GRAY DAWES
TRAVEL

GDPR Policy

Version Issued

21/02/2025

Suzanne Horner
CEO

GDPR Compliance Procedure

Context and Overview

Key Details

- Policy prepared by: Jeffery Paul (Data Protection Officer)
- Approved by: Suzanne Horner (Chief Executive Officer)
- Policy became operational on: 4th April 2022

Our Commitment

Gray Dawes Group ensures compliance with all relevant laws regarding data storage, management, and control. These include, but are not limited to:

- The General Data Protection Regulation (EU GDPR) (Regulation (EU) 2016/679)
- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018 (DPA 2018)

We will keep customers, suppliers, and staff updated on policies and procedural changes implemented to ensure ongoing compliance.

Why this policy exists

This data protection policy ensures that Gray Dawes Group:

- Complies with data protection law and follows best practices
- Protects the rights of staff, customers, and partners
- Is transparent about how it stores and processes personal data
- Protects itself from the risks of a data breach

Review of this policy

This policy will be reviewed and updated quarterly by the Data Protection Officer (DPO) in consultation with senior management and the CEO.

Annual compliance assessments will also be conducted to ensure continued adherence to regulatory frameworks, including UK GDPR, EU GDPR, and DPA 2018.

Under GDPR, the data protection principles set out the main responsibilities for organisations. Personal data must:

- Be processed lawfully, fairly, and transparently
- Be collected for specified, explicit, and legitimate purposes
- Be adequate, relevant, and limited to what is necessary
- Be accurate and kept up to date
- Not be retained for longer than necessary
- Be processed securely to maintain confidentiality and integrity

GDPR Compliance Procedure

Scope of this Policy

This policy applies to:

- The head office and all branches of Gray Dawes Group
- All employees of Gray Dawes Group
- Contractors, suppliers, and other individuals working on behalf of Gray Dawes Group
- Digital systems and third-party service providers supporting Gray Dawes Group

It applies to all personal data the company holds, including:

- Name
- Passport information
- Date of birth
- Visa details
- Contact information
- Home address
- Frequent traveller and other memberships
- Payment details

Data Protection Risks

Adherence to this policy will mitigate data security risks, including breaches of confidentiality and cyber threats.

Responsibilities

All personnel at Gray Dawes Group are responsible for ensuring data is collected, stored, handled, and processed in line with this policy and data protection principles.

- *CEO (Suzanne Horner)*: Holds ultimate accountability for ensuring the organisation remains legally compliant and resilient in data protection matters. She provides strategic leadership, ensures adequate resource allocation for compliance initiatives, and fosters a culture of data protection awareness throughout the company.
- *DPO (Jeffery Paul)*: is responsible for implementing and maintaining data protection policies across Gray Dawes Group. He provides training and awareness programmes to employees, acts as the primary point of contact for regulatory authorities, and oversees compliance with GDPR and other relevant data protection laws. Additionally, he conducts regular audits and risk assessments to identify and mitigate data security vulnerabilities.
- *Chief Technology Officer (Sophie Taylor)*: is accountable for maintaining a secure IT infrastructure that safeguards personal data. She ensures that appropriate cybersecurity measures, such as encryption, access controls, and incident response plans, are in place. Furthermore, she evaluates the security posture of third-party service providers and continuously enhances digital safeguards against cyber threats.
- *Marketing Director (John Cooper):* ensures that all marketing activities align with data protection regulations. He oversees consent management for marketing communications, ensuring that customer data is used appropriately and in accordance with GDPR. He works closely with the DPO to monitor the secure handling of personal data within marketing databases and ensures transparency in customer interactions.

- *Chief Operating Officer (David Bishop)*: is responsible for managing supplier contracts and ensuring third-party compliance with data protection and security requirements. He conducts due diligence on external service providers, oversees annual supplier audits, and ensures that vendors adhere to GDPR and contractual obligations. Additionally, he integrates data protection controls into operational processes to maintain compliance and security across business operation.

General Data Handling Guidelines

- Data should only be accessed by authorised personnel for legitimate business purposes.
- Personal data should not be shared informally or outside of approved systems.
- Employees must follow encryption and secure data transmission guidelines.
- Workstations must be locked when unattended to prevent unauthorised access.

Data Use- Traveller Profiles

- Traveller profiles are maintained to facilitate booking and travel management services.
- Data collected includes personal information, travel preferences, payment details, and loyalty program memberships.
- Profile data is processed only with traveller consent or under contractual obligations.
- Travellers have the right to access, modify, or request the deletion of their profile data.
- Data security measures, including encryption and restricted access, ensure confidentiality.

Data Use – Marketing

- Personal data is used for marketing purposes only when explicit consent has been obtained.
- Marketing communications comply with GDPR.
- Users can opt out of marketing communications at any time.
- Marketing databases are regularly reviewed to ensure data accuracy and compliance.

Data Control and Record Policy

- Gray Dawes Group maintains accurate records of **data processing activities** under **GDPR Article 30**.
- Processing activities are documented to ensure compliance and support regulatory audits.
- Security controls, access restrictions, and audit logs ensure controlled data access.
- Employees handling sensitive data are trained to comply with record management policies.

