Data Security Breach Management Policy and Procedure

1. Introduction

1.1 – Intech Centre is committed to ensuring that all personal data we process, including that of colleagues and clients, is managed appropriately and in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) (collectively referred to as "Data Protection legislation")

1.2 - As Intech Centre processes personal data it is committed to ensuring all unauthorised or unlawful processing, loss, destruction of or damage to data (personal data breaches) are swiftly identified and reported within the Centre and, where the Information Commissioner's Office and affected individuals.

1.3 – Senior Manager (Data Protection Officer) may deal with negligent or malicious non-compliance with this policy through the disciplinary process.

1.4 - Under the Data Protection Act 2018 and General Data Protection Regulation, Intech Centre is a Data Controller. This is a "person" who determines the purposes for which and the manner in which any personal data are, or are not to be processed. The sixth Data Protection principle states that organisations, which process personal data, must ensure 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 ('integrity and confidentiality')."

1.5 - As well as defining Intech Centre's policy, this procedure lays out the actions, once a breach has occurred.

1.6 - GDPR standards and ICO guidance will need to continue after the UK leaves the EU. The role of the DPO and need for reporting to the ICO will continue. GDPR will be known as UK GDPR.

2. Scope

2.1 - This policy and procedure applies to all users of Intech Centre's information, data, information systems and the Centre's physical building. It applies to not only staff and members but also where appropriate voluntary staff, consultants and anyone else engaged to work in the organisation and encompasses data, information, software, systems, and paper documents.

2.2 - This policy should be read in conjunction with other relevant policies, including but not limited to:

- Data Protection Policy
- Information Security Policy
- Disciplinary Policy
- Social Media Policy
- Whistle-blowing Policy and Procedure

All staff, including all new starters, must read this policy as this forms part of the Staff Terms and Conditions.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

2.3 - Other useful documents:

- ICO Information Security Guide(link is external)
- ICO Guidance on Personal Data Breaches(link is external)
- Act Now Blog post (link is external)

3. Responsibilities

3.1 - The Senior Manager has overall responsibility for deciding whether to report personal data breaches to the ICO and/or to affected individuals.

3.2 - The Senior Manager has overall responsibility for monitoring compliance with this procedure. He will process incident reports, assess risk and advise the Director accordingly, and liaise with the ICO and the public as appropriate.

3.3 - The Senior Manager has overall responsibility for monitoring compliance with this procedure, as well as the day-to day management of breaches including receiving and processing incident reports and assessing the risk

3.4 – Senior Manager is responsible for ensuring that all staff are aware of their responsibilities to report incidents; for assisting the Senior Manager in his duties through providing all appropriate information and support relevant to an incident; for continuing with appropriate incident management and mitigation.

3.5 - All staff are responsible for immediately reporting any incident or breach affecting personal data held by the Centre.

4. Types of Breach

4.1 - A number of factors could cause data protection breaches. The following is a list of examples but it is not exhaustive and there may be others which will need to be considered at the time of the breach:

- loss or theft of data
- loss or theft of equipment on which data is stored
- inappropriate access controls allowing unauthorised use, both electronic and paper
- equipment failure
- human error in dealing with personal information including both electronic and paper
- unforeseen circumstances such as fire or flood
- hacking attack on the Centre's ICT systems
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it
- unauthorised access into secure areas

5. Notification of Breaches Once Discovered

5.1 - Instances of the loss of personal data are rare in the Centre, however, the consequences to its reputation and the potential impacts on individuals of the loss of personal information means we need to take swift action in the event of a loss.

5.2 - The person who discovers/receives a report of a breach must inform the Senior Manager immediately. Notify any breach discovered outside of normal working hours as soon as is practicable

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

during the next working day however any serious breaches that could cause serious adverse effect or media interest must be reported as a matter of urgency. The contact email address for data protection is **salih@intechcentre.com (link sends e-mail)**

5.3 - The Senior Manager, will then decide whether to involve other departments or a prime contractor.

