Data Protection Schedule ("Schedule") to Order Form

1 This Data Protection Schedule applies as linked to the Order Form (including the Business Travel Terms and Conditions and/or Meetings & Event Services Terms and Conditions as applicable) (collectively, "Agreement") between Reed & Mackay Travel Australia Pty Limited ("R&M") (ABN 32 623 184 387) whose principal office is at Concierge House, 332 Kent St, Sydney NSW 2000 and you the Client. Defined terms used elsewhere in the Agreement shall have the same meaning in this Schedule. Where R&M processes Data on behalf of the Client, R&M shall:

1.1 only use the Data to:

(a) perform its obligations under this Agreement and process such Personal Information in accordance with the Client's written instructions; and/or

(b) comply with the Data Protection Legislation or the Relevant Laws (provided that R&M has, prior to the relevant processing, informed the Client of such requirement (unless the Relevant Law prohibits such notification));

1.2 subject to Paragraphs 2, 4 and 5 (inclusive) of this Schedule, implement and maintain appropriate technical and organisational measures to protect Data processed in connection with this Agreement from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access;

1.3 take all reasonable steps to ensure the reliability of any of the R&M Employees or Personnel who have access to Data processed in connection with this Agreement and ensure that all such R&M Employees or Personnel are bound by enforceable obligations of confidentiality;

1.4 taking into account the nature of the processing, assist the Client by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Client's obligation to respond to requests from Individuals exercising their rights with regard to the processing of their Data;

1.5 assist the Client in ensuring compliance by the Client with its obligations under applicable Data Protection Legislation to the extent required by law, taking into account the nature of the processing and the information available to R&M;

1.6 notify the Client without undue delay, and in any event within 48 hours upon becoming aware of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Data processed by R&M in connection with this Agreement;

1.7 make available to the Client, within a reasonable period of time following notice from the Client, all information necessary to demonstrate compliance with the obligations set out in this Schedule and allow for and contribute to audits, including inspections, conducted by the Client or another auditor mandated by the Client provided any such audits, and/or inspections occur only on one (1) occasion in any twelve (12) month period, that such inspections, and/or audits are strictly limited to R&M's arrangements for compliance with this Schedule, such inspections, and/or audits are carried out during normal business hours, and the Client (or the relevant third party conducting such an audit) provides R&M reasonable prior notice of such an audit, and/or inspection in writing and the scope of such an audit, and/or inspection is agreed with R&M prior to its commencement;

1.8 immediately notify the Client, if in R&M's opinion, any instruction or direction from the Client infringes Data Protection Legislation; and

1.9 at the Client's choice, delete or return to the Client all Data when the Services cease to be provided to the Client, and delete all then existing copies (unless required to be retained by R&M by applicable law).

2 The Client acknowledges and agrees, and shall ensure that the Travellers and Users acknowledge and agree, that it is necessary for R&M to provide Data to Service Providers (whether or not within the Territory) in order to provide Services.

3 The Client acknowledges and agrees that R&M shall be authorised to use Sub-Processors in relation to the processing of Data on the Client's behalf for the provision of the Services under this Agreement. A list of Sub-Processors used by R&M is available here . R&M shall inform the Client of any changes to the list of Sub-Processors, including the addition of any new Sub-Processors. If the Client objects to a change to the list of Sub-Processors, the Client shall notify R&M in writing within 15 days of the updated list of Sub-Processors being published. If the Client provides R&M with such a notification, where possible, R&M will perform its obligations under this Agreement without the processing of Data in connection with this Agreement by the new Sub-Processors. However, if it is not reasonably feasible for R&M to perform its obligations

under this Agreement without the processing of Data in connection with this Agreement by the new Sub-Processors, R&M shall notify the Client of the same, and the Client shall be entitled to terminate this Agreement on thirty (30) days prior written notice to R&M. In the event that the Client does not object to any change or addition to the list of Sub-Processors within 15 days of the updated list being published by R&M, the Client shall be deemed to have approved any changes and/or additions to the list of Sub-Processors. R&M remains responsible and liable for any acts or omissions of its Sub-Processors. R&M shall ensure it has a written contract with the Sub-Processors which contains terms for the protection of Personal Information which are no less protective than the terms set out in this Schedule

