ENGAGING NETWORKS

DATA BREACH MANAGEMENT POLICY FOR STAFF MEMBERS

Last updated: April 2020

Under the General Data Protection (GDPR) and the Data Protection Act 2018, a personal data breach may need to be notified to our clients or directly to the Information Commissioners Office and the people affected by the breach. Engaging Networks collects, processes and stores significant volumes of personal data daily. We are therefore, obliged under these laws to keep personal data safe, secure and to respond promptly and appropriately to data security breaches. It is vital to take prompt action in the event of any actual, potential or suspected breaches of data security or confidentiality. This will help us to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the company.

What is a data breach?

The purpose of this document is to help you report and manage data security breaches. It applies to everyone who handles Engaging Networks data and the personal data help in databases belonging to our clients. This includes those who are directly and indirectly employed by Engaging Networks. Failure of any staff member or agent to comply with this policy may lead to disciplinary action being taken. Do not assume that someone else has already reported the breach. Always take steps to report it.

Personal data security breaches can happen for several reasons, including:

- the disclosure of confidential data to unauthorised individuals;
- loss or theft of data or equipment on which data is stored;
- loss or theft of paper records;
- inappropriate access controls allowing unauthorised use of information;
- suspected breach of Engaging Networks' IT security and Acceptable Use policies;
- attempts to gain unauthorised access to computer systems, e.g. hacking;
- records altered or deleted without authorisation by the data owner;
- malware or other security attacks on IT equipment systems or networks;
- breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information
- confidential information left unlocked in accessible areas;
- leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information;
- emails containing personal or sensitive information sent in error to the wrong recipient;
- unforeseen circumstances such as a flood or fire which destroys information.

Reporting

All personal data security incidents (including suspected incidents) must be reported without delay. Once you discover a breach, report it to your line manager so they can fill the form below with your input. This form is essential for regulatory reporting requirements, it must be filled out fully and it is your responsibility to work with your manager to find all required information to the best of your ability. It will be used by the Data Protection Officer (DPO) to assess the severity of the breach and will be added to the company log of data breaches.

You must always handle personal data with care and respect and protect the privacy and confidentiality of the information.

The DPO will assess the breach and decide on the next steps to be taken. Personal data security breaches also require a long-term recovery plan. This will be composed by various members of Engaging Networks management team.

The process of recording starts once the breach has been detected, with the procedure being run in the following five-step process:

1. **Identify and Classify**

Once you think a breach has taken place, report it immediately to your line manager who will notify the DPO. Try and outline the facts of the incident as clearly as possible:

- what personal data is involved in the breach;
- the cause of the breach;
- the extent of the breach (how many people are affected);
- any potential harm to those people that the breach might cause;
- how you think the breach can be contained.

Once you have done this, the incident will be taken over by an investigation team, who will:

2. **Contain and Recover**

The line manager (or lead investigator) and DPO will take any further steps required. These steps will include making other relevant staff members aware of the incident. Investigate whether there can be a recovery of losses and limit the damage of the breach if possible. They will also decide if the people affected need to be notified.

3. **Assess the Risks**

Fully assess risks, this includes the risks to the individual and the company. Decide on any remedial steps.

4. **Notify**

The DPO and others involved in the investigation of the breach will decide whether the incident needs to be reported to the ICO and others. The DPO will consider who to notify, what the message must be, how to communicate this message and define the reason for the notification.

5. **Evaluate Actions**

This stage involves a review of the actions taken. This will be in consultation with all relevant stakeholders. The breach will be included in the central record (log) of data security incidents.

EXAMPLES OF PERSONAL DATA BREACHES

Example	Notify the Commission?	Notify the data subject?	Notes/Recommendations
Engaging Networks suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the ICO, if there are potential consequences to individuals as this is a loss of availability. As Engaging Networks processes special categories of data Engaging Networks needs to ensure there are no legal consequences for individuals	Yes, report to individuals, depending on the nature of the Personal data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or confidentiality. However, the supervisory authority may consider an investigation to assess compliance with the broader security requirements under Art. 32 of GDPR "Security of Processing".
Engaging Networks identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, we must notify our affected clients (the controllers) without undue delay. We will have conducted our own investigation so the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by Engaging Networks (the processor). The client then must notify the ICO.	If there is likely no high risk to the individuals they do not need to be notified.	We must consider any other notification obligations (e.g. under the Directive on security of network and information systems). If there is no evidence of this vulnerability being exploited with this particular controller a notifiable breach may not have occurred but is likely to be recordable or be a matter of noncompliance under Art. 32 of GDPR "Security of Processing".
Engaging Networks stored a backup of an archive of personal data encrypted on a CD. The CD is stolen during a break-in.	No.	No.	As long as the data is encrypted with a state-of-the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However, if it is later compromised, notification is required.

Personal data of individuals are exfiltrated from a secure website managed by Engaging Networks during a cyber-attack.	Yes, report to ICO if there are potential consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the potential consequences to individuals is high.	
A direct marketing e-mail is sent to recipients in “to:” or “cc:” field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of Personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.

PERSONAL DATA SECURITY BREACH REPORT FORM

Please act promptly to report any data security breaches. If you discover a data security breach, please notify your manager immediately. Managers complete Section 1 of this form and email it to the Data Protection Officer at dpo@engagingnetworks.net

Section 1: Notification of Personal data Security Breach	**To be completed by Head of Department/Function of person reporting incident**
Date incident was discovered:	
Date(s) of incident:	
Place of incident:	
Name of person reporting incident:	
Contact details of person reporting incident (email address, telephone number):	
Brief description of incident or details of the information lost:	
Number of Data Subjects affected, if known:	
Has any personal data been placed at risk? If, so please provide details	
Brief description of any action taken at the time of discovery:	
For Office Use	
Received by:	
On (date):	
Forward for action to:	
On (date):	
Section 2: Assessment of Severity	**To be completed by Data Protection Officer**
Details of the IT systems, equipment, devices, records involved in the security breach:	

Details of information loss:	
What is the nature of the information lost?	
How much data has been lost? If laptop lost/stolen: how recently was the laptop backed up onto central IT systems?	
Is the information unique? Will its loss have adverse operational, research, financial, legal liability or reputational consequences for Engaging Networks or third parties?	
How many data subjects are affected?	
Is the data bound by any contractual security arrangements?	