DATA PROTECTION POLICY

VERSION 1.4 OCTOBER 2018

REED & MACKAY

CONTENTS

POLICY STATEMENT

The Board of Reed & Mackay recognise the significance of protecting data and for compliance with our data protection obligations.
Our priorities are:

- Adherence to the data protection regulations and principles
- Protection of our reputation and brand
- Continuity of our business and income streams

Adherence to the Data Protection is achieved through holding regular risk reviews where vulnerabilities and threats are identified and assessed and putting appropriate controls in place to minimise the risk. These controls are continuously monitored, reviewed and improved, where necessary, to ensure that compliance needs are met. Reed & Mackay is committed to continual improvement of the management of data.

Reed & Mackay obtains, keeps and uses personal information (also referred to as data) for a number specific lawful purposes, as set out in the Privacy Notice on the Reed & Mackay website.

Personal information is subject to certain legal safeguards and restrictions on its use.

POLICY SCOPE & COMPLIANCE

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to clients and suppliers. For data protection obligations relating to employees, please refer the Employee Data Projection Policy in R&M People.

The Resilience Working Group is responsible for identifying relevant statutory, regulatory and contractual requirements that the company must adhere to, and through compliance to these Reed & Mackay will demonstrate confidence, integrity and credibility both internally and externally.

All employees and contractors working for, or on behalf of Reed & Mackay are responsible for complying with this policy. Failure to comply with the policy puts at risk the individuals whose personal information is being processed; carries the risk of significant civil and criminal sanctions for the individual and Reed & Mackay; and may amount to a criminal offence by the individual. Wilful or negligent disregard of this policy will be investigated and may be treated as a disciplinary offence. If you do not understand the implications of this policy or how it may apply to you, seek advice from the Head of Governance, Risk Management and Compliance.

PURPOSE

Reed & Mackay have created a Data Protection Policy to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work; and to set a clear direction, demonstrate support for, and commitment to the management of data throughout the company.

The objectives are:

- To help you understand what the law requires and how Reed & Mackay expects you to deal with data in order to comply with the law.
- To offer assurance about how Reed & Mackay is committed to the protection of data for our employees, clients, suppliers and others.
- To manage the risk of serious financial loss, loss of client confidence or other serious business impact which may result from a failure in compliance with regulations and principles.
- To identify and support improvements to the way data is handled throughout the organisation.
- To comply with all relevant regulatory, contractual and legislative requirements and obligations.

DEFINITIONS

Data is information which is stored electronically on a computer or in certain paper based filing systems

Personal Data means any information relating to a living individual who can be identified from that information (of from that information and other information in our possession). Personal information can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal)

Data subjects include all living individuals about whom we hold personal information. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information

Data controllers determine the purpose for which and the manner in which any personal information is processed.

Data processors process personal information on behalf of a data controller.

Data users include employees whose work involves using personal information. Data users have a duty to protect the information that they handle by following our data protection and security policies at all times.

Processing means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it.

Sensitive personal information (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

Note: with respect to Reed & Mackay's client contractual relationships the client is the data controller of client personal information and Reed & Mackay is the processor of client personal information.

DATA PROTECTION PRINCIPLES

Reed & Mackay will comply with the following data protection principles when processing personal information –

- processing personal information lawfully, fairly and in a transparent manner
- collecting personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes
- process the personal information that is adequate, relevant and necessary for the relevant purposes
- keeping accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;
- keeping personal information, in a form which permits identification of data subjects, for no longer than is necessary for the purposes for which the information is processed
- taking appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage

BASIS FOR PROCESSING PERSONAL INFORMATION

The purposes for which Reed & Mackay uses personal data and the lawful basis for that processing is described in the Privacy Notice which can be found on the Reed & Mackay website.

PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where Reed & Mackay is planning to use a new form of technology), we will carry out a Data Protection Impact Assessment (DPIA) to assess –

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals
- what measures can be put in place to address those risks and protect personal information.

Reed & Mackay's Project Framework identifies the requirement to perform a DPIA for projects that have an impact on personally identifiable information (in addition to carrying out an Information Security Assessment for projects that deliver a technology solution, or have an impact on the availability, integrity and confidentiality of information).

The result of these assessments is used to help embed privacy and security in the design and delivery of the solution.

