St Georges, University of London (SGUL)

Data Incident Investigation Process

1 Introduction

1.1 In accordance with the Data Protection Act 2018 (DPA 18) organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data.

1.2 This document sets out the personal data incident investigation process for SGUL.

2 Personal Data Incidents

2.1 All personal data incidents are reported to the Data Protection Officer (DPO) via the personal data incident on-line form on the staff portal or directly emailed. An incident number will be generated by the DPO who will identify an IAO to take the lead on investigating the breach. The IAO may assign a senior manager to carry-out the investigation on their behalf.

2.2 Personal data incidents will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers.

2.3 The assigned officer is to consider the following:

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise.
- This could be isolating or closing a compromised section of the network, finding a lost piece of equipment/data or simply changing the access permissions.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause.
- As well as the physical recovery of equipment, this could involve the use of back up tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts.
- Where appropriate, in consultation with the DPO and SIRO, inform the police.

2.4 Serious Incidents will be overseen by the DPO, in-conjunction with the Information Governance Manager, who will escalate to the Senior Information Risk Owner as needed.

3 Investigation

3.1 The assigned officer has 10 days in which to complete a data breach investigation report, unless notified any differently, and is to determine the circumstances below for all incidents:

- What data has been compromised
- Whether it has been inappropriately accessed
- How the incident can be contained (limiting or restricting further impact of the incident)
- The risk to data subjects
- How data subjects will be told, or 'notified' of the incident
- How the incident occurred
- Check weaknesses in SGUL processes or procedure which may have led to the incident and what corrective action is required to prevent reoccurrence, this may include:
  - Training
  - Guidance
  - Disciplinary, and
  - Process or guidance that needs to be modified.

4 Assessing the Risk

4.1 Before deciding on what steps are necessary to put in place immediate containment the IAO lead is to assess the risks which may be associated with the incident. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

4.2 The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it?
  - Remember that some data is sensitive because of its very personal nature (health records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
  - What has happened to the data?
  - If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk
  - Regardless of what has happened to the data, what could the data tell a third party about the individual?
  - Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people

- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment

- Who are the individuals whose data has been breached?
    - Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks

- What harm can come to those individuals?
    - Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?

- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?

- If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

5 Response to the incident

5.1 The assigned officer is to, in agreement with their IAO, implement an action plan which will address the following factors, listed in priority order:

- Impact on the data subject
- Impact on normal business operations
- Damage to SGUL reputation
- Prevention of any similar incident
- Recovery of stolen assets
- Disciplining or prosecution of the person or people responsible

6 Notification of breaches

6.1 All organisations have a legal requirement to notify the Information Commissioners Office (ICO) of any significant personal data incident within 72 hours. The SIRO and DPO will lead on whether a notification should be sent to the ICO.

6.2 Informing people and organisations that you have experienced a personal data incident is an important element in breach management. However, informing people about an incident is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

6.3 Answering the following questions will assist the SIRO in deciding whether to notify the ICO:

- Are there any legal or contractual requirements?
- Can notification help you meet your security obligations with regard to protecting personal data?
- Can notification help the individual?
- Bearing in mind the potential effects of the incident, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences, you should advise that the ICO is to be informed.
- Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.
- Have you considered the dangers of 'over notifying'. Not every incident will warrant notification and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.

6.4 The DPO will also need to consider who to notify, what they are going to tell them and how they are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to their decision:

- Make sure the appropriate regulatory body is notified. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data
- There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation
- The notification should at the very least include a description of how and when the incident occurred and what data was involved. Include details of what you have already done to respond to the risks posed by the incident.
- When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what you are willing to do to help them
- Provide a way in which they can contact SGUL for further information or to ask questions about what has occurred – this could be a helpline number or a web page, for example.

6.5 If the decision is notifying the ICO the DPO should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures in place at the time the breach occurred. The DPO should also inform them if the media are aware of the breach so that they can manage any increase in enquiries from the public. The ICO has produced guidance for organisations on the information they expect to receive as part of a personal data incident notification and on what organisations can expect from them on receipt of their notification. This guidance is available on their website: https://ico.org.uk/for-organisations/guide-to-data-protection/ principle-7-security/

6.6 If informing the media, it is useful to inform them whether SGUL have contacted the ICO and what action is being taken. The ICO will not normally tell the media or other third parties about an incident notified to them, but they may advise SGUL to do so.

6.7 Also consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

7 Post event reporting

7.1 The DPO will report on the findings to the Information Governance Steering Group.

7.2 The SIRO may request the risk is be added to the SGUL Risk Register.

7.3 The SIRO, in conjunction with the DPO and Head of IT Services, will analyse the risk to the affected system or process and list the actions to mitigate the risk together with a date for the estimated completion date.

7.4 Any risk that is deemed to be high should be reported to the Executive Board and Dir Governance, Legal & Assurance Services

8 Evaluation and response

8.1 It is important not only to investigate the causes of the incident but also to evaluate the effectiveness of the response to it. Clearly, if the incident was caused, even in part, by systemic and ongoing problems, then simply containing the incident and continuing 'business as usual' is not acceptable; similarly, if SGUL's response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience.

8.2 If it is found that existing procedures could lead to another incident then appropriate IAO will need to identify where improvements can be made. The following points will assist:

- Make sure you know what personal data is held and where and how it is stored. Dealing with a personal data incident is much easier if you know which data are involved.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?
- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice

- Consider whether you need to establish a group of technical and nontechnical staff who discuss ‘what if’ scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions

9 Learning from Personal Data Incidents

9.1 To learn from incidents and improve the response process then incidents, where appropriate, are to be recorded and a Post Incident Review conducted. The following details are to be retained:

- Types of incidents.
- Volumes of incidents and malfunctions.
- Costs incurred during the incidents.
- The information will be collated and reviewed on a regular basis by DPO and any patterns or trends identified.

10 External reporting

10.1 Notification to the Information Commissioners Office

- Although there is no legal obligation within DPA 18 on data controllers to report all personal data incidents which result in loss, release or corruption of personal data its does place a legal obligation that significant incidents in breach of the DPA 18 must be notified to the ICO within 72 hours.

10.2 The nature of the breach can then be considered together with whether the data controller is properly meeting his responsibilities.

10.3 Factors to consider are the volume of data lost, number of records lost, nature of the data lost, and potential impact on the data subjects.

10.4 The decision to notify the ICO will be made by the SIRO.