



RMR CONSTRUCTION GROUP LIMITED

incorporating RMR FACADES (a division of RMR Construction Group)

Data Protection & Privacy Policy

Contents

Forward.....	3
Aims and Objectives.....	3
Scope.....	4
Data Subject Rights and Data Integrity.....	4
Technical and Organisational Data Security Measures.....	4
Data Disposal.....	6
Data Retention.....	7
Roles and Responsibilities.....	9
Implementation of Policy.....	9
PRIVACY POLICY.....	10

Forward

This policy sets out the obligations of RMR regarding retention of personal data collected, held, and processed by the Organisation in accordance with EU Regulation 2016/679 General Data Protection Regulation (“GDPR”).

The GDPR defines “personal data” as any information relating to an identified or identifiable natural person (a “data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

The GDPR also addresses “special category” personal data (also known as “sensitive” personal data). Such data includes, but is not necessarily limited to, data concerning the data subject’s race, ethnicity, politics, religion, trade union membership, genetics, biometrics (if used for ID purposes), health, sex life, or sexual orientation.

Under the GDPR, personal data shall be kept in a form which permits the identification of data subjects no longer than is necessary for the purposes for which the personal data is processed. In certain cases, personal data may be stored for longer periods where that data is to be processed for archiving purposes that are in public interest, for scientific or historical research, or for statistical purposes (subject to the implementation of the appropriate technical and organisational measures required by the GDPR to protect that data).

In addition, the GDPR includes the right to erasure or “the right to be forgotten”. Data subjects have the right to have their personal data erased (and to prevent the processing of that personal data) in the following circumstances:

- a) Where the personal data is no longer required for the purpose for which it was originally collected or processed (see above);
- b) When the data subject withdraws their consent;
- c) When the data subject objects to the processing of their personal data and the Organisation has no overriding legitimate interest;
- d) When the personal data is processed unlawfully (i.e. in breach of the GDPR);
- e) When the personal data has to be erased to comply with a legal obligation;
- f) or Where the personal data is processed for the provision of information f) society services to a child.

This Policy sets out the type(s) of personal data held by the Organisation, the period(s) for which that personal data is to be retained, the criteria for establishing and reviewing such period(s), and when and how it is to be deleted or otherwise disposed of.

Aims and Objectives

The primary aim of this Policy is to set out limits for the retention of personal data and to ensure that those limits, as well as further data subject rights to erasure, are complied with. By extension, this Policy aims to ensure that the Organisation complies fully with its obligations and the rights of data subjects under the GDPR.

In addition to safeguarding the rights of data subjects under the GDPR, by ensuring that

excessive amounts of data are not retained by the Organisation, this Policy also aims to improve the speed and efficiency of managing data.

Scope

This Policy applies to all personal data held by the Organisation and by third party data processors processing personal data on the Organisation's behalf.

Personal data, as held by the Organisation, is stored in the following ways and in the following locations:

- a) The Organisation stores electronic data encrypted on cloud servers which are GDPR compliant.
- b) Third-party data processors e.g. payroll provider, accountant, health and safety provider, etc.
- c) Computers permanently located in the Organisation's premises at 70a King Street, Norwich NR1 1PG.
- d) Laptop computers and other mobile devices provided by the Organisation to its employees and volunteers (where applicable) are stored with and at their homes securely.
- e) Computers and mobile devices owned by employees, volunteers, freelance consultants, volunteers, and external sub-contractors.
- f) Physical records are stored at our premises at 70a King Street, Norwich NR1 1PG; and
- g) Physical records such as case records are securely stored at employee or associate's homes or at the Organisation's premises at 70a King Street, Norwich NR1 1PG.

Data Subject Rights and Data Integrity

All personal data held by the Organisation is held in accordance with the requirements of the GDPR and data subjects' rights thereunder, as set out in the Organisation's Data Protection Policy.

