



Data Processing Agreement

Purpose

Dale Building Maintenance Ltd recognises its obligations under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 to ensure that personal data is processed lawfully, fairly, securely, and transparently.

Where personal data is processed on behalf of, or shared with, customers, suppliers, subcontractors, service providers, and other third parties, appropriate contractual safeguards are implemented through Data Processing Agreements (DPAs), data protection clauses, or equivalent contractual arrangements.

Arrangements

Customer Agreements

Where Dale Building Maintenance Ltd acts as a data processor on behalf of customers, contractual agreements include provisions covering:

- The nature and purpose of processing.
- Categories of personal data processed.
- Types of data subjects affected.
- Responsibilities and obligations of each party.
- Confidentiality requirements.
- Information security controls.
- Data retention and disposal requirements.
- Incident and breach notification processes.
- Subject access request support.
- Audit and compliance rights.
- International data transfer controls where applicable.

Supplier and Service Provider Agreements

Where suppliers or service providers process personal data on behalf of Dale Building Maintenance Ltd, the company seeks to ensure that appropriate Data Processing Agreements are in place with key providers, including those providing:

- Cloud hosting services.
- Microsoft 365 services.
- IT support and managed services.
- HR and payroll systems.
- Document management systems.



- Backup and disaster recovery services.
- Software-as-a-Service (SaaS) platforms.
- Professional advisory services where personal data is processed.

Agreements require suppliers to maintain appropriate technical and organisational security measures and comply with applicable data protection legislation.

Due Diligence and Procurement

Before engaging suppliers who may process personal data, the company undertakes proportionate due diligence which may include:

- Review of privacy and security arrangements.
- Assessment of cyber security controls.
- Verification of relevant certifications or accreditations.
- Review of data processing terms.
- Confirmation of incident reporting arrangements.
- Assessment of overseas data processing and data transfer safeguards.

Ongoing Monitoring

The company periodically reviews key data processing relationships to ensure:

- Contracts remain current.
- Processing activities remain lawful and proportionate.
- Appropriate security controls are maintained.
- Regulatory changes are reflected in contractual arrangements.