Risk Assurance Management Ltd

Data Breach Policy

Sam Corby
Operations Director

Revision 1
May 2018

Risk Assurance Management Limited

Risk Assurance Management Limited is authorised and regulated by the Financial Conduct Authority

Registered Address:
23a Picton House, Hussar Court, Waterlooville, Hampshire PO7 7SQ
Registered in England and Wales No: 1334065

Chancery House, Leas Road,
Guildford, Surrey GU1 4QW
Tel: 0370 7200 780
Email: group.risk@ram-ltd.co.uk
Web: www.ram-ltd.co.uk

Contents

Overview 3
What Constitutes a Data Breach? 3
Breach Detection Measures 3
When and Who Should a Breach be reported to? 4
How will we investigate a Data breach? 4
When a Breach will be notified to the Information Commissioner 4
Who will we notify of a Breach? 5

Overview

We are aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

All staff members are responsible for maintaining Risk Assurance Management Limited (RAM)'s Data Protection Policy and reporting of any breaches of that policy.

What Constitutes a Data Breach?

The accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed whether deliberate or accidental. Examples of breaches include;

- Access by an unauthorised third party; including computer hacking by an external entity
- Loss of data through theft of equipment or paper records
- The incorrect sending (or access) of data to an unrelated party (e.g. accidently emailing the wrong person with sensitive data or allowing 3rd parties to access data on company computers or websites).
- Loss of data in transit to a 3rd party by staff or courier services including loss of information in the postal system
- Portable devices containing personal data being lost or stolen;
- Alteration of personal data without permission;
- Loss of availability of personal data
- Unauthorised access of data by staff (e.g. accessing personnel files or salary records).

The examples given are not exhaustive but should give a pointer to the types of data breach that could occur and needs to be reported.

Breach Detection Measures

We have implemented the following measures to assist us in detecting a personal data breach:

- Training staff on how to identify fraudulent requests for data and proper procedures for protecting data.

- Auditing our staffs' access to IT systems.
- Auditing staffs' access to personal data, with automatic alarms if suspicious activity is identified.
- Monitoring and logging of Web and Email Access
- Antivirus and monitoring of suspicious activity on personal computers.

When and Who Should a Breach be reported to?

Any breaches (or suspected breaches) should be reported immediately to RAM's Data Controller who will take appropriate action.

How will we investigate a Data breach?

RAM's Data Controller will carry out the following:

- Assess the reported data breach
- Decide the severity of the breach
- Decide if RAM needs to notify the Information Commissioners Office
- Notify the Broker of the scheme
- Decide if RAM needs to notify any affected individuals
- Decide if RAM needs to notify the Trustees of the scheme

When a Breach will be notified to the Information Commissioner

In accordance with the GDPR, we will undertake to notify the Information Commissioner of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's rights and freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

The Information Commissioner will be notified without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale we will make an initial report to the Information Commissioner and then provide a full report in more than one instalment if so required.

Who will we notify of a Breach?

In accordance with the GDPR we will undertake to notify the individual whose data is the subject of a breach if there is a high risk to people's rights and freedoms. A high risk may be, for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details where more information can be obtained
c) a description of the likely consequences of the personal data breach and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Where we do not hold the applicable details to notify the individual directly, we will notify the Trustees of the Scheme detailing the above points and request that they notify the affected individuals immediately on our behalf.

In accordance with our Terms of Business Agreements with Intermediaries we will notify the Intermediary of any data breach affecting a mutual client. The notification will include a copy of the notification to the affected individuals.