

R&M POLICY · DATA AND CYBER SECURITY

Data Protection Policy

R&M Property Group Ltd

Document	RM-DC-01
Reference	RM-DPP-001
Version	2.0
Issued	June 2026
Next review	June 2027
Approved by	Thomas McKenna, Director
Website issue	22 October 2026

Part A - Data Protection Policy

1. Purpose

This policy sets out how R&M Property Group Ltd ('R&M', 'the company') collects, uses, stores, shares, and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It establishes the company's programme for maintaining GDPR compliance, defines responsibilities for handling personal and sensitive data throughout the organisation, and describes the arrangements in place for IT data security. This policy incorporates the company's Privacy Notice at Part B.

2. Scope

This policy applies to:

- All employees, workers, contractors, sub-contractors, consultants, and any other third party who processes personal data on behalf of R&M Property Group Ltd.
- All personal data processed by the company, whether in digital or paper format, including data held on company systems, cloud platforms, project management software, mobile devices, and physical records.
- All processing activities carried out by the company as a data controller, and any processing carried out by third parties on the company's behalf as data processors.

3. Data Protection Principles

R&M Property Group Ltd is committed to processing all personal data in accordance with the six data protection principles set out in Article 5 of the UK GDPR:

- **Lawfulness, fairness, and transparency -** personal data is processed lawfully, fairly, and in a transparent manner. Data subjects are informed about how their data is used through this policy and the Privacy Notice at Part B.
- **Purpose limitation -** personal data is collected for specified, explicit, and legitimate purposes and is not further processed in a manner incompatible with those purposes.
- **Data minimisation -** personal data collected is adequate, relevant, and limited to what is necessary for the purpose for which it is processed.
- **Accuracy -** personal data is accurate and, where necessary, kept up to date. Reasonable steps are taken to ensure inaccurate data is corrected or deleted without delay.
- **Storage limitation -** personal data is retained only for as long as necessary to fulfil the purpose for which it was collected, or as required by law. Retention periods are set out in Section 12.
- **Integrity and confidentiality -** personal data is processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage.

4. Lawful Basis for Processing

R&M will only process personal data where there is a lawful basis under Article 6 of the UK GDPR. The lawful bases the company relies on include:

- **Contractual necessity -** processing is necessary for the performance of a contract with the data subject, for example employment contracts, sub-contractor agreements, or client contracts.
- **Legal obligation -** processing is necessary to comply with a legal obligation, for example HMRC reporting, health and safety record-keeping, right to work checks, or Building Safety Act duties.
- **Legitimate interests -** processing is necessary for the company's legitimate interests (such as business administration, security, or fraud prevention), provided those interests are not overridden by the individual's rights and freedoms.
- **Consent -** where none of the above bases apply, the company obtains the individual's freely given, specific, informed, and unambiguous consent. Consent can be withdrawn at any time.
- **Vital interests -** in exceptional circumstances, processing may be necessary to protect someone's life, for example sharing medical information with emergency services following a site accident.

For special category data (see Section 7), additional conditions under Article 9 are satisfied before processing takes place.

5. Responsibilities

5.1 Thomas McKenna, Director (Data Protection Responsible Person)

- Overall accountability for the company's compliance with data protection legislation.
- Approves this policy and any updates following review.
- Ensures adequate resources are allocated to data protection compliance.
- Acts as the primary point of contact for data protection queries and data subject rights requests.
- Responsible for notifying the Information Commissioner's Office (ICO) of reportable data breaches within 72 hours.

5.2 Phillip Hollingworth, H&S Adviser (Spectra Safety)

- Advises the company on data protection obligations and monitors compliance.
- Supports the completion of Data Protection Impact Assessments (DPIAs) for new processing activities.
- Maintains the company's Record of Processing Activities (ROPA).
- Reviews data processing agreements with third-party processors.
- Coordinates data protection training and awareness programmes.

5.3 Chris Walker, IT Support

- Implements and maintains technical security measures to protect personal data held on company systems.
- Manages access controls, encryption, backup, and disaster recovery for IT systems containing personal data.

