MRC Print Limited Data Breach Policy And Reporting

Version: 1.0
Date: 24th May 2018
Author: MRC Print Limited

Data Breach Policy

Background

As an organisation we store, process, and share a large amount of personal information. Data is a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage or detrimental effect on the organisation.

Aim

We are obliged under the Data Protection Act and the GDPR to have a process in place designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

Scope

This policy relates to all personal and sensitive data held by the organisation regardless of format.

This policy applies to everyone at this organisation. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the organisation.

Definition/Types of breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action that may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes but is not restricted to, the following

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system
- Unauthorised disclosure of sensitive/confidential data
- Website defacement
- Hacking attack

- Unforeseen circumstances such as a fire or flood
- Human error
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it

Reporting an incident

Any individual who accesses, uses or manages information is responsible for reporting data breach and information security incidents immediately to the appropriate manager using the form attached.

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. All staff should be aware that any breach might result in disciplinary procedures being instigated.

Containment and Recovery

Appropriate steps must be taken immediately to minimise the effect of the breach. An initial assessment will be made to establish the severity of the breach and to establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The investigation will need to take into account the following

- The type of data involved
- Any sensitivity
- The protections that are in place (e.g. encryptions)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to any illegal or inappropriate use
- Who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the breach

Notification

Management shall determine who needs to be notified of the breach. Every incident will be assessed on a case-by-case basis; however, the following will need to be considered.

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected – could they act on the information to mitigate risks

- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Would notification help the company meet its obligations under the seventh data protection principle;
- If a large number of people are affected, or there are very serious consequences
- Whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/media/1536/breach_reporting.pdf

All suspected and actual breaches should be recorded on the appropriate log to facilitate further evaluation and breach avoidance activity.

The dangers of over notifying

Not every incident warrants notification and over notification may cause disproportionate enquiries and work. Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves, and include what action has already been taken to mitigate the risks. Individuals will also be provided with information on what has occurred.

Evaluation and response

Once the initial incident is contained, the organisation will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. Existing controls should be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

Data Breach Reporting Form

The following form should be used to report/record a data breach:

Notification of Data Security Breach	To be completed by 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 use by the Data Protection Officer or Management
Received by
On (date)
Forwarded for action to
On (date)

Data Breach Form Letter

Dear

Sadly, it has come to our attention that a breach in our processing system has exposed items of your personal data to *unauthorised external parties/unlawful processing*. As an immediate course of action we have notified the ICO (Information Commissioner's Office) and the relevant law enforcement agency. If needed, we will work with cyber security experts, forensic examiners and legal counsel to ensure everything is being done to minimise further exposure.

What happened?

At time of writing, we believe the following timeline of events to have taken place leading to the reported breach.

- *List the timeline of events contributing to the breach event. There is no requirement to expose sensitive information about the organisation unless it is crucial in describing the breach.*

The following items of personal data were involved

- *List the types of personal data. For example, first name, surname and DOB*

What this means for you

Considering the nature of the breach and the types of personal data involved in the breach, we believe the consequences to you are as follows

- *Try to list any personal actions the data subject will need to take. e.g will they need to change their password or seek legal advice. The ICO would like to see the data controller taking the lead when it comes to repairing or containing damage.*

How we will stop this happening again?

In order to prevent such a breach taking place again and to minimise the impact on our customers, we have started to take the following steps.

- *List the actions your organisation is taking to ensure that this breach is not repeated. Again, this does not need to compromise the organisations' confidentiality but should be as reassuring to data subject as possible*

Please note, we will not send further email updates about this incident. All future updates in regards to this security breach can be found on our website at: www.mrcprintltd.co.uk. Any emails you receive about this security incident should be treated as suspicious.

We apologise wholeheartedly for this breach of security, but please be assured that we are doing

everything in our power to ensure that the damage is mitigated and that this doesn't happen again in the future. For further information please contact Lisa Briggs at lisa@mrcprintltd.co.uk.

Breach Log Template

Complete the following table to track data breach events.

Breach Number	Date Received	Data Subject Impact	Breach Contained	Breach Reported To ICO	Data Subjects Informed

End of document.