Gendered Intelligence

Data Breach Security Procedure (DBSP)

1. Introduction
Gendered Intelligence is committed to being open and transparent about its data processing, and meeting its obligations under the General Data Protection Regulation (GDPR). Our overall approach is outlined in the Data Protection Policy (DPP) which can be found on our website at www.genderedintelligence.co.uk. Jay Stewart, CEO, is the Named Representative in relation to data protection and any questions should be addressed to him at jay.stewart@genderedintelligence.co.uk.

This document explains what Gendered Intelligence will do in the event of a breach of our data security.

Gendered Intelligence is committed to taking appropriate measures against unauthorised or unlawful processing of data and against accidental loss, destruction of or damage to personal data.

2. Definitions
For definitions of personal data and special categories of data please see the DPP.

A data security breach is considered to be, and can happen for a number of reasons, namely:

- Loss or theft of data in hard copy format, or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- 'Blagging' or "Phishing" offences where information is obtained by deceiving the organisation who holds it.

3. Risks
Data security breaches will vary in impact and risk depending on the content and quantity of data involved, the circumstances of the loss and the speed of response to the incident.

The risks for Gendered Intelligence include:

- significant reputational risk;
- rectification costs in dealing with the breach, including staff time;
- potential fines imposed by the Information Commissioners' Office (ICO) - up to 4% of turnover.

The risks for the Data Subject can vary from negligible to severe, depending on the nature of the data that is lost or stolen, and, for example, whether the data is subsequently made public or used for illegal purposes, such as identity fraud. All breaches will be treated

seriously and appropriate procedures followed as GI cannot decide without following due process what the potential impact for the Data Subject(s) will be.

4. Security Breach Management Plan

The following procedure outlines the four main stages in managing a breach and will help ensure that all breaches are dealt with effectively and efficiently. The individual stages may run concurrently.

i) Containment & recovery

As soon as a data security breach has been detected or is suspected the following steps should be taken:

a) Identify who should lead on investigating and managing the breach
b) Establish who (within GI) should be aware of the breach – the CEO/ Named Representative must be contacted
c) Identify and implement any steps required to contain the breach
d) Identify and implement any steps required to recover any losses and limit the damage of the breach
e) If appropriate inform the Police/Insurance Company

ii) Assessment of risk & action plan

All data security breaches must be managed according to their risk. Following the immediate containment of the breach, the risks associated with the breach should be assessed in order to identify an appropriate response. The checklist in Appendix A should be used to help identify the exact nature of the breach and the potential severity. This information can then be used to establish the action required.

iii) Notification of breach

The Information Commissioners Office **must** be informed of the Breach, within 72 hours of the breach being identified. They will advise what other action is to be taken.
GI must also decide which other individuals or organisations should be notified of the breach. This will depend on the nature of the breach. Any notification must be carefully managed; do not disclose information before the full extent of the breach is understood; and when disclosure is required ensure that it is clear, complete informative. The checklist in Appendix B should be used to identify who should be notified and to establish what information should be disclosed. The CEO or other member of the Management Team must be involved in the notification process and no message should be sent without the CEO's approval. The Information Commissioner's Office should be notified only after liaison with the CEO or Board.

iv) Evaluation and response

It is important to investigate the causes of the breach and evaluate GI's response to the breach. A brief report on the breach, summarising how it was dealt with; providing recommendations on how to prevent the breach reoccurring; and reviewing similar risks should be written. The documents created by completion of Appendices A-C should be used to inform this evaluation, and may be included as appendices to the report.

5. Record Keeping
Throughout the breach, records should be kept of what action has been taken and by whom. Appendix C provides an activity log template to record this information. In addition, copies of any correspondence relating to the breach should be retained.

If there are recommended changes to this procedure, such as additional information that would have been helpful or further explanation required, these should be communicated to the CEO.

Document review process
Version: 1.0
Draft approved for circulation: May 2018
Board approval due: July 2018
Review Due: July 2020

Appendix A: Security Breach Initial Risk Assessment Checklist

a) What is the nature of the breach? (This information should be as detailed as possible covering what has happened e.g. theft/unauthorised access)
b) How did the breach occur?
c) What type of data is involved? (The individual data fields should be identified e.g. name, address, bank account number, photos)
d) How many individuals or records are involved?
e) If the breach involved personal data, who are the individuals? (Staff, Service Users, Clients etc.)?
f) What has happened to the data?
g) Establish a timeline. (when did the breach occur, when was it detected, who detected the breach, when was the breach isolated? etc.)
h) Were there any protections in place? (e.g. Encryption)
i) What are the potential adverse consequences for individuals or for Gendered Intelligence? How serious or substantial are they and how likely are they to occur?
j) What could the data tell a third party about an individual, what harm could this cause? What commercial value does the information have?
k) What processes/systems are affected and how? (e.g. web page taken off line, access to database restricted).

A full written report covering the above points must be produced and should be dated and timed.

Appendix B: Notification of Breach Checklist

Who to Notify

Internally

1. The CEO and Named Representative for Data Security
2. The Chair of the Board
3. The Public Engagement Lead or other individual responsible for GI's Press coverage

Externally

4. Police – in the case of criminal activity
5. Information Commissioner's Office (ICO) - there is a legal obligation to inform the ICO **as soon as possible but must be within 72 Hours**
6. Individuals whose data has been compromised
7. Other regulatory bodies, funders, clients as appropriate
8. Others – e.g. banks where steps may be required to protect accounts

The CEO or Named Representative for Data Security must be informed first and as soon as possible. They will notify the ICO and make the decision about further actions in conjunction with the ICO.

Media - what to say

The CEO will be able to advise on the content of any notification. No statement to the media should be made without CEO approval.

It is important that the extent of the breach is understood prior to any statement, in order that useful information is provided. However if there are important steps that individuals need to take, this should be communicated promptly.

Consider including the following:

- Details of what happened and when the breach occurred
- What data was involved
- The ICO has been informed
- What steps have been taken to contain the breach and prevent reoccurrence
- Advice on what steps they should take e.g. contact banks
- How will you help and keep them informed (if necessary)
- Provide a way to be contacted

Appendix C: Data Security Breach Activity Log

DATE/TIME	ACTIVITY	ACTION TAKEN	OWNER	TIME COMPLETED