- Supports the investigation of data breaches involving IT systems.
- Ensures IT systems comply with the company's Cyber Security Policy (RM-CSP-001).

5.4 All Employees, Workers, and Contractors

- Understand and comply with this policy and any associated procedures.
- Only access personal data that is necessary for their role.
- Keep personal data secure - locking screens, securing physical files, not sharing passwords, and not transferring data to personal devices.
- Report any suspected data breach, loss of data, or misuse of personal information immediately to Thomas McKenna.
- Complete data protection training on induction and annually thereafter.

6. Data Subject Rights

Under the UK GDPR, individuals whose personal data is processed by R&M have the following rights:

- **Right to be informed -** individuals have the right to be told how their data is collected and used. The Privacy Notice at Part B fulfils this requirement.
- **Right of access -** individuals can make a Subject Access Request (SAR) to obtain a copy of the personal data the company holds about them. SARs are responded to within one calendar month.
- **Right to rectification -** individuals can request correction of inaccurate or incomplete personal data.
- **Right to erasure -** individuals can request deletion of their personal data where there is no compelling reason for its continued processing, subject to legal retention obligations.
- **Right to restrict processing -** individuals can request that the company limits how it uses their data in certain circumstances.
- **Right to data portability -** where processing is based on consent or contract and carried out by automated means, individuals can request their data in a structured, commonly used, machine-readable format.
- **Right to object -** individuals can object to processing based on legitimate interests or for direct marketing purposes.
- **Rights related to automated decision-making -** individuals have the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects. R&M does not currently carry out automated decision-making.

Requests to exercise any of these rights should be made in writing to Thomas McKenna at thom@randmproperty.co.uk. The company will respond within one calendar month. Where a request is complex or the company has received a large number of requests, the response period may be extended by a further two months, and the individual will be informed of this within the initial one-month period.

7. Special Category and Sensitive Data

Special category data is personal data that requires additional protection because of its sensitive nature. Under Article 9 of the UK GDPR, this includes data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic

data, biometric data, health data, and data concerning sex life or sexual orientation. Criminal conviction data is subject to separate additional safeguards under Article 10.

7.1 Special Category Data Processed by R&M

In the course of its business, R&M may process the following types of special category and sensitive data:

- **Health data -** occupational health assessments, fit notes, accident and incident reports, health surveillance records, disability and reasonable adjustment information, and emergency medical information held for site personnel.
- **Trade union membership -** where disclosed by an employee for the purpose of union representation or consultation.
- **Criminal conviction data -** DBS checks for roles requiring them, and declarations made during pre-employment screening.
- **Biometric data -** where site access control systems use biometric identification (fingerprint or facial recognition).
- **Right to work documentation -** which may reveal racial or ethnic origin or nationality.

7.2 Handling Requirements

Special category data is subject to the following additional controls:

- It is only collected where there is a lawful basis under Article 6 and an additional condition under Article 9 (typically employment law obligation, health and safety obligation, or explicit consent).
- Access is restricted to the minimum number of people who need it for a specific purpose - typically the Director, Compliance Officer, or relevant project manager.
- It is stored separately from general personnel files where practicable, in access-controlled digital folders or locked physical storage.
- It is not shared with any third party unless there is a lawful basis and, where required, a data processing agreement in place.
- It is retained only for the minimum period necessary and securely destroyed when no longer required (see Section 12).
- Paper records containing special category data are stored in locked cabinets and shredded when disposed of.

8. Data Protection by Design and Default

R&M applies data protection by design and by default when introducing new systems, processes, or projects that involve the processing of personal data. This means that data protection considerations are built into the design of processing activities from the outset, and that the default settings of any system minimise the amount of personal data collected and the extent of processing. Before any new processing activity, system, or project involving personal data is implemented, the Compliance Officer assesses whether a Data Protection Impact Assessment (DPIA) is required.

