

Data Protection Policy Statement

This policy applies to JSM Group Holdings Limited, including all UK and International subsidiaries and its personnel.

As a leading provider of integrated utility infrastructure solutions, JSM recognises that the personal data of our employees, candidates, clients, supply chain and other stakeholders is entrusted to us, and that protecting it is fundamental to the trust placed in our business. JSM believes personal data should never be put at risk through our operations, and we are committed to handling it lawfully, fairly, transparently and securely in everything we do.

As part of our Integrated Management System (IMS) we will develop and maintain a data protection framework aligned to the UK GDPR and the Data Protection Act 2018, supported by our ISO 27001 certified Information Security Management System. We apply a risk-based approach to identify, assess and manage privacy risks, ensuring resilience and continual improvement, with independent oversight provided by our appointed Data Protection Officer.

This standard applies across the Group. Our entities in Germany, Ireland and Sweden operate under the EU GDPR and their national data protection laws; JSM India under the Digital Personal Data Protection Act 2023; and JSM Bahrain under the Personal Data Protection Law (Law No. 30 of 2018). Where local requirements are lower than the UK GDPR and the Data Protection Act 2018, we adopt the UK standard as the Group minimum; where they are higher, local law prevails. Transfers of personal data between Group entities are made only on a lawful basis under the Data Sharing, Third Parties and International Transfers Procedure.

Our key commitments are to:

- Comply with the UK General Data Protection Regulation, the Data Protection Act 2018 and all other applicable privacy legislation, whilst striving to achieve even higher standards.
- Process personal data lawfully, fairly and transparently, collecting it only for specified, explicit and legitimate purposes and limiting it to what is necessary.
- Keep personal data accurate and up to date and retain it only for as long as necessary before secure disposal.
- Protect personal data through appropriate technical and organisational measures, aligned to our ISO 27001 certified Information Security Management System.
- Respect and uphold the rights of data subjects, ensuring requests are handled promptly and within statutory timescales.
- Apply data protection by design and by default, screening all new projects, systems and suppliers and completing Data Protection Impact Assessments where required.
- Report, investigate and review all personal data breaches, notifying the Information Commissioner's Office within 72 hours where required, to identify root causes and prevent recurrence.
- Maintain accurate Records of Processing Activities across all business functions.
- Empower our workforce with the right training, resources and ongoing communication to handle personal data responsibly.
- Engage with our supply chain and third parties to ensure personal data shared with or processed by them is appropriately protected.

The Board actively promotes leadership in data protection and privacy management and commits to reviewing this policy annually or following significant organisational or legislative change, and to communicate it within the organisation and externally to interested parties.

A handwritten signature in black ink, appearing to read 'M Booth'.

Michael Booth
Chief Executive Officer

Date: 22 September 2026