

# Group Data Protection Policy Summary

Jet2 are committed to protecting personal data in accordance with the Data Protection Act 2018 and the UK GDPR. This policy outlines how personal data is collected, processed, stored, and protected across the Group.

## Key Principles of Data Protection

### 1. Lawfulness, Fairness & Transparency

Personal data must be processed legally and transparently. The Group relies on lawful bases such as legal obligations, contract performance, legitimate interests, and consent (where applicable).

### 2. Purpose Limitation

Data is collected for specific, legitimate purposes as outlined in the Employee and Customer Privacy Notices.

### 3. Data Minimisation

Only data necessary for the intended purpose is collected and used.

### 4. Accuracy

Data must be accurate and kept up to date. Corrections should be made promptly when inaccuracies are found.

### 5. Storage Limitation

Data is retained only as long as necessary, following defined retention schedules. Exceptions apply for legal holds or ongoing investigations.

### 6. Security & Confidentiality

Technical and organisational measures are in place to protect data, including encryption, access controls, and secure storage practices.

## Additional Responsibilities

### Privacy by Design

New systems or processes involving personal data must be reviewed by the Privacy Team. High-risk processing requires a Data Protection Impact Assessment (DPIA).

### Data Breaches

All suspected breaches must be reported immediately to the Privacy Team. The Group is required to notify the ICO within 72 hours if necessary.

### Third-Party Processors

Due diligence and contractual safeguards are required when engaging third-party data processors.

### International Transfers

Data transfers outside the UK/EU require appropriate safeguards and Privacy Team approval.

### Data Subject Rights

Individuals have rights including access, correction, and deletion of their data. Requests must be handled promptly and forwarded to the appropriate team.

### Use of AI

AI systems processing personal data must comply with data protection principles. DPIAs are required for high-risk AI applications.

## Governance & Support

### Data Protection Officer (DPO)

The DPO oversees compliance and can be contacted at [dataprotection@jet2.com](mailto:dataprotection@jet2.com).

### Departmental Data Protection Accountable Managers (DPAMs)

Each department has a designated DPAM to support data protection compliance.

## Training & Awareness

Regular GDPR training is provided to all colleagues. Enhanced training is available upon request.