4 Without prejudice to Paragraph 2 above, and notwithstanding any other provision in this Agreement, the Client:

(a) hereby consents to R&M transferring Data to any Service Provider (whether or not within the Territory) for the purposes of supplying the Services in accordance with this Agreement; and

(b) hereby acknowledges that R&M transferring the Travellers' and the Users' Data to Service Providers is reasonably necessary for, or directly related to the provision of this Agreement.

5 In light of Paragraph 2 above, R&M shall use its reasonable endeavours to help the Client to respond to any failure (whether act or omission) by a Service Provider to process Data in accordance with appropriate and industry standard methods but R&M shall otherwise have no liability to the Client, any member of the Client's Group or any Traveller or User (whether in contract, tort (including negligence or breach of statutory duty), misrepresentation or otherwise) arising out of or in connection with any Service Providers' processing, using, misusing, losing, damaging or corrupting Data, or otherwise infringing a person's rights in relation to Data.

6 Without prejudice to Paragraphs 2, 4 and 5 above (inclusive) of this Schedule, the Client shall ensure that the collection and disclosure of Data is necessary for, or directly related to, one or more of the Client's functions or activities, and has provided Travellers and Users with all necessary information to enable the Data to be lawfully provided to R&M in accordance with the Data Protection Legislation.

7 The Client acknowledges and agrees that Annex 1 to this Schedule contains certain details relating to the processing of Data by R&M pursuant to this Agreement.

8 The Client acknowledges and agrees that it shall bear the cost of, and reimburse R&M for, reasonable costs and expenses incurred by R&M in providing assistance as described in paragraphs 1.4 and 1.5 above.

Annex 1

Data Processing Activities

Categories of Personal Information	Traveller and/or booker details – title, forename, middle name, surname, known name (if different), gender, date, place and country of birth, country of residence, nationality, marital status; location of Traveller – destinations and locations on trip. Company Information – company name, department, cost centre, account number, job title, employee number Main contact details – addresses (home, offices etc), telephone numbers, fax numbers, mobile telephone numbers, email address Travel Booker/PA Information – name, telephone number, email address Methods of payment – card type, card number, expiry date, usage preferences, debit/credit, personal/business Documents – Passport - passport country, issue country, passport number, forename, middle names, surname, date of issue, date of expiry, biometric (Y/N) Visa (inc. ESTA, Redress, Schengen, Work Permit, Global Entry) – visa county, issue country, type of visa, document number, issue date and date of expiry TSA – TSA number, start date, expiry date Driving Licences – country, licence number, forename, middle name, surname, start date, expiry date, provisional (Y/N), international (Y/N) ID Cards – country, ID card number, forename, middle name, surname, start date, expiry date Vaccine and Covid and health information as required for bookings Travel Preferences – Air - seat type, home airport, on-line check-in preference, meal type Car – category, style, transmission, fuel/aircon, satnav (Y/N), Rail – seat allocation, meal type Eurostar – coach number, seat number, seat type, seat allocation, meal type Hotel - smoking/non smoking, preferred room type Any accessibility requirements for trip Memberships – loyalty cards - service type, supplier, membership number, date of expiry, status, level Personal Hobbies/Interests
Categories of individuals whose Personal Information is used	Employees and guests of client, and others for whom the Client requires travel
Processing Operations	Provision of travel and travel-related services
Purposes	Provision of travel and travel-related services
Duration	Financials – duration of contract + 7 years Profiles – duration of contract, reviewed annually and deleted at request of Client

Annex 2 – Appendix 1

Description of Transfer

Categories of individuals whose Personal Information is transferred

As set out in Annex 1 under "Categories of individuals whose Personal Information is used ".

