GRAY DAWES
TRAVEL

GDPR Policy

Version Issued

04/04/2022

Suzanne Horner
CEO

GDPR Compliance Procedure

Context and Overview

Key Details

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

Our Commitment

The Gray Dawes Group will ensure that it complies with all laws relating to the storage, management and control of data. These include, but are not limited to, the General Data Protection Regulation (UK-GDPR) and The Data Protection Act 2018 (DPA 2018) (EU) 2016/679 (new legislation from 31 January 2020). We will endeavour to keep customers, suppliers, and staff updated on policies and procedural changes implemented.

Why this policy exists

This data protection policy ensures the Gray Dawes Group:

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

Review of this policy

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

These rules apply regardless of whether data is stored electronically, on paper or on other material.
Under the GDPR, the data protection principles set out the main responsibilities for organisations. These state that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects

GDPR Compliance Procedure

Policy Scope

This policy applies to:
The head office of Gray Dawes Group
All branches of Gray Dawes Group
All staff employed by Gray Dawes Group
All contractors, suppliers and other people working on behalf of Gray Dawes Group
It applies to all data that the company holds that can identify an individual. This can include:

- Name
- Passport information
- Date of birth
- Visa information
- Mobile phone number and contact details
- Home address
- Frequent Traveller & other memberships
- Form of payment

Data Protection Risks

Adherence to this policy will protect Gray Dawes Group from data security risks, including breaches of confidentiality.

Responsibilities

Everyone who works for or with Gray Dawes Group has responsibility for ensuring data is collected, stored, handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The CEO, Suzanne Horner, is ultimately responsible for ensuring that Gray Dawes Group meets its legal obligations.

The DPO Richard Munday, is responsible for:
Keeping the CEO updated about data protection responsibilities, risk and issues.
Reviewing all data protection procedures and related policies, in line with an agreed schedule.
To facilitate data protection training to all employees to help them understand their responsibilities when handling data and to ensure that they are fully aware of this policy.

Handling data protection questions from staff and anyone else covered by this policy.
Dealing with requests from individuals to see the data Gray Dawes Travel holds about them (also called 'Subject Access Requests.')

The Chief Technology Officer, Sophie Taylor, is responsible for:
Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
Performing regular check s and scans to ensure security hardware and software is functioning properly.
Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

GDPR Compliance Procedure

The Marketing Director, John Cooper, is responsible for:
Approving any data protection statements attached to communications such as emails and letters.
Addressing any data protection queries from journalists or media outlets like newspapers.
Where necessary, working with other staff to ensure marking initiatives abide by data protection principles.

The Chief Operating Officer, David Bishop, is responsible for:
Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
To audit key suppliers on a 12-monthly basis to review their data protection policies and standards. The adequate completion of this audit logged in the Supplier Data protection log. This is reviewed by the DPO.

General Staff Guidelines

The only people able to access data covered by this policy should be those who need it for their work.
Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
In particular, strong passwords must be used and they should never be shared.
Personal data should not be disclosed to unauthorised people, either within the company or externally.
Data should be regularly reviewed and updated if it is found to be out of date. If no longer required by the Business or by Law, it should be deleted and disposed of.
Employees should request help from their line manager or the DPO if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Head of Technology.
When data is stored on paper, it should be kept in a secure place where unauthorised people cannot access it.
These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
Gray Dawes Group is actively working towards a paper free environment, however if still in use, any paper or files should be kept in a locked drawer or filing cabinet.
Employees should make sure paper and printouts are not left where unauthorised people could seem them, like on a printer.
Staff should avoid printing out data wherever possible and print only in exceptional circumstances. Data printouts should be shredded and disposed of securely (shredded) on the day when they are no longer
When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
Data should be protected by strong passwords that are changed regularly and never shared between employees.
The business does not permit the storage of data on removable media (like a CD or DVD.) All computers are locked down to prevent this.
Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
Servers containing personal data will be sited in a secure location, away from general office space.