INDIVIDUAL RIGHTS

Individuals have the following rights in relation to their personal information –

- to be informed about how, why and on what basis that information is processed
- to obtain confirmation that their information is being processed and to obtain access to it by making a Subject Access Request
- to have data corrected if it is inaccurate or incomplete

- to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten')

Any client wishing to understand how their information is being processed should be referred to the Privacy Notice on the Reed & Mackay website.

Any requests from clients to exercise the other rights above should be referred to the relevant Account Manager assigned to the client's account, so that they can direct the queries to the authorised person in the client's organisation. The Account Manager is responsible for verifying the identity of the individual before processing the request.

Employees wishing to exercise their individual rights should refer to the Employee Data Protection Policy in R&M/People.

INDIVIDUAL OBLIGATIONS

Employees may have access to the personal information of other members of in the course of their employment or engagement. If so, Reed & Mackay expects those employees to help meet data protection obligations to those individuals. For example, employees should be aware that those individuals may also enjoy the rights set out above.

If employees have access to personal information, they must –

- Only access the personal information that they have authority to access, and only for authorised purposes.
- Only allow other Reed & Mackay staff to access personal information if they have appropriate authorisation.
- Only allow individuals who are not Reed & Mackay staff to access personal information if the employee has specific authority to do so.
- Keep personal information secure (e.g. by complying with policies regarding access to premises, computer access, password protection and secure file storage and destruction and other precautions as part of Reed & Mackay's Information Security Policy.
- Not remove personal information, or devices containing personal information (or which can be used to access it) from Reed & Mackay premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device.
- Not store personal information on local drives or on personal devices that are used for work purposes and comply with Reed & Mackay's Mobile and Personal Device Policy.

Employees should report instances of any data breach to SecurityIncident@reedmackay.com. Data breaches may take many different forms, for example –

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- personal information loss due to unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it

STORAGE AND RETENTION OF PERSONAL INFORMATION

Personal information will be kept securely in accordance with the Reed & Mackay's Information Security Policy, and should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Employees should follow the Data Retention Policy when determining retention period for information. Personal information (and sensitive personal information) that is no longer required will be deleted permanently from information systems and any hard copies will be destroyed securely.

INFORMATION SECURITY

Reed & Mackay will use appropriate technical and organisational measures in accordance with the Information Security Policy to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where Reed & Mackay uses external organisations to process personal information on its behalf, additional security arrangements may need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that -

- the organisation may act only on the written instructions of Reed & Mackay
- those processing the data are subject to a duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of Reed & Mackay and under a written contract
- the organisation will assist Reed & Mackay in providing subject access and allowing individuals to exercise their rights
- the organisation will assist Reed & Mackay in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the Company as requested at the end of the contract; and
- the organisation will submit to audits and inspections, provide Reed & Mackay with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Reed & Mackay immediately if it is asked to do something infringing data protection law.

POLICY GOVERNANCE, REVIEW & REVISION

The following table identifies who within Reed & Mackay is Accountable, Responsible, Informed or Consulted with regard to this policy.

RESPONSIBLE	Head of Governance, Risk Management & Compliance, Global Client Services Director
ACCOUNTABLE	Group Chief Financial Officer
CONSULTED	Group Chief Executive Officer, Founder & Executive Director, Group Chief Technology Officer, In-house Legal Counsel,
INFORMED	All employees

This policy will be reviewed as it is deemed appropriate, but no less frequently than annually. Policy review will be undertaken by the Group Chief Financial Officer and the Head of Governance, Risk Management & Compliance.

ROLES & RESPONSIBILITIES

Accountability for Data Protection lies with the Group Chief Financial Officer and is managed on a day to day basis by the Head of Governance, Risk Management & Compliance. The Global Client Services Director has responsibility specifically relating to client data and the HR Director for employee data (see Employee Data Protection Policy in R&M People). Heads of Departments and Directors are responsible for ensuring the data protection obligations and principles are adhered to within their teams.

All staff have a responsibility for adhering with this policy and reporting any identified weaknesses. Reports can be made either verbally or in writing and should in the first instance be raised with the appropriate Head of Department, and then with the Governance, Risk Management & Compliance department.

AWARENESS, TRAINING & QUERIES

The Data Protection policy is readily accessible internally via the intranet and also publicly upon request.

Our awareness programme is incorporated in our induction process and via annual training.

To discuss any matter relating the Data Protection Policy, contact the Head Governance, Risk Management & Compliance.