Data Protection Policy

arrangeMY's (AM) focus is to provide business travel services to the employees of businesses with whom they work alongside and for. In doing so, AM receives individual data from the corporate clients.

Data Protection Principles
AM adheres to the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

arrangeMy process personal data under the following lawful bases:

- **Contractual necessity** – to arrange and manage travel services
- **Legal obligation** – compliance with financial, tax, or regulatory requirements
- **Legitimate interests** – improving services, reporting, and operational efficiency
- **Consent** – for specific activities (e.g. marketing communications, optional services) – Where consent is relied upon, it can be withdrawn at any time.

Categories of Personal Data
We may collect and process:

- Identification data (name, date of birth)
- Contact details (work email address)
- Travel information (e.g. itinerary, preferences, passport information for flight bookings)
- Financial data (for the corporate client, employer, no individual's financial data)
- Sensitive data where necessary (e.g. dietary requirements, accessibility needs)

When servicing a given corporate client, AM may create a "Traveller Profile" with travel data for each traveller, which is kept on file as a reference document and consulted each time a reservation is to be made. When a reservation is made, AM creates a "passenger name record" (PNR), which contains all of the information, needed to fulfil the travel request of each traveller. Based on the travel expenses incurred by travellers of each corporate client, AM produces reports that summarise and analyse the travel trends of that client.

What we do with the information:
In addition to creating Traveller Profiles and PNRs, AM uses the travel data with the consent of the traveller for the following travel and other travel-related purposes.
Reservations: AM may need to transfer travel data to various third party travel suppliers and computer reservation systems for the purposes of making reservations within the traveller's home country or to another country where the traveller may be travelling.
Consolidation of Travel Data: At the request of the corporate client (the traveller's employer), AM or a third party prepares information reports that summarise and analyse the travel expenditures per destination, per travel supplier, etc.
Compliance with Travel Policy: Also at the request of the corporate client, AM may report on the compliance of the travellers with the travel policy of the client and identify any exceptions to the compliance.
Collecting Travel Payments: AM may transfer travel data to third parties in the traveller's home country or in another country for the purpose of collecting payments related to travel reservations.
New products and Services: Also with the goal of improving service and based on the data given to AM, we may send additional information to the traveller if it applies to his/her trip. An example would be a list of restaurants near a specific hotel, in a specific city.

AM as a Data Controller or a Data Processor:
Depending on the engagement:

- **As Data Controller**: AM determines how and why traveller data is processed
- **As Data Processor**: AM processes data on behalf of the corporate client

Where acting as a processor, AM:

- Follows documented client instructions
- Ensures confidentiality
- Supports data subject rights
- Allows audits where contractually required

Measures we are taking:
AM is implementing, step-by-step, a process through which we will standardise the way our company and its affiliates handle travel data.

Transfer to Third Parties: Prior to a transfer, third parties (except for travel suppliers such as the airlines, computer reservation systems, hotels, etc.) may be required to sign a transfer agreement with AM, which requires them to follow the applicable data protection laws. This will ensure that even if the laws governing the third party are less strict than our standards, the level of protection that the traveller's data receives will be consistent. For instance, data consolidators are required to sign an agreement.

Security: Pursuant to the various data protection laws, AM is implementing appropriate technical and organisational measures to protect the personal travel data, obtained from our clients' travellers, against accidental or unlawful disclosure or destruction. The measures are being determined for each department, according to their handling of the travel data.

Destruction: Under many data protection laws, Personal data is retained only as long as necessary:
Travel records: typically **6–7 years** (for tax and audit purposes)
Traveller profiles: retained while client relationship is active
Marketing data: until consent is withdrawn
Data is securely deleted or anonymised after the retention period.

Our policy may be subject to additional requirements in compliance with local legislation in certain countries (please see below, under “Notes”).

Infrequent travellers: If the client provides personal data to us about a traveller, they must ensure that they are entitled to disclose that data to us and that without us taking any further steps required by privacy/data protection laws, we may collect, use and disclose such information for the purposes described above. For example, the client should take reasonable steps to ensure the individual traveller concerned is aware of the various matters detailed in this AM Privacy/Data Protection Policy as those matters relate to that individual, including our identity, how to contact us, our purposes of collection, our information disclosure practices, the individual's right to obtain access to the data and the consequences for the individual if the data is not provided.

Data Security
arrangeMY implement appropriate technical and organisational measures, including:

- Access controls and authentication
- Encrypted systems and secure data transfer
- Staff training and confidentiality obligations
- Regular security reviews and risk assessments

Data Subject Rights
Individuals have the right to:

- Access their personal data
- Rectify inaccurate data
- Request erasure (“right to be forgotten”)
- Restrict processing
- Data portability
- Object to processing (including marketing)
- Withdraw consent where applicable

Requests can be made via: support@arrangemy.com

Complaints
Individuals have the right to lodge a complaint with:
Information Commissioner’s Office (ICO)
Website: https://ico.org.uk
We encourage individuals to contact us first to resolve concerns.

Data Breaches
In the event of a personal data breach:

- Incidents will be reported internally immediately
- Risk assessments will be undertaken
- Where required, breaches will be reported to the ICO within 72 hours
- Affected individuals will be notified where there is high risk

Third-Party Processors
All third parties must:

- Enter into a Data Processing Agreement (DPA)
- Comply with GDPR
- Implement appropriate security measures

<u>This policy will be reviewed every 12 months from April 2026</u>

Signed:  Dated: 16/04/26