9. Data Protection Impact Assessments (DPIAs)

A DPIA is carried out before any processing activity that is likely to result in a high risk to the rights and freedoms of individuals. This includes but is not limited to:

- Introduction of new technology that processes personal data (for example new site monitoring systems, biometric access controls, or AI-based tools).
- Large-scale processing of special category data.
- Systematic monitoring of publicly accessible areas (for example CCTV on construction sites).
- Processing that could result in automated decisions with significant effects on individuals.

The DPIA is carried out by the Compliance Officer in consultation with the Director and, where appropriate, Chris Walker (IT Support). It identifies the risks to individuals, assesses whether the processing is proportionate and necessary, and sets out the measures to mitigate identified risks. Where a DPIA identifies a high residual risk that cannot be mitigated, the company consults the ICO before proceeding. Completed DPIAs are retained as part of the company's accountability records.

10. Records of Processing Activities

R&M maintains a Record of Processing Activities (ROPA) as required by Article 30 of the UK GDPR. The ROPA is maintained by the Compliance Officer and records the following for each processing activity:

- The purpose of the processing.
- The categories of data subjects and categories of personal data.
- The recipients or categories of recipients to whom personal data is disclosed.
- Whether personal data is transferred outside the UK, and the safeguards in place.
- The retention period for each category of data.
- A general description of the technical and organisational security measures in place.

The ROPA is reviewed at least annually and updated whenever a new processing activity is introduced or an existing activity changes materially.

11. IT Data Security Arrangements

R&M implements appropriate technical and organisational measures to protect personal data from unauthorised access, alteration, disclosure, destruction, or accidental loss. The full detail of the company's IT security controls is set out in the Cyber Security Policy (RM-CSP-001). The key measures relevant to personal data protection are summarised below:

11.1 Access Controls

- Access to systems containing personal data is restricted to authorised personnel on the principle of least privilege.
- Multi-factor authentication (MFA) is enabled on all cloud-hosted systems, email accounts, and remote access connections.
- Access rights are reviewed when an employee changes role and revoked immediately on departure.
- Strong password requirements are enforced - minimum 12 characters, mixed case, numbers, and symbols.

11.2 Encryption and Secure Storage

- Personal data stored on company systems, cloud platforms, and portable devices is encrypted at rest and in transit.

- USB drives and external storage devices must be encrypted and approved before use.
- Sensitive data is stored in access-controlled folders with permissions limited to those who need it for their role.

11.3 Backup and Recovery

- Critical systems and data are backed up daily to a geographically separate secure location.
- Backup integrity is tested quarterly.
- Recovery procedures are documented and tested to ensure personal data can be restored following an incident.

11.4 Monitoring and Logging

- Access to systems containing personal data is logged and monitored.
- Security logs are reviewed monthly for anomalies.
- Logs are retained for a minimum of 12 months.

11.5 Secure Disposal

- When hardware is decommissioned, all data is securely wiped using an approved method and a certificate of destruction is retained.
- Paper records containing personal data are cross-cut shredded.

For full details of the company's cyber security controls, including incident response, malware protection, home working arrangements, and NCSC 10 Steps alignment, refer to the Cyber Security Policy (RM-CSP-001).

12. Data Retention

Personal data is retained only for as long as necessary to fulfil the purpose for which it was collected, or as required by legal, regulatory, or contractual obligations. At the end of the applicable retention period, data is securely deleted, destroyed, or anonymised. The following retention periods apply:

- **Employee personnel records -** 6 years after the end of employment (Limitation Act 1980).
- **Payroll and tax records -** 6 years from the end of the tax year to which they relate (HMRC requirements).
- **Health and safety records (accident reports, risk assessments) -** minimum 3 years; 40 years for records relating to exposure to hazardous substances (COSHH Regulations).
- **Right to work checks -** 2 years after the end of employment (Immigration, Asylum and Nationality Act 2006).
- **DBS certificates -** reviewed and destroyed within 6 months of the recruitment decision, unless a dispute is ongoing (DBS Code of Practice).
- **Training records and competency evidence -** duration of employment plus 6 years.
- **Sub-contractor pre-qualification records -** duration of the engagement plus 6 years.
- **Project records and building safety information -** in accordance with the Building Safety Act 2022 golden thread requirements, retained for the life of the building where applicable.
- **Client and supplier contract records -** 6 years after the end of the contract (Limitation Act 1980).
- **CCTV footage -** maximum 30 days unless retained for an ongoing investigation or legal proceedings.
- **Recruitment records (unsuccessful candidates) -** 6 months after the recruitment decision.