6. Assessing the Risk

6.1 - The Senior Manager will carry out the initial assessment of the breach on the day it is reported and consider whether the event meets the GDPR definition of a personal data breach.

6.2 - During this initial assessment, a risk assessment of the impact and likelihood of impact on the rights and freedoms of the affected individual's, data subjects, will be undertaken this must be completed within 72 hours of the breach being reported.

6.3 - This will consider the risks to the affected individuals arising from the personal data breach including adverse impact on their:

- Privacy
- Personal financial interests
- Other material damages
- Health and safety
- Emotional wellbeing
- Other non-material damages

6.4 - In considering the risk, the Senior Manager may work with the prime contractor if necessary and required

6.5 - Factors to be considered (these factors are not exhaustive):

- The type of breach
- The nature, volume and sensitivity of the personal data breached
- How easy it is to identify individuals
- The potential consequences for individuals
- Any special characteristics of the data subject (for example they are children or otherwise venerable)

6.6 - Some data security breaches will not lead to risks beyond the possible inconvenience to those who use the data to do their job, for example if a laptop is irreparably damaged or lost, or in line with the Information Security Policy, it is encrypted, and no data is stored on the device. There will be a monetary cost to the Centre by the loss of the device but not a security breach.

6.7 - Whilst these types of incidents can still have significant consequences, the risks are very different from those posed by, for example, the theft of customer data, whereby the data may be used to commit identity fraud.

6.8 - Helpful tips for assessment of risks (these tips are not exhaustive):

- what type of data is involved?
- how sensitive is it? Is it sensitive personal details as defined by the Article 9 of GDPR (e.g. housing benefits) or other data types which are sensitive because of what might happen if it is misused (e.g. bank account details).

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

- if data has been lost or stolen, are there any protections in place such as encryption?
- what has happened to the data?
- can the data be restored or recreated?
- how usable is the lost data?
- if data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates; if it has been damaged, this poses a different type and level of risk
- 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 is 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? Are they staff, customers, clients or suppliers?
- what harm can come to those individuals because of the breach? Are there risks to physical safety or reputation, financial loss, fraudulent use or a combination of these and other aspects of their life?
- are there wider consequences to consider such as a risk to loss of public confidence in one of the service areas?

7. Reporting Personal Data Breaches to the Affected Individuals

7.1 - As part of the risk, consider whether the person/people whose information has been breached should be informed. Inform the person/people concerned, as suggested by guidance from the Information Commissioner unless to inform them will cause additional or undue distress/stress.

7.2 - If the Senior Manager considers the personal data breach a high risk, a report will be provided to the Director including a recommendation on whether to report the breach to the affected individuals.

7.3 - If the Senior Manager decides to notify the individuals, consider the following:

- what is the most appropriate method of communication? Always bear in mind the security of the medium as well as the urgency of the situation
- the notification should include as a minimum, a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach
- give the individuals clear advice on what they should do to protect themselves and what the Centre is willing to do on their behalf
- provide a means of contacting Senior Manager for further information. This could include a named individual, a helpline number, a web page or a combination of all of these.

8. Appointment of Investigator

8.1 - The Senior Manager is responsible for advising services on assessing the impact of any data breach of the Data Protection legislation. This can include recommendations to restore data security.

8.2 - The Senior Manager must consider whether the police need to be informed. This could be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that

illegal activity might occur in the future. If credit card numbers are lost then tell the appropriate bankcard provider.

8.3 - If necessary, consider notifying all staff to prevent additional breaches.

8.3 - The Senior Manager will maintain a log with the details of all breaches. This will include when the breach occurred, who is involved and what action must be taken after the breach.