Categories of Personal Information transferred

As set out in Annex 1 under "Categories of data".

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

R&M do not routinely process sensitive data. When related to the travel service provided, sensitive data may be inferred e.g. where assistance is required (which may imply health conditions), vaccine and/or testing information (as required for bookings, which may imply health status), and meal preference (from which religion could be inferred). R&M applies the same high level of security measures to all Personal Information.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

The transfer is on a continuous basis for the purposes of provision of travel and travel-related services.

Nature of the processing

As set out in Annex 1 under "Processing Operations".

Purpose(s) of the data transfer and further processing

As set out in Annex 1 under "Purposes"

The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period

As set out in Annex 1 under "Duration".

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As set out in Schedule 3, Paragraph 3

Annex 2 – Appendix 2

Technical and Organisational Measures Including Technical and Organisational Measures to Ensure the Security of the Data

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Version 2.5 – July 2024 (as may be updated by R&M from time to time)

DEFINITIONS

"Staff" means Reed & Mackay's employees, contractors or consultants that are involved in the service Reed & Mackay provides to its clients.

"Data" means Reed & Mackay's Data, including any Client data provided to Reed & Mackay by the Client (Data Controller) in accordance with any Data Processing Agreements, Standard Contractual Clauses and/or contracts between the Client and Reed & Mackay.

INTRODUCTION

The Executive Team of Reed & Mackay recognises the significance of Information Security, and maintaining the highest standards of confidentiality, integrity, and availability of internal, customer and supplier information is fundamental to our Vision "To be the most valued, recommended and entrepreneurial travel, advisory and events business in the world".

As described in this document, Reed & Mackay maintains a set of Technical and Organisational Security Measures in line with Industry Best Practices and Standards and Certifications we maintain to mitigate the risks to data, information assets, service, performance, client confidence, or other areas of the business which may result from a failure in Information Security.

1. CERTIFICATIONS

1.1. Our head office maintains certification to ISO/IEC 27001, the international standard for Information Security Management, ISO 22301 - Business Continuity Management, ISO 9001 - Quality Management, and ISO 14001 - Environmental Management certifications. Reed & Mackay is also certified to PCI-DSS – The Payment Card Industry – Data Security Standard, which is also a pre-requisite of IATA licensing, and consequently taken very seriously by Reed & Mackay.

1.2. Certifications are maintained via an external and an internal audit program, which include periodic internal and annual external audits, and ongoing continual improvement activities.

2. INFORMATION SECURITY MANAGEMENT SYSTEM

2.1. Reed & Mackay's Information Security Polices set a clear direction for Information Security and demonstrate support for, and commitment to the management of Information Security throughout the company.

2.2. Information Security is managed through a stringent set of controls, including policies, processes, procedures, software, and hardware functions that constitute Reed & Mackay's Information Security Management System (ISMS). These controls are monitored, reviewed, and where necessary, improved to ensure that specific security and business objectives are met.

2.3. All Staff receive a comprehensive and mandatory induction and training programme on joining the company and an annual compliance refresher including Information Security and data protection.

2.4. The ultimate responsibility for Information Security lies with the Chief Information Officer but this responsibility is discharged through the designated role of Director of Security & Trust, who has primary responsibility for Information Security, Information Security Risk, Cyber Security, and Security Incident Management within Reed & Mackay and acts as the central point of contact for Information Security for both Staff and external organisations.

2.5. Heads of Departments are responsible for enforcing Information Security Policies within their business areas and for adherence by their Staff. All Staff have a responsibility for Information Security; ensuring that they follow relevant company policies, processes, and procedures; have a general awareness of importance of Information Security and the potential risks; reporting any incidents, events, or potential weaknesses.

3. HUMAN RESOURCE SECURITY

3.1. Reed & Mackay liaises closely with our recruitment agency contacts to ensure that pre-employment screening requirements are carried out on our behalf.