- 1) Data subjects are kept fully informed of their rights, of what personal data the Organisation holds about them, how that personal data is used and how long the Organisation will hold that personal data (or, if no fixed retention period can be determined, the criteria by which the retention of the data will be determined).
- 2) Data subjects are given control over their personal data held by the Organisation including the right to have incorrect data rectified, the right to request that their personal data be deleted or otherwise disposed of (notwithstanding the retention periods otherwise set by this Data Retention Policy), the right to restrict the Organisation's use of their personal data, and further rights relating to automated decision-making and profiling.

Technical and Organisational Data Security Measures

The following technical measures are in place within the Organisation to protect the security of personal data:

- a) All emails containing personal data must be encrypted and transferred by secure methods (see below);
- b) All emails containing personal data must be marked "confidential";
- c) Personal data may only be transmitted over secure networks;
- d) Personal data may not be transmitted over a wireless network if there is a reasonable wired alternative;

- e) Personal data contained in the body of an email, whether sent or received, should be copied from the body of that email and stored securely. The email itself and associated temporary files should be deleted;
- f) Where personal data is to be sent by facsimile transmission the recipient should be informed in advance and should be waiting to receive it;
- g) Where personal data is to be transferred in hardcopy form, it should be passed directly to the recipient; All personal data transferred physically should be transferred in a suitable container marked "confidential";
- h) No personal data may be shared informally and if access is required to any personal data, such access should be formally requested from Matthew Read, Managing Director.
- i) All hardcopies of personal data, along with any electronic copies stored on physical media should be stored securely;
- j) No personal data may be transferred to any employees, volunteers, contractors, or other parties, whether such parties are working on behalf of the Organisation or not, without authorisation; Personal data must be handled with care at all times and should not be left unattended or on view;
- k) Computers used to view personal data must always be locked before being left unattended;
- l) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to contractors or other parties working on behalf of the Organisation where the party in question has agreed to comply fully with the Organisation's Data Protection Policy and the GDPR;
- m) All personal data stored electronically should be encrypted and be backed up periodically with backups stored securely at 70a King Street, Norwich, NR1 1PG;
- n) All backups should be password protected, stored off site in a safe as the Chief Executive Officers home;
- o) All electronic copies of personal data should be stored securely using passwords and encryption;
- p) All passwords used to protect personal data should be changed regularly and should must be secure;
- q) Under no circumstances should any passwords be written down or shared. If a password is forgotten, it must be reset using the applicable method;
- r) All software should be kept up-to-date. Security-related updates should be installed as soon as reasonably possible after becoming available;
- s) No software may be installed on any Organisation-owned computer or device without approval; and
- t) Where personal data held by the Organisation is used for marketing purposes, it shall be the responsibility of Matthew Read, Managing Director or any successor in the role to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service.

The following organisational measures are in place within the Organisation to protect the security of personal data:

- a) All employees, volunteers and other parties working on behalf of the Organisation shall be made fully aware of both their individual responsibilities and the Organisation's responsibilities under the GDPR and under the Organisation's Data Protection Policy;
- b) Only employees, volunteers and other parties working on behalf of the Organisation that need access to, and use of, personal data in order to perform their work shall have access to personal data held by the Organisation;
- c) All employees and other parties working on behalf of the Organisation handling personal data will be appropriately trained to do so;
- d) All employees and other parties working on behalf of the Organisation handling personal data will be appropriately supervised;
- e) All employees and other parties working on behalf of the Organisation handling personal data should exercise care and caution when discussing any work relating to personal data at all times;
- f) Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- g) The performance of those employees and other parties working on behalf of the Organisation handling personal data shall be regularly evaluated and reviewed;
- h) All employees and other parties working on behalf of the Organisation handling personal data will be bound by contract to comply with the GDPR and the Organisation's Data Protection Policy;
- i) All sub-contractors, or other parties working on behalf of the Organisation handling personal data must ensure that any and all relevant employees are held to the same conditions as those relevant employees of the Organisation arising out of the GDPR and the Organisation's Data Protection Policy;
- j) Where any sub-contractor or other party working on behalf of the Organisation handling personal data fails in their obligations under the GDPR and/or the Organisation's Data Protection Policy, that party shall indemnify and hold harmless the Organisation against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

Data Disposal

Upon the expiry of the data retention periods set out below in Part 7 of this Policy, or when a data subject exercises their right to have their personal data erased, personal data shall be deleted, destroyed, or otherwise disposed of as follows:

- 1) Personal data stored electronically (including any and all backups thereof) shall be deleted securely;
- 2) Personal data stored in hardcopy form shall be shredded and securely disposed of;

Data Retention

As stated above, and as required by law, the Organisation shall not retain any personal data for any longer than is necessary in light of the purpose(s) for which that data is collected, held, and processed.

