QBD.27 Data Protection Policy (UK)

1. Introduction

This Data Protection Policy explains how Rayan Facilities Management Ltd ("the Company", "we", "our", "us") processes and protects Personal Data in accordance with:

- The UK General Data Protection Regulation (UK GDPR).
- The Data Protection Act 2018.
- The Data (Use and Access) Act 2025 (DUAA), including provisions commencing in 2025 and 2026.

This policy applies to all Personal Data processed by the Company, regardless of the medium, and to all Company Personnel. Compliance with this policy is mandatory.

2. Key Legislative Changes Reflected in this Policy

- Recognised Legitimate Interests: A new statutory basis under DUAA allowing certain processing without a balancing test.
- Automated Decision-Making (ADM): DUAA now permits wider use of ADM, with specific safeguards.
- Mandatory Data Protection Complaints Procedure: Organisations must provide a complaints route, acknowledge within 30 days, and provide timely outcomes.
- Updated international transfer rules.
- Updated statutory definition of scientific research.

3. Principles of Data Protection

We follow the seven UK GDPR principles: lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity/confidentiality, and accountability.

4. Lawfulness, Fairness and Transparency

Our lawful bases include:

- Consent
- Contract
- Legal obligation
- Vital interests
- Legitimate interests
- Recognised Legitimate Interests

Privacy Notices must reflect the DUAA transparency requirements.

5. Consent

Consent must be freely given, specific, informed, unambiguous and withdrawable. Explicit Consent is required for certain Special Category or Criminal Convictions data.

6. Mandatory Data Protection Complaints Procedure

We must:

- Provide a clear method for data protection complaints.
- Acknowledge complaints within 30 days.
- Investigate promptly and inform complainants of outcomes.
- Maintain records of complaints.

7. Purpose Limitation

Personal Data must only be collected for specified purposes. New purposes must be approved by the DPO.

8. Data Minimisation

Only data necessary for the relevant purpose may be collected and processed.

9. Accuracy

We must ensure Personal Data is accurate and up to date, correcting or deleting inaccuracies without delay.

10. Storage Limitation

Data must not be retained longer than necessary. Privacy Notices must clearly state retention periods.

11. Security, Integrity and Confidentiality

Personal Data must be secured using appropriate organisational and technical measures, including encryption and pseudonymisation where relevant.

12. Personal Data Breaches

All breaches must be reported immediately. The Company must notify the ICO and affected individuals where required.

13. International Data Transfers

Cross-border data transfers must comply with updated DUAA rules, using recognised transfer tools or adequacy decisions and DPO approval.

14. Data Subject Rights

We must uphold all UK GDPR rights, including the right to access, rectification, erasure, portability, object, restrict processing and rights related to ADM.

15. Automated Decision-Making (ADM)

Under DUAA, ADM may be used where safeguards are in place, including the right to human review, transparency of logic, and the ability to challenge decisions.

A DPIA is required for new ADM technologies.

16. DPIA and Privacy by Design

DPIAs must be carried out for high-risk processing, especially involving AI, profiling, or new technologies.

17. Direct Marketing

Marketing activities must comply with UK GDPR, DUAA and PECR. Individuals must be able to opt out easily.

18. Sharing Personal Data

Data may only be shared with approved partners following checks, contractual controls and DPO approval.

19. Record Keeping

We must maintain accurate and complete Article 30 records of processing activities.

20. Training and Audit

All staff must complete data protection training. Regular audits must be undertaken.

21. Updates to this Policy

This policy will be reviewed annually or earlier if required by law or ICO guidance.

Signed:

Siobhan Hamill

Managing Director

10/03/2026