Data Storage and Security

- Gray Dawes Group operates a paperless environment, ensuring digital security measures for data. Any printed data must be stored securely and shredded immediately after use.
- Data is encrypted in storage and transit to prevent unauthorised access.
- Servers and cloud-based solutions are continuously monitored for security compliance.
- Data backups must be conducted and tested regularly.
- Data transfers outside the UK/EU must comply with GDPR-approved safeguards (e.g., Standard Contractual Clauses, IDTA).

Data Use Policies

- Personal data should only be used for its intended purpose and processed with consent.
- Unauthorised access or modification of personal data is strictly prohibited.
- Employees must adhere to clear guidelines on handling and transferring sensitive data.

GDPR Compliance Procedure

Data Accuracy and Maintenance

- Employees must verify customer and employee data to ensure accuracy.
- Outdated or incorrect data must be updated promptly.
- Personal data no longer required should be securely deleted in accordance with the data retention policy.

Data Deletion Policy

- Personal data is retained only as long as necessary for operational or legal purposes.
- Unnecessary data is securely deleted using approved deletion methods.
- Data subjects may request data erasure, which will be processed in accordance with GDPR regulations.
- Regular audits ensure compliance with data retention and deletion policies.

Data Release Policy

- Personal data is only released under **explicit authorisation** and for **legitimate purposes**.
- Data requests from clients, travellers, or regulatory bodies are processed securely.
- Data is transferred using encrypted methods to prevent unauthorised access.
- A record of all data releases is maintained for compliance and audit purposes.

Incident and Data Breach Response

- Any suspected or actual data breach must be reported immediately to the DPO.
- Incidents are assessed based on their impact, including whether they involve cross-border data processing.
- If a breach poses a high risk to individuals, affected parties will be informed within 48 hours.
- The ICO will be notified within 72 hours of any significant breach.
- A full investigation and post-incident review will be conducted to strengthen security measures and prevent recurrence.

Subject Access Requests

- Data subjects have the right to request access to their personal data.
- SARs must be submitted to the DPO.
- Requests will be processed within one month unless deemed excessive, in which case a reasonable fee may be charged.

Data Disclosure for Legal Purposes

- Personal data may be disclosed to law enforcement or regulatory bodies when legally required and assessed by the DPO for compliance.
- International data transfers comply with Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to ensure GDPR compliance.
- Transfers outside the EEA require risk assessments and safeguards.
- Third-party contracts include legally binding data protection and security clauses.
- Affected individuals will be informed unless legally prohibited.
- All disclosures are logged for compliance tracking. to law enforcement or regulatory bodies when legally required and assessed by the DPO for compliance.

GDPR Compliance Procedure

Data Processing Activities

- Gray Dawes Group primarily acts as a **data processor**, managing client traveller profiles and related information.
- Data processing includes collection, storage, retrieval, transmission, and deletion, ensuring secure handling at all stages.
- Encryption, access control, and audit trails are used to maintain data integrity and confidentiality.
- Data is only processed as per contractual agreements, with no unauthorised repurposing.
- The company does not engage in automated decision-making or profiling that produces legal or significant effects on individuals.
- If automated processing is introduced in the future, it will be reviewed for GDPR compliance, and individuals will be informed of their rights regarding such processing.

Auditing and Compliance Measures

- Internal audits are conducted quarterly to ensure adherence to data security and privacy policies, including GDPR, UK GDPR, and DPA 2018.
- Annual external audits validate compliance with industry standards and global data protection laws, including CCPA (California Consumer Privacy Act), and PDPA (Personal Data Protection Act in Singapore and other jurisdictions where applicable).
- Third-party suppliers are audited annually to confirm compliance with contractual and regulatory obligations, ensuring that any data shared with vendors meets the highest security and privacy standards.
- Employee training is regularly updated to cover not only GDPR but also international data protection regulations, ensuring a global standard for compliance.
- Compliance reports and risk assessments are documented and reviewed by senior management to align with evolving global regulatory requirements.
- Data protection impact assessments (DPIAs) are conducted where required to assess risks related to new processing activities or system implementations, in line with GDPR and other regulatory frameworks.

Employee Data Management

- Employee personal data is collected and processed in compliance with applicable employment and data protection laws across different regions where Gray Dawes Group operates.
- Data is processed for legitimate HR and operational purposes, such as payroll, benefits administration, and performance management.
- Employee records are securely stored and retained only for the legally required period in each jurisdiction.
- Access to employee data is strictly restricted to HR personnel and authorised individuals on a need-to-know basis.
- International employee data transfers comply with GDPR and relevant local regulations through mechanisms such as Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs).
- Employees have the right to access, update, or request deletion of their personal data, subject to applicable legal and contractual obligations.
- Specific policies are in place to govern the processing of sensitive employee data, including health records and background checks, in alignment with global privacy laws.

Compliance Declaration

- All employees, contractors, and third-party service providers must comply with this policy.
- Regular training is provided to ensure ongoing data protection awareness.
- Non-compliance with data protection policies may result in disciplinary action or contractual termination
- Leadership fosters a culture of accountability and transparency in all data processing activities.