Where an individual requests erasure of their data, the company will comply unless a legal retention obligation applies, in which case the individual will be informed of the reason for continued retention.

13. Data Breach Response

A personal data breach is any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. All employees must report any suspected data breach immediately to Thomas McKenna.

13.1 Breach Response Process

On receiving a report of a suspected breach, the following process is followed:

- **Containment -** immediate steps are taken to contain the breach and limit further exposure. This may include disabling access, isolating systems, or recovering lost devices.
- **Assessment -** the nature and scope of the breach are assessed, including what data was involved, how many individuals are affected, and the likely consequences for those individuals.
- **ICO notification -** if the breach is likely to result in a risk to the rights and freedoms of individuals, the ICO is notified within 72 hours of the company becoming aware of the breach. The notification includes the nature of the breach, categories and approximate number of individuals affected, likely consequences, and measures taken or proposed to address the breach.
- **Individual notification -** if the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected individuals are notified without undue delay.
- **Record-keeping -** all breaches, whether or not they are reported to the ICO, are recorded in the company's breach log with the facts of the breach, its effects, and the remedial action taken.
- **Lessons learned -** following resolution, a review is conducted to identify the root cause and any improvements needed to prevent recurrence.

14. Data Processors and Third Parties

Where R&M engages a third party to process personal data on its behalf (a data processor), the company ensures that:

- A written data processing agreement is in place that meets the requirements of Article 28 of the UK GDPR, setting out the subject matter, duration, nature, and purpose of the processing, and the obligations of the processor.
- The processor provides sufficient guarantees that it will implement appropriate technical and organisational measures to meet UK GDPR requirements.
- The processor does not engage a sub-processor without the prior written consent of R&M.
- The processor is required to notify R&M immediately of any personal data breach.

Current data processors include cloud service providers (Microsoft 365), payroll providers, health and safety advisers (Spectra Safety), IT support providers, and project management platform providers (Autodesk Build). A register of data processors is maintained by the Compliance Officer as part of the ROPA.

15. International Data Transfers

R&M does not routinely transfer personal data outside the United Kingdom. Where a transfer outside the UK is necessary - for example where a cloud service provider stores data in data centres outside the UK - the company ensures that appropriate safeguards are in place in accordance with Chapter V of the UK GDPR. These safeguards may include adequacy decisions, standard contractual clauses, or binding corporate rules. No transfer of personal data outside the UK will take place without the approval of the Director.

16. Training and Awareness

All employees receive data protection training as part of their induction, covering the key principles of the UK GDPR, their responsibilities under this policy, how to identify and report a data breach, and how to handle data subject rights requests. Refresher training is provided annually. Additional targeted training is provided to employees whose roles involve regular handling of special category data or high volumes of personal data. Training records are maintained by the Compliance Officer. Training is delivered in accessible formats in line with R&M's commitment to training accessibility - a mixture of oral, written, visual, and digital methods, with adaptations for operatives where English is not their first language.

Part B - Privacy Notice

17. Privacy Notice

This Privacy Notice explains how R&M Property Group Ltd collects, uses, stores, and shares personal data about individuals who interact with the company. It is provided in accordance with Articles 13 and 14 of the UK GDPR.

17.1 Who We Are

R&M Property Group Ltd is the data controller for the personal data described in this notice. Our registered address and contact details are available on our website and on request. The person responsible for data protection is Thomas McKenna, Director, who can be contacted at thom@randmproperty.co.uk.