GDPR Compliance Procedure

Data will be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
All servers and computers containing data will be protected by approved security software and a firewall.
Owing the nature of travel business that requires travel and accommodation to be made to destinations throughout the world, data pertaining to reservations may be processed by suppliers outside of the European Economic Area (EEA) and US Privacy Shield framework.
Gray Dawes primary GD technical suppliers currently host data in the following locations:

- Travcom (UK)
- Travelport (US)
- Evolvi (UK)
- Atriis (Western Europe)
- Agentivity (Western Europe)
- Grapevine (UK)

In regard to the July 2020, Court of Justice of the European Union (CJEU) ruling determining the EU-US Privacy Scheme as invalid, Travelport have implemented the 'European Commission's model contracts', more commonly referred to as 'Standard Contractual Clauses'. You can read more about this on their website here: https://www.travelport.com/privacy

Data Use

Gray Dawes Travel will only process data that is required for legitimate business reasons. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:
When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
Personal data should not be shared informally.
Data must be encrypted before being transferred electronically. The Head of Technology can explain how to send data to authorised external contacts.
Should there be a business requirement to transfer personal data will always endeavour to put in place adequate safeguards to protect the rights of the data.

Data Accuracy

The law requires Gray Dawes Travel to take reasonable steps to ensure data is kept accurate and up to date.
The more important it is that the personal data is accurate, the greater the effort Gray Dawes Travel should put into ensuring its accuracy.
It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
Gray Dawes will make it easy for data subjects to update the information Gray Dawes holds about them. .
Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

GDPR Compliance Procedure

Data Breach

Gray Dawes Travel will respond to any personal data breaches (including unauthorised access/loss) that may occur, in adherence to the ICO guidelines.
The DPO and/or CEO are responsible for managing data breaches.
An ongoing training plan will ensure that staff will know how to escalate a security incident to the DP and/or CEO.
We have a process to inform affected individuals within 48 hours of being made aware of a data breach when it is likely to result in a high risk to their rights and freedoms.
We document all breaches (Data Protection Activity Log), even if they do not all need to be reported to the ICO. You must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.
In the event of the traveller or any authorised party wishing to make a complaint, this should be placed in writing (email or recorded post) and addressed to the DPO or CEO. An acknowledgement receipt will be issued within 72 hours of receipt.

Subject Access Requests

All individuals (clients and personnel) who are the subject of personal data held by Gray Dawes Group are entitled to:
Ask what information the company holds about them and why.
Ask how to gain access to it.
Be informed how to keep it up to date.
Be informed how the company is meeting its data protection obligations.
If a request for information is received, this is called a subject access request.
Subject access requests from individuals should be made to the DPO.
The DPO will maintain a record of subject access requests (Data protection activity log).
The Gray Dawes Group will provide a copy of the information free of charge. However should we receive an unfounded or excessive subject access request we may charge individuals £10 per enquiry. The DPO will endeavour to respond to a subject access request promptly, and in any event within 40 calendar days of receiving it.
The DPO will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data For Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.
Under these circumstances, Gray Dawes Group will disclose requested data. However, the DPO will ensure the request is legitimate, seeking assistance from the CEO and from the company's legal advisers where necessary.

Data Applications

For the purpose of GDPR regulations, Gray Dawes Group acts as a data processor.
For clarity, Gray Dawes Group stores and processes traveller profile information for the purpose of acting on behalf of the traveller. Gray Dawes Group does not determine at any time the purpose for which this information is used, only acting once we have instruction to do so.

GDPR Compliance Procedure

Audit and Compliance

Audit

Adherence to the policy will be audited through ISO27001:2013 quality control system. The DPO is responsible for completing internal audits on a quarterly basis. The DPO will then report back to the CEO and Senior Management Team outlining their findings and proposals for further process enhancements.

New key suppliers cannot be added without an audit of their data protection policy and completion of due diligence. A Copy of their policy must be provided to the DPO.

We audit our key suppliers on a 12-monthly basis to review their data protection policies and standards. The adequate completion of this audit logged in the Supplier Data protection log. This is reviewed by the DPO.

Security – access is 2 factor authenticated (256AES.) Access is only permitted to individuals on a needs to know basis within the business. Every action is fully audited and access is recorded and audited.

Compliance

All employees of Gray Dawes Group must comply with this policy and the spirit of overall Data Protection. Data protection will be consciously built into every aspect of Gray Dawes business interactions.

Information Management Policy

Collection of data – Client Traveller Profiles

For a traveller profile to be built, we will seek consent to be provided by the traveller for information to be stored for future use and reference. This which can be found at www.gdg.travel or other authorised form containing a data consent statement.

We will alternatively accept consent from the corporate under the terms of the contract between the corporate and GDG.

We are unable to build a traveller profile without the completion of a form with consent or contractual terms from the corporate.

Information collected for the purpose of making a booking, where we are acting as a data processor, will not be stored as a traveller profile without the express permission of the traveller.

