Investigation
No
No Further Action
Yes
72 hours
Record the Breach
Assess Risk
Likely to result in a *high* risk
Unlikely to result in a risk
No Further Action
Likely to result in a risk
Notify ICO
Notify ICO
Notify Data Subjects
ICO may require us to notify data subjects