Data Protection Policy

Introduction

This policy has been approved by the RMR Group Board. It sets out rules on data protection and the legal conditions that must be satisfied when we collect, handle, process, store and transfer personal data.

The Data Controller is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Controller.

This policy applies to all employees, officers, contractors, consultants, temporary and agency staff, volunteers and anyone else processing personal data on behalf of RMR Group.

Key Definitions

Data is information which is stored electronically, on a computer or other device, or in certain paper-based filing systems.

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

Personal data means data relating to a living individual who can be identified, directly or indirectly, from that data (or from that data and other information in our possession). This includes any expression of opinion about the individual and any indication of our intentions or those of any other person in respect of the individual.

Data controllers are the people who, or organisations which, determine the purposes and means of processing personal data. They are responsible for establishing practices and policies in line with the Data Protection Legislation.

We are the data controller of all personal data used in our business for our own commercial purposes other than where we process data in the context of providing services to a third party who is the data controller, in which case we will be a data processor.

Data users are those of our employees or other workers whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.

Data processors include any person or organisation (other than a data user) that processes personal data on our behalf and on our instructions.

Data Protection Principles

Anyone processing personal data must comply with the enforceable principles of good practice. Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary
- Processed in a manner that ensures appropriate security of the personal data

We are accountable for demonstrating compliance with these principles.

Fair and Lawful Processing

The Data Protection Legislation is not intended to prevent the processing of personal data. Rather, it ensures that personal data is processed fairly and without adversely affecting the rights of the data subject.

For personal data to be processed lawfully, certain conditions must be met. These may include obtaining the consent of the data subject or that the processing is necessary for the legitimate interests pursued by the data controller or by the third party to whom the data is disclosed.

When sensitive personal data is being processed, more stringent conditions must be met. Explicit consent of the data subject will usually be required unless processing is necessary for certain specific reasons.

Processing for Limited Purposes

In the course of our business, we may collect and process personal data. This may include data we receive directly from a data subject or from third parties.

We will only process personal data for the specific purposes notified to the data subject when we first collected the data, or for any other purposes specifically permitted by the Data Protection Legislation.

Notifying Data Subjects

If we collect personal data directly from data subjects, we will inform them about:

- The purpose or purposes for which we intend to process that personal data
- The types of third parties, if any, with which we will share or to which we will disclose that personal data
- How the data subject can limit our use of their personal data

If we receive personal data about a data subject from other sources, we will provide the data subject with this information as soon as possible thereafter.

Adequate, Relevant and Non-Excessive Processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject, unless otherwise permitted by the Data Protection Legislation.

Accurate Data

We will ensure that personal data we hold is accurate and kept up to date. We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

Data subjects have the right to request rectification of inaccurate personal data.

Timely Processing

We will not keep personal data longer than is necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy or erase from our systems all data which is no longer required.

Data Security

We will take appropriate security measures against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

We will put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data will only be transferred to a data processor if they agree to comply with those procedures and policies, or if they put in place adequate measures themselves.

We will maintain data security by protecting the confidentiality, integrity and availability of personal data, defined as follows:

Confidentiality means that only people who are authorised to use the data can access it.

Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.

Availability means that authorised users should be able to access the data if they need it for authorised purposes.

Security procedures include:

- Entry controls to secure any buildings and storage systems in which personal data is held
- Procedures for granting access to personal data, including the use of secure passwords and encryption where appropriate
- Methods for ensuring personal data is stored securely and in accordance with legal requirements
- Training for staff on information security and data protection

---

Transferring Personal Data Outside the UK

We may transfer any personal data we hold to a country outside the UK provided that one of the following conditions applies:

- The country to which the personal data are transferred ensures an adequate level of protection for the data subjects' rights and freedoms (this includes countries in respect of which a finding of adequacy has been made)
- The data subject has explicitly consented to the transfer, after having been informed of the possible risks of such transfers
- The transfer is necessary for one of the reasons set out in the Data Protection Legislation, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject
- The transfer is authorised by the relevant data protection authority where we have provided adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights

Subject to the requirements in the section headed 'Data Security' above, personal data we hold may also be processed by staff operating outside the UK who work for us or for one of our suppliers. That staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

Data Subject Rights

Data subjects have rights when it comes to how we handle their personal data. These include rights to:

- Be informed about how their data is being used
- Access personal data we hold about them
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of their data
- Data portability (allowing them to obtain and reuse their data)
- Object to how their data is processed in certain circumstances

We will respect these rights and provide appropriate responses to any requests from data subjects exercising their rights.

Data Breaches

Data breaches will be handled in line with our data breach policy. Where a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the relevant supervisory authority within 72 hours of becoming aware of the breach.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, we will also notify those concerned directly.

Sharing Personal Data

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, where this is necessary for legitimate business purposes and in accordance with data protection requirements.

In certain circumstances, we may be legally required to share personal data, for example with law enforcement agencies or regulatory bodies.

Training and Awareness

We will ensure that all staff who handle personal data receive appropriate training on data protection and understand their responsibilities under this policy and relevant legislation.

Review and Updates

This policy will be reviewed regularly to ensure it remains current and compliant with data protection legislation. Any updates will be communicated to all relevant staff.

Contact

If you have any questions about this policy or about data protection matters generally, please contact the Data Controller at:

RMR Group
Matthew Read

Managing Director

This policy was last reviewed: 2024