3.2. Reed & Mackay utilizes a third-party Employee Screening company to conduct background screening in line with the UK Government's Baseline Personnel Security Standard (BPSS) on all Staff regardless of their role, subject to limitations in accordance with local legislation.

3.3. Confidentiality clauses are in place in Staff contracts that provide adequate protection for the confidentiality of Reed & Mackay Data.

3.4. A disciplinary process is in place to address non-compliance with security policies and requirements.

3.5. Upon termination of employment, access is revoked from Staff on their last working day and all equipment and Intellectual Property is returned by the leaver.

4. ASSET MANAGEMENT AND DATA SECURITY

4.1. Assets associated with information and information-processing facilities are identified and an inventory of assets is maintained.

4.2. Information and Data is classified and managed in line with a management approved Information Classification, Asset & Data Management Policy.

4.3. Only trusted devices have access to Reed & Mackay corporate network resources. These include Reed & Mackay domain joined computers and mobile devices that have been enrolled with Reed & Mackay's Mobile Device Management Solution and comply with security policies.

4.4. Security controls requirements for personal and Reed & Mackay issued mobile devices are defined in the Mobile and Personal Device policy. The controls include, but are not limited to, encryption, remote wipe, and disabled USB ports.

4.5. All endpoints are encrypted. USB ports and the use of removable media is restricted.

4.6. Technical DLP measures as well as a Clear Desk & Clear Screen policy are in place to mitigate the risk of data leakage and inadvertent disclosure of Reed & Mackay Data.

4.7. A Data Retention Policy and Data Retention Schedule are in place to define data retention requirements in line with GDPR, as well as secure data disposal requirements of sensitive data on physical or electronic media to recognized IT industry security standards / best practice (e.g., CESG or DOD approved standards).

4.8. Media containing any information is destroyed using secure means of disposal in accordance with WEEE (Waste Electrical and Electronic Equipment) and CESG (Communications Electronics Security Group) approved data destruction standards. The Tech Services Department maintain records.

4.9. Documentation is destroyed securely either via the use of crosscut shredders or by using approved third parties providing services to BS EN 15713 security shredding standard and at least DIN P-3 security level, suitable for confidential documents.

5. ACCESS CONTROL

5.1. A Role Based Access Control model is in place with roles assigned to individuals based on job roles and need-to-know basis.

5.2. Separation of Duties and Least privilege Principles are followed, and privileged access is granted upon documented approval by senior management.

5.3. Privileged IT administrative rights are provided via a separate User ID (elevated account) to the users' normal User ID.

5.4. We monitor all events associated with logon to servers + workstations with administrative accounts and as well changes/modifications to privilege groups.

5.5. Access Rights Reviews are conducted periodically with the frequency depending on the criticality of the information asset and varying between quarterly to annually.

5.6. The Reed & Mackay Password Policy is defined as follows: Passwords must contain a minimum of 12 characters, at least one upper case letter, one lower case letter and one number or special character. Passwords must avoid international (non- ASCII) characters, shall not include a dictionary words or information about the user (such as the user ID, names of family members, date of birth, etc.), shall be changed at least once every 90 days, and cannot be the same as the 24 previously used passwords.

5.7. User accounts are locked out after 5 invalid logon attempts and will remain locked until an administrator or the user unlocks them (the latter is via self-service and multifactor authentication).

5.8. Multifactor authentication is enforced on all Reed & Mackay user and administrative accounts.

6. CRYPTOGRAPHY

6.1. As defined by Reed & Mackay's Cryptography Policy, cryptographic controls are employed to protect sensitive data both whilst in transit and at rest.

6.2. Encryption on Mobile Devices is enforced via Microsoft Intune Endpoint Manager policies.

6.3. PII Database encryption is in place via Thales CipherTrust (AES 256-Bit Encryption, data tokenisation and encryption services).

