Morson Group

Data Breach Policy

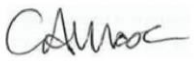
MG | HR | POL | 023

Issue 2 – Aug 2020

Contents

Document Control

Morson Reference:	MG/HR/POL/023
Title:	Data Breach Policy
Version:	2
Date:	August 2020
Prepared For:	HR
Classification:	INTERNAL

	Name	Signature	Date
Created By	Joseph Mason		21/08/2020
Checked By:	Phil Beardwood		21/08/2020
Q/A Approval:	Gareth Morris		21/08/2020
MG Approval:	Ged Mason		21/08/2020

Introduction

This document provides guidance across the Morson Group which includes Morson Human Resources Limited, Morson Projects Limited, Vital Human Resources Limited, Morson Cyber Securities Limited and the Bridge Limited (individually and collectively referred to as the Group) in respect to dealing with data protection breaches.

This policy applies to all employees, workers, contractors, agency works, consultants, directors and members ("Staff").

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to prevent further breaches.

The Morson group is required under data protection laws to ensure the security, interests and categories of confidentiality of all the personal and special personal data it processes including that processed by third parties on its behalf. Every care should be taken by Staff to protect the personal data they work with and to avoid the unauthorised disclosure or loss of personal data.

This policy applies to all personal and special personal data processed by the Morson Group or anyone acting on behalf of the Morson Group.

Legislative Framework

There are seven data protection principles contain in the data protection legislation which must be complied with when processing personal data. Failure to comply with any of these principles is a breach of the legislation.

This policy is concerned with the sixth data protection principle:

"Personal Data shall be processed in a manner that ensures 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."

Examples of a breach of this principle would include:

- personal data accidentally being sent to someone (either internally or externally) who does not have a legitimate need to see it;
- databases containing personal data being compromised, for example being illegally accessed by individuals outside the Morson Group;
- loss or theft of laptops, mobile devices, or paper records containing personal data;
- paper records containing personal data being left unprotected for anyone to see, for example:
  - files left out when the owner is away from their desk and at the end of the day;
  - papers not properly disposed of in secure disposal bins that can then be extracted or seen by others;
  - papers left at photocopying machines;
- Staff accessing or disclosing personal data outside the requirements or authorisation of their job;
- being deceived by a third party into improperly releasing the personal data of another personal; and
- the loss of personal data due to unforeseen circumstances such as a fire or flood.

The difference between a security breach and a data breach and the notification process to follow

A data breach relates to the loss of personal data and should be notified following the procedure described. A security breach relates to the loss of equipment containing personal data. Where a security breach has been notified that also involves personal data Staff must also follow the data breach policy.

Action to be taken in the event of a data breach

On discovery of a breach the following actions should be taken:

- Reporting an incident;
- Containment and recovery;
- Investigation and risk assessment;
- Notification of breach to the Information Commissioner's Office (ICO);
- Evaluation and response;

Reporting an incident

The member of Staff committing the breach is responsible for reporting any data breach and information security incidents immediately to the Compliance and Assurance Director (at **phil.beardwood@morson**.com and copy in **gdpr@morson.com**) and IT Services (at **ITsupport@morson.com**).

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

The report must 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 (refer to Appendix 1).

All Staff should be aware that any breach of data protection legislation may result in the disciplinary procedure being instigated.

Containment and Recovery

The Compliance and Assurance Director (CAD) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

Where personal data has been sent to someone not authorised to see it, the manager of Staff/the CAD should:

- tell the recipient not to pass it on or discuss it with anyone else;
- tell the recipient to destroy or delete the personal data and to confirm in writing they have done so; and
- warn the recipient of any implications if they further disclose the data;

An initial assessment will be made by the CAD in liaison with relevant Staff to establish the severity of the breach and who will take the lead investigating the breach, as the Lead Investigation Officer (LIO)(this will depend on the nature of the breach; in some cases it could be the CAD).

The LIO will establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The LIO or the CAD will establish who may need to be notified as part of the initial containment and will inform the police, where appropriate.

Investigation and risk assessment

An investigation will be undertaken by the LIO immediately and wherever possible, within 24 hours of the breach being discovered/reported.

The LIO will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved;
- its sensitivity;
- the protections that are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen);
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- where there are wider consequences to the breach.

Notification

The LIO and/or the CAD in consultation with relevant colleagues will establish whether the Information Commissioner's Office will need to be notified of the breach, and if so, notify them within 72 hours of becoming aware of the breach, where feasible.

Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- whether the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms under data protection laws;
- whether notification would assist the individual(s) affected (e.g. could they act on information to mitigate risk?);
- whether notification would help prevent the unauthorised or unlawful use of personal data;
- whether there are any legal/contractual notification requirements;

- the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adversely affecting that individual's rights and freedoms, will be informed without undue delay. Notification 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 a way in which they can contact the Morson Group for further information or to ask questions on what has occurred.

The LIO and/or the CAD must consider notifying third parties such as the police, insurers, banks or credit card companies. This would 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.

The LIO and/or the CAD will consider whether the Communications Team should be informed regarding a press release and to be ready to handle any incoming press enquiries.

A record will be kept of any personal data breach, regardless of whether notification was required.

Evaluation and response

Once the initial incident is contained, the CAD will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to the systems, policies and procedures should be undertaken.

Existing controls will be reviewed to determine their adequacy, and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

The review will consider:

- where and how personal data is held and where and how it is stored;
- where the biggest risks lie including identifying potential weak points within existing security measures;
- whether methods of transmission are secure; sharing minimum amount of data necessary;
- Staff awareness;
- Implementing a data breach plan and identifying a group of individuals responsible for reacting to reported breaches of security.

If deemed necessary, a report recommending any changes to systems, policies and procedures will be considered by the Board.

Policy Review

This policy will be updated as necessary to reflect the best practice and to ensure compliance with any changes or amendments to relevant legislation.

Appendix 1

DATA BREACH REPORT FORM

Please act promptly to report any data breaches. If you discover a data breach, please notify your Line Manager immediately, complete Section 1 of this form and email it to the Compliance and Assurance Director (**phil.beardwood@morson.com** & **gdpr@morson.com**) and IT Helpdesk (**ITsupport@morson.com**) where appropriate].

Notification of Data Security Breach	**To be completed by person reporting incident**
Date of report:	
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, when, what, who:	
Type and amount of personal data:	
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 Compliance and Assurance Director	
Received by:	
On (date):	
Forward for action to:	
On (date):	

Amendments Record

Issue No	Issued by	Issue Amendments	Date
1	Phil Beardwood	First Issue No Changes	August 2018 August 2019
2	Joseph Mason	Rebrand	August 2020