Data Use - Traveller Profiles

The information contained within a Traveller Profile will only be used for the completion of a travel booking request and its associated management before, during and after travel. As such we act upon the data solely at the request of the traveller or their agencies and as such remain a Data Processor. In the act of performing this task, we may securely transmit this data to our partner suppliers (such as hotel booking platforms or airline) who will act upon this data in their own right as a Data Processor.

Data Use - Marketing

We will not send any data to 3rd party organisations with the purpose of marketing and we do not purchase data lists. We operate fully in accordance with the Privacy and Electronic Communication Regulations (PECR) for all our email marketing activities. We send e-alerts and regular, relevant travel related content to our clients' personnel. We operate a fully GDPR complaint consent based, double opt-in e-marketing to non-clients. All e-marketing will be directly related to the services that we offer and come with a one click unsubscribe option and clearly displays our corporate name and contact details.

GDPR Compliance Procedure

Data Control and Record Policy

Client Traveller Profiles (personal & business)
The table below outlines the data held within a profile that may be classed as personal data:

PNR / journey information	Dietary requirements	Personal preferences
Name	Visa information	Memberships
Passport details	Date of Birth	Personal email
Mobile number	Home address	Form of Payment

The reasons for storing such information in the usual course of business is defined as follows:
PNR / Journey Information – this is the information relating to a current or past booking itself including:
Dates of travel
Times of travel
Routing information
Supplier choice and detail
Cost
Dietary Requirements – in the event of specific dietary requirements / preferences for airlines or hotels
Personal Preferences – this information may include seating requirements, preferred departure points, times of travel or supplier preferences. Information is used (where provided) in order to provide a high-quality service and comply with appropriate legislation
Passport Details – information including numbers, nationalities and expiries may be used in order to add to reservations to complete the booking or for countries that require Advance Passenger Information (APIS) prior to travel.
Date of Birth – this may be used alongside Passport Details as well as for ensuring that correct supplier pricing and discounts are applied
Memberships – traveller may choose to be members of supplier frequent traveller membership schemes. Such information is added to the reservation at time of booking in order to enable the benefit throughout the booking and travel process.
Mobile Number – used for contacting the traveller during the course of the booking or for emergency purposes.
Home Address – information is contained for travellers that require documentation to be regularly sent to them or for service (e,g, car collections) to commence from home.
Personal Email – this would be used only in circumstances where the traveller has expressly requested that correspondence be sent to them via this channel rather than a company / employment email.

GDPR Compliance Procedure

Data Deletion Policy

Client Profile Deletion
A traveller profile will be deleted from our systems
Upon request received in writing from the traveller
Upon request from the traveller's company upon the conclusion of a contract.
After 18 months in-activity
Booking records where we act as a Data Processor will be stored in our systems for 12 months for the fulfilment of contract by providing client historical travel reports/patterns etc for negotiation of supplier deals.
Management Information including name and journey detail is stored for the purpose of providing a financial, accounting and statistical record of a journey taken. Such information is held for up to 7 years.
Accounts records will be held for the legal minimum period, currently 7 years.

Data Release Policy

Who can apply for information, why and how
We will not disclose the full contents of a traveller profile to any individual that is not the traveller.
We will only disclose booking information to the following:
The traveller
The travel booker (when this is not the traveller)
The key client contact (or nominated individual(s)) for the overall contract management when the reservation has been paid by the client company.
A third-party data supplier (such as data aggregator or security partner) where we have received a Data Release Authority (DRA) from the client company.

Employee Data

Treatment of data in the employment process:
Prospective employees – as part of the recruitment process there are items of personal data given which will only be held for the duration of the recruitment process and will only be held longer if the offer of employment is made. Some items of data such as employment history are required for the assessment of suitability for the position available. At the end of the recruitment campaign the data received will be destroyed. No automated processing is used during the recruitment process.
Current employees – During employment, data will be retained while there is a legal or contractual need for it to be retained. All employees have access to their record within the HR database and can see data held. Data will be shared with benefit providers where the employee has requested to be in receipt of the benefit
Former employees – Once employment has ended, data will only be held for the duration required by law. In terms of financial data, salary, tax etc this will be for a period of six years. All data not required will be destroyed.
Full details of the data held and the retention periods applicable can be found in the data processing schedule available on the intranet site.

As data subjects, employees are able to make a Subject Access Request (SAR) which should be directed to the Data Protection Officer.