6.4. Database Encryption is in place using Transparent Data Encryption (TDE) AES-256 Encryption.

6.5. All traffic from/to our public facing applications (Websites + Mobile App) utilize HTTPS certificates issued by GlobalSign Certificate Authority and are encrypted with TLS 1.2 or higher.

6.6. All backups are encrypted.

7. OPERATIONS SECURITY

7.1. Changes to production environments are controlled in line with Reed & Mackay's IT Change Management Policy.

7.2. Malware detection, prevention, and recovery controls are in place via a next generation anti-malware solution.

7.3. A comprehensive patch management process is in place. Patches and security updates are deployed monthly, or more frequently if a significant security risk is identified. Patch management is subject to change control and the IT Change Management Policy.

7.4. A technical vulnerability management programme is in place including an ongoing programme of remediation. Vulnerabilities are identified via internal and external infrastructure scans, quarterly PCI-DSS ASV scans and penetration tests.

7.5. A comprehensive annual penetration test programme is in place, carried out by CREST accredited independent penetration testers. This covers all R&M's critical infrastructure.

8. LOGGING, MONITORING & SECURITY INCIDENT MANAGEMENT

8.1. Event logs recording user activities, exceptions, faults, and Information Security events are generated, retained, protected from tampering, and regularly reviewed.

8.2. A 24/7 Security Operations Centre (SOC) service is in place via a trusted third-party Managed Security Services Provider, which includes monitoring, log collection & analysis, security information & event management (SIEM), security incident response & mitigation, and forensic analysis capabilities to understand the cause of security incidents and methods of reducing or removing potential areas for attack.

8.3. Observed or suspected security incidents are reported centrally, logged automatically, and are followed up by the Security Incident Response Team in line with the Information Security Incident Response Plan and Data Breach Management Process if applicable.

9. CLOUD SECURITY

9.1. Reed & Mackay's Travel Management Platform and server infrastructure is hosted in Microsoft Azure's UK South data centre.

9.2. MS Azure is configured to encrypt information at rest regardless of the storage medium, be it a managed disk attached to a virtual machine, a storage account that contains telemetry data or application source code, or a platform database service like Microsoft SQL.

9.3. A management approved Cloud Security Policy is in place to define cloud security requirements.

9.4. A Cloud Security Posture Management solution is in place to monitor and manage governance across Reed & Mackay's Microsoft Azure-based assets and services including visualization and assessment of security posture, misconfiguration detection, and enforcement of security best practices and compliance frameworks.

9.5. Microsoft Network Security Groups and Next Generation Checkpoint virtual firewall appliances protect our environment on the perimeter with Intrusion Prevention enabled.

10. PHYSICAL SECURITY

10.1. In line with our Physical & Environmental Security Policy, adequate physical and environmental security measures are in place to prevent unauthorised physical access, damage and interference to Reed & Mackay Data, premises, and processing facilities. The following controls are in place:

10.1.1. Head Office: 24x7 manned building reception, Reed & Mackay office reception operates during office hours. CCTV at all building access points providing coverage of most common areas and the areas of entry and egress from the building. The IT Comms room is accessed using a swipe card system and keypad entry system. Entry is restricted to authorised individuals with a business need.

10.1.2. Regional Offices: Regional offices have the same controls implemented as Head Office, with some exceptions. Our smaller offices do not have 24/7 manned reception and or access card system, however compensating controls are in line with our Physical and Environmental Security Policy to ensure that physical security in these offices is adequate.

10.2. Visitors are granted access for specific and authorised purposes only and are always supervised / escorted whilst in Reed & Mackay offices. Visitor logs are maintained for all physical access to Reed & Mackay offices, server rooms and data centres hosting Reed & Mackay IT equipment and information assets.

11. COMMUNICATION & NETWORK SECURITY

11.1. Networks are managed through appropriate security controls such as network segmentation, network access management, firewalls, configuration standards and logging and monitoring.

11.2. Information transfer procedures and controls are in place to protect the transfer of Data using all types of communication facilities.