9. Investigation Procedure

9.1 - Begin investigation immediately on receipt of notification. Complete urgently and wherever possible within 72 hours of the breach being discovered/reported. Carry out, if necessary, a further review of the causes of the breach and recommendations for future improvements once the matter has been resolved

9.2 - The next state, in most cases, would be to investigate the breach by the Senior Manager. The Senior Manager should ascertain whose data was involved in the breach, the person or people responsible for the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation.

9.3 - Breaches will require not just an initial investigation, decision on the severity and containment of the situation but also a recovery plan including, where necessary damage limitation. This will often involve input from all staff. In some cases, contact with external stakeholders or suppliers may be required.

9.4 - The Senior Manager will establish the questions for interviews and then meet with the participants. This could be (but is not limited to or necessarily all of them) witnesses, victims and perpetrators.

9.5 - The Senior Manager will identify if there is a need for expert advice from either professional advisers or Legal Services.

9.6 - Issues to be addressed during the investigation will include:

- the date when the breach occurred
- the date when the breach was identified to Centre and by whom
- the type of data and the number of records involved
- its sensitivity
- the circumstances of the release
- what protection is in place (for example encryption)
- what has happened to the data?
- whether the data could be put to any illegal or inappropriate use
- how many people are affected?
- what group of people has been affected (the public, suppliers etc)
- whether there are wider consequences of the breach

9.7 The Senior Manager will keep an electronic record of all activities during the investigation. This could include the actions taken to mitigate the breach and lessons learnt. The reason for this is that the records may need sharing if there are actions by the police, Information Commissioner's Office, legal proceedings or Audit.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

9.8 There could be a number of investigations going on at any one time for example by ICT.

9.9 If systemic or on-going problems are identified, draw up an action plan to correct. If the breach warrants a disciplinary investigation (for example due to negligence), the Senior Manager should pass on any relevant information to Director who will make the final decision on sanctions against staff.

9.10 The Senior Manager should produce a report for the Director and be written with it in mind that it may be shared with the ICO.

9.11 The report must address the following:

- establish the facts (including those that may be disputed)
- include a chronology of events including the containment, recovery and how the breach has been investigated
- a risk analysis
- a commentary of the weight of evidence
- action to minimise/mitigate effect on individuals involved including whether the victims have been informed
- whether any other regulatory body and been informed and their response
- recommendations to reduce the chance of the same breach happening again

10. Containment

10.1 - At the same time as an investigation is happening, containment and recovery must also happen.

10.2 - The Senior Manager must ascertain whether the breach is still occurring. If so, it must be stopped immediately and minimise the effect of the breach. This will involve liaison with appropriate staff. Examples might be the ICT Manager authorising the shutdown of a computer system or stopping the delivery of electronic mail.

10.3 - Marketing may need telling of a breach if there is a possibility of information published on the Internet or the press told and their assistance is required in managing a media response.

11. Reporting Personal Data Breaches to the Information Commissioner's Office

11.1 -The GDPR places a duty on all organisations to report certain types of data breach to the Information Commissioner's Office

11.2 - In the case of a personal data breach, the Centre shall without undue delay and, where feasible, no later than 72 hours after becoming aware of breach, notify the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual. A reason for the delay, if notification is not within 72 hours, is required along with the notification.

11.3 - The GDPR states that a personal data breach must be reported to the ICO if the breach is likely to result in a risk to the rights and freedoms of the individuals concerned. By this, it means discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. It also requires that this be on a case-by-case basis. There is no need to notify the ICO if there is not a risk to persons' rights and freedoms.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

11.4 - After carrying out a full assessment of the risk, the decision as to whether or not to inform the ICO would normally rest with the Senior Manager.

11.5 - The Senior Manager will also need to consider whether any officer concerned with the breach will be subject to disciplinary procedures.

11.6 - Providing all information may not be possible in the initial response but it should contain the minimum recorded in the log. Use either the online reporting tool or via the telephone. Failing to notify a breach when required to do so can result in a fine up to €10 million.

12. Review

12.1 - A policy review will take place after a serious breach or after legislative changes, important changes in case law or guidance.

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com