AirGateway Data Processing Policy

At AirGateway GmbH, we understand and are committed to fulfilling our responsibilities as a data processor under the General Data Protection Regulation (GDPR) and other applicable data protection laws. This Data Processing Addendum (DPA) Policy outlines our commitment to robust data protection practices when we process personal data on behalf of our clients (who act as data controllers).

1. Our Role as a Data Processor

When AirGateway provides its services, such as through our Website (https://airgateway.com/) and our Desktop Agent Tool (https://web.bookingpad.com), we may process personal data on behalf of our clients. In such instances, our clients are the "Controllers" of the personal data, and AirGateway GmbH acts as the "Processor." This DPA Policy details the measures and commitments we undertake to process personal data in accordance with our clients' instructions and applicable data protection laws.

2. Commitment to GDPR Article 28 Compliance

AirGateway is dedicated to complying with the requirements of Article 28 of the GDPR, which governs the relationship between controllers and processors. Our standard contractual terms, or specific Data Processing Addenda executed with our clients, reflect these obligations.

3. Scope of Data Processing

The personal data processed by AirGateway typically includes information necessary to provide our travel technology services, which may involve:

- Processing of travel bookings and reservations.
- Managing user accounts and profiles within our platforms.
- Facilitating communication related to travel services.
- Analyzing usage data to improve our services and platform functionality.

The specific types of personal data processed, and the categories of data subjects, will be detailed in the individual DPA agreed upon with each client, based on the services provided.

4. Our Data Processing Principles and Measures

As a data processor, AirGateway commits to the following:

4.1 Processing on Documented Instructions: We will only process personal data strictly in accordance with the documented instructions from our clients, unless required by Union or Member State law. In such cases, we will inform the client of the legal requirement before processing, unless prohibited by law.

4.2 Confidentiality: All personnel authorized to process personal data are bound by strict confidentiality obligations, whether by employment contract or statutory duty.

4.3 Security of Processing: We implement appropriate technical and organizational measures to ensure a level of security commensurate with the risks associated with the processing of personal data. These measures are designed to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. Specific measures include:

* Monitoring for privacy breaches.
* Minimization of data storage periods.
* Restricted access to personal data based on the "need-to-know" principle.
* Regular testing, assessing, and evaluating the effectiveness of our security measures.
* Where appropriate, pseudonymisation and encryption of personal data.

4.4 Use of Sub-processors: We may engage sub-processors to assist us in providing our services. Any engagement of a sub-processor will be carried out in accordance with Article 28(2) and (4) of the GDPR. This means:

* We will obtain prior specific or general written authorization from the client.
* We will inform clients of any intended changes concerning the addition or replacement of sub-processors, providing an opportunity for objection.
* We will impose the same data protection obligations on our sub-processors as those set out in our DPA with our clients, ensuring they provide sufficient guarantees to implement appropriate technical and organizational measures.

4.5 Data Subject Rights Assistance: AirGateway will assist clients, by appropriate technical and organizational measures, in fulfilling their obligations to respond to requests from data subjects exercising their rights under Chapter III of the GDPR (e.g., right of access, rectification, erasure, restriction of processing, data portability, objection).

4.6 Assistance with Controller Obligations: We will assist our clients in ensuring compliance with their obligations concerning the security of processing (Article 32 GDPR), notification of a personal data breach to the supervisory authority (Article 33 GDPR), communication of a personal data breach to the data subject (Article 34 GDPR), data protection impact assessment (Article 35 GDPR), and prior consultation (Article 36 GDPR).

4.7 Data Breach Notification: In the event of a personal data breach, AirGateway will notify the affected client(s) without undue delay after becoming aware of it. The notification will

include all information required by Article 33(3) of the GDPR, to the extent available to us. We will cooperate with our clients in investigating and mitigating any breach.

4.8 Deletion or Return of Data: Upon termination of the services involving personal data processing, AirGateway will, at the client's choice, delete or return all personal data to the client and delete existing copies, unless applicable law requires continued storage of the personal data.

4.9 Audits and Information: AirGateway will make available to clients all information necessary to demonstrate compliance with our obligations as a processor and will allow for and contribute to audits, including inspections, conducted by the client or an auditor mandated by the client, subject to reasonable notice and confidentiality undertakings.

5. International Data Transfers

AirGateway's primary data processing servers are located in the Republic of Ireland and Germany. However, due to the global nature of travel technology, personal data may be transferred to, and processed in, countries outside the European Economic Area (EEA) where our clients, sub-processors, or third-party service providers operate.

For any such transfers to countries not deemed to provide an adequate level of data protection by the European Commission, AirGateway ensures that appropriate safeguards are in place. These safeguards primarily include the implementation of the European Commission’s Standard Contractual Clauses (SCCs), or reliance on other lawful transfer mechanisms as permitted by the GDPR. We ensure that our sub-processors and partners similarly adhere to these safeguards.

6. Contact Information

For any questions or concerns regarding this Data Processing Addendum Policy, or to request a specific Data Processing Addendum for our services, please contact our Data Protection Officer, heyData GmbH, located at Schützenstraße 5, 10117 Berlin, via their website at https://www.heydata.eu or by email at datenschutz@heydata.eu.

Last Updated: 22 July 2026