11.3. Our recommended data transfer protocol for regular data exchanges (e.g., data files, HR feeds) is to establish an SFTP connection between organisations - which party pushes/pulls the data is open to agreement between the parties.

12. SOFTWARE DEVELOPMENT

12.1. In-house software development follows Agile/Sprint life-cycle methodology and follows OWASP best practices.

12.2. An SDLC (Software Development Life Cycle) Policy is in place including requirements analysis and specifications, security by design, secure engineering principles, secure development environment, application support, QA, testing, implementation, training, and post-implementation review.

12.3. Single-Sign-On integration is available within our client-facing applications. SAML 2.0-based solutions, such as Azure AD, Ping Identity, Duo, and Okta are supported, other third-party options may also be supported, but may require development and testing.

12.4. Development, Test and Production systems are segregated. Anonymised data is used for testing purposes in non-production environments.

12.5. Client data is segregated using unique identifiers assigned at the time of account implementation. Segregation is ensured by using unique identifiers, e.g., Corporate ID's, Traveller ID's, and Account ID's.

13. SUPPLIER RELATIONSHIPS

13.1. New direct suppliers (including data sub-processors) undergo due diligence covering Information Security, Data Protection, Business Continuity, Corporate Governance and Quality, Health & Safety, Environment, Equal Opportunities, Diversity, Anti-Bribery & Anti-Corruption, Modern Slavery and Child Labour, Ethical Business Practices / Corporate Social Responsibility as well as a credit check, a review of policies, certifications, independent audit reports, independent penetration tests (inc. remediation follow-up) etc. as appropriate.

13.2. Suppliers are subject to confidentiality and right-to-audit clauses within their contracts.

13.3. Suppliers are required to comply with Reed & Mackay's Supplier Operating principles and suppliers of products/services which interact with R&M information systems or process personal data are contractually required to agree to our Supplier Information Security Requirements.

13.4. Suppliers are reviewed on a periodic basis. The nature, scope and frequency of this review depends on several factors including the product/service being provided and the supplier's criticality.

13.5. Critical supplier resilience and recovery capabilities are formally reviewed on an annual basis as part of our Business Impact Analysis (BIA) of our BC recovery capabilities.

14. BUSINESS CONTINUITY AND DISASTER RECOVERY

14.1. In line with our head office's ISO 22301 certification, Business Continuity Plans, including Reed & Mackay's Crisis Management Plan, are formally reviewed on an annual basis, or more frequently if necessary (e.g., if there is a significant change).

14.2. A rolling Business Continuity exercise and test programme is in place, consisting of desk-based scenario exercises and physical recovery site tests.

14.3. An annual Business Impact Analysis is carried out to define the amount of disruption the business can tolerate to its key activities; the minimum level of these activities required for operation; and the resources and dependencies required to resume activities

14.4. The Reed & Mackay Travel Management Platform is hosted in Microsoft Azure, which offers high degrees of redundancy and resilience.

14.5. A third-party online backup service to ensure that critical information contained within Virtual Machines and storage accounts is stored securely and independently from the Azure environment and is available for restoration in the event of accidental loss or corruption.

14.6. Our proprietary database, including all accounting, client, and reporting data, is subject to incremental backups throughout, and a full daily backup. The RPO is 1 hour, and the RTO is 3 hours. Servers are backed up daily on an "incremental forever" basis. The RPO is 1 day, the RTO is 4 hours. Our overall RTO is 4 hours.

14.7. Backups are encrypted and tested periodically.

15. INFORMATION SECURITY RISK

15.1. Risk based thinking and awareness is incorporated into Reed & Mackay's management system and processes that underpin it.

15.2. The Information Security Risk Management Program is part of the Corporate Risk Management Framework and covers the identification and assessment of Information Security risks arising both from various periodic activities and from planned and unplanned change. Identified risks are prioritised, treated / accepted, and approved in a timely manner.

15.3. Activities within the Reed & Mackay Information Security Management program are prioritised based on identified risks and their impact on the services provided to clients.