Different types of personal data, used for different purposes, will necessarily be retained for different periods (and its retention periodically reviewed), as set out below.

When establishing and/or reviewing retention periods, the following shall be taken into account:

- a) The objectives and requirements of the Organisation;
- b) The type of personal data in question;
- c) The purpose(s) for which the data in question is collected, held, and processed;
- d) The Organisation's legal basis for collecting, holding, and processing that data;
- e) The category or categories of data subject to whom the data relates;

If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

Notwithstanding the following defined retention periods, certain personal data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the Organisation to do so (whether in response to a request by a data subject or otherwise).

In limited circumstances, it may also be necessary to retain personal data for longer periods where such retention is for archiving purposes that are in the public interest, for scientific or historical research purposes, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organisational measures to protect the rights and freedoms of data subjects, as required by the GDPR.

Data Ref.	Type of Data	Purpose of Data	Review Period	Retention Period or Criteria	Comments
E-O-01	Staff Data	Recruitment Employment Contracting	Annually	7 Years	
E-O-02	Sub-Contractors	Management of Sub-contractors	Annually	2 Years	
E-O-03	Marketing Databases	Promotion & Sales	Annually	1.5 Years	
E-O-04	Contracts Files	Records of projects	Annually	7 Years	
E-O-05	Client Database	Records of Clients	Annually	7 Years	
E-O-06	Suppliers Database	Records of Supplier	Annually	7 Years	

Roles and Responsibilities

The Data Controller is Matthew Read, Managing Director, matthew@rmrgroup.co.uk

The Data Controller shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, the Organisation's other Data Protection-related policies (including, but not limited to, its Data Protection Policy), and with the GDPR and other applicable data protection legislation.

The Data Controller shall be directly responsible for ensuring compliance with the above data retention periods throughout the Organisation.

Any questions regarding this Policy, the retention of personal data, or any other aspect of GDPR compliance should be referred to the Data Controller.

Implementation of Policy

This Policy shall be deemed effective as of 01st January 2025. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

PRIVACY POLICY

This Policy shall be deemed effective as of 1st January 2025. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

Our contact details

Name: RMR Construction Group Limited
Address: 70a King Street, Norwich, NR1 1PG
Phone Number: 01603 622595
E-mail:matthew@rmrgroup.co.uk

The type of personal information we collect

We currently collect and process the following information:

- Personal identifiers, contacts and characteristics (for example, name and contact details)
- Financial information on customers.

How we get personal information and why we have it

Most of the personal information we process is provided to us directly by you for one of the following reasons:

- For the purpose of processing employees and their payroll.
- For the purpose of processing sub-contractors and their payments
- For the purpose of processing orders with suppliers.
- For the purpose of deciding whether to undertake contracts.

We may share this information with HMRC & other government bodies.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases we rely on for processing this information are:

- a) Your consent. You are able to remove your consent at any time. You can do this by contacting Matthew Read
- b) We have a contractual obligation.
- c) We have a legal obligation.

How we store your personal information

Your information is securely stored.

All information is reviewed annually and kept for a period as defined in the data protection policy.

Your data protection rights

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information.

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at matthew@rmrgroup.co.uk, 01603 622595, 70a King Street, Norwich, NR1 1PG if you wish to make a request.

How to complain

If you have any concerns about our use of your personal information, you can make a complaint to us at matthew@rmrgroup.co.uk, 01603 622595, 70a King Street, Norwich, NR1 1PG

You can also complain to the ICO if you are unhappy with how we have used your data.

The ICO's address:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

ICO website: <https://www.ico.org.uk>

For and on behalf of RMR Construction Group Limited

Signed:

Matthew Read

Managing Director

Date: January 2025