17.2 What Personal Data We Collect

The categories of personal data we collect depend on your relationship with us:

- **Employees and workers -** name, address, date of birth, National Insurance number, bank details, emergency contact details, right to work documentation, qualifications and training records, health and safety records, occupational health data, performance records, disciplinary records, CCTV images (on construction sites), and photographs for identification purposes.
- **Sub-contractors and suppliers -** company and individual contact details, pre-qualification information, competency and training records, health and safety documentation, insurance details, financial information for payment processing, and CCTV images (on construction sites).

- **Clients and prospective clients -** contact details, project information, correspondence, and contract-related financial data.
- **Site visitors -** name, company, contact details, vehicle registration, CCTV images, and site induction records.
- **Job applicants -** name, contact details, CV, employment history, qualifications, references, right to work documentation, and DBS check results where applicable.

17.3 How We Use Your Data

We use personal data for the following purposes:

- Administering employment and worker relationships, including payroll, benefits, training, and performance management.
- Managing contracts with clients, sub-contractors, and suppliers.
- Complying with health and safety obligations, including accident reporting, risk assessments, and occupational health monitoring.
- Complying with Building Safety Act 2022 duties, including maintaining the golden thread of building information.
- Verifying right to work in the United Kingdom.
- Verifying competency, qualifications, and training for site-based roles.
- Pre-qualifying sub-contractors and suppliers.
- Fulfilling legal and regulatory obligations, including HMRC reporting, modern slavery due diligence, and construction industry scheme (CIS) requirements.
- Site security and safety monitoring through CCTV.
- Responding to legal claims and regulatory investigations.

17.4 Who We Share Your Data With

We may share personal data with the following categories of recipient where there is a lawful basis to do so:

- HMRC - for tax and National Insurance reporting.
- HSE - for statutory accident and incident reporting (RIDDOR).
- Building Safety Regulator - for mandatory occurrence reporting and competence records under the Building Safety Act 2022.
- Clients and framework operators - where contractually required, for example pre-qualification information, competency evidence, and project records.
- Sub-contractors and suppliers - limited project-related information necessary for contract performance.
- Spectra Safety (The Safety Group Limited) - as our retained health and safety advisers, acting as a data processor.
- Payroll provider - for payroll administration, acting as a data processor.
- IT service providers - for system support and maintenance, acting as data processors.
- Insurers - for the administration of employer's liability, public liability, and professional indemnity claims.
- Legal advisors - where necessary for legal proceedings or regulatory compliance.
- Police and law enforcement - where required by law or to protect vital interests.

17.5 How Long We Keep Your Data

Retention periods for each category of personal data are set out in Section 12 of this policy.

17.6 Your Rights

Your rights as a data subject are set out in Section 6 of this policy. To exercise any of these rights, contact Thomas McKenna at thom@randmproperty.co.uk. If you are not satisfied with how we handle your request, you have the right to lodge a complaint with the Information Commissioner's Office (ICO) at ico.org.uk or by calling 0303 123 1113.

17.7 Changes to This Notice

This Privacy Notice may be updated from time to time to reflect changes in our processing activities or legal requirements. The current version is always available from Thomas McKenna on request.

18. Policy Review

This policy and the incorporated Privacy Notice are reviewed annually by the Compliance Officer and the Director, or sooner if there is a significant change in data protection legislation, ICO guidance, the company's processing activities, or following a data breach. The review considers the effectiveness of existing measures, any breaches or near-misses since the last review, changes to ICO or government guidance, new processing activities, and any changes to the company's IT systems. All changes are approved by the Director.

19. Related Documents

- Cyber Security Policy (RM-CSP-001)
- Record of Processing Activities (ROPA)
- Data Breach Log
- DPIA Register
- Risk Management Policy
- Right to Work Verification Policy
- Anti-Slavery and Human Trafficking Policy
- Competency Management Procedure (RM-CMP-001)
- Prevention of Sexual Harassment Policy

Signed and Approved:

Thomas McKenna

Director, R&M Property Group Ltd

Date: June 2026