PRIVACY STATEMENT

Schiphol Travel b.v.

Introduction

Schiphol Travel is a corporate travel organization offering specialized travel-related services to large and medium-sized multinational companies. This statement outlines how Schiphol Travel has integrated the rights and responsibilities mandated by relevant regulations into its policies and operational procedures.

Schiphol Travel processes personal data of travelers to deliver their service to our clients and their passengers. In compliance with regulatory requirements, we detail the types of personal data we handle, the purposes for which it is processed, and the technical and organizational measures we have in place to ensure compliance and safeguard the rights of travelers.

Definitions

In this document, we employ the following terminology:

- **Client** refers to either a legal entity or an individual conducting business activities, instructing Schiphol Travel to provide travel-related services.
- **Traveler** refers to the individual receiving one or more services as per the agreement established with the client. In the context of this document, the traveler is equivalent to the data subject, as defined by the GDPR.

Terms and conditions

Articles 10.1 and 10.2 of the ANVR Business Conditions, which apply as the general terms and conditions to all (framework) agreements with Schiphol Travel, pertain to EU Regulation 2016/679, commonly known as the General Data Protection Regulation (GDPR). These articles delineate the lawfulness of personal data processing and the responsibilities associated with such processing.

Schiphol Travel acts as an autonomous data controller under the purview of the GDPR. This designation was conferred by the Data Protection Group of the European Commission in 2010, as indicated in Advisory Opinion 1/2010, Example 7. Consequently, no data processing agreement is applicable.

What personal data do we process, and to what means?

To deliver optimal service, we process a broad array of personal data. These include data provided by the client, as well as additional information supplied by travelers. Typically, this includes details such as:

- Gender as per the travel document
- Full name
- Residential address
- Private phone number
- Date, city, and country of birth
- Nationality
- Passport or ID details
- Driver's license particulars
- Frequent flyer information
- Family details
- Employment details (position, phone, email, department, manager, etc.)

- Travel preferences
- Travel policy adherence
- Travel history
- Payment details
- Login credentials for online tools

We exclusively handle data that is relevant to each individual traveller. The traveller must grant explicit consent before any personal data can be processed for purposes beyond its initial provision. Implicit consent may also be inferred if the traveller or client issues an order from which it can reasonably be assumed that data processing is necessary to fulfil that request.

In the event of an emergency posing life-threatening risks to the traveller, Schiphol Travel will utilise personal data to ensure the traveller's safety. Subsequently, this information will be reported to the client.

Data security measures

Personal data is of paramount importance to both travelers and ourselves. As such, we employ rigorous measures to prevent data loss or unauthorized access by third parties.

Data no longer required is deleted after a 14-day retention period. The client must specify when specific data should cease processing. Data in backups is automatically removed following the backup retention period, with specific data removal not feasible.

Access to personal traveler information is restricted on a need-to-know basis within Schiphol Travel, with only authorized personnel granted access. Employees at Schiphol Travel are provided unique usernames and passwords for their tasks. We have also implemented measures to enhance the security of login information, both intentional and unintentional, including two-factor authentication and automated monitoring and logging of specific communication methods.

Considering available technology, implementation costs, the nature, size, context, processing objectives, and the likelihood and severity of risks to individuals' rights and freedoms, we employ suitable technical and organizational measures to maintain an adaptive level of security. These measures encompass:

- Pseudonymization and encryption of personal data
- Ensuring confidentiality, integrity, availability, and resilience of processing systems and services
- Rapid recovery of personal data access in case of physical or technical incidents
- A systematic approach to testing, assessing, and evaluating the effectiveness of security measures at regular intervals

New Schiphol Travel employees are hired contingent upon receiving a Declaration of Conduct for Information, Money, and Business Transactions from the Ministry of Justice and Security. These employees are also bound by contractual obligations to uphold customer and personal data confidentiality.

Should the client have a legal obligation to report data processing to the Dutch Data Protection Authority, Schiphol Travel is committed to offering full cooperation in fulfilling this obligation.

Schiphol Travel provides all necessary information to demonstrate compliance with legal obligations to the client. Audits, conducted either by the client or an appointed agency, are facilitated with

cooperation, provided the instructions align with applicable legislation. Audits requested by the client will be at the client's expense, unless Schiphol Travel deems an audit necessary due to a security incident or other reasons, or if mandated by the Authority for Personal Data.

Data stored on Schiphol Travel's systems are further secured by firewalls and physical access control. Encryption is employed wherever feasible. External administrators of our automation systems adhere to GDPR legislation. New systems are developed with privacy-by-design and privacy-by-default principles in mind.

Third parties entrusted with storing or processing data are required to comply with GDPR legislation. Personal data is not shared with parties unable to demonstrate sufficient compliance with this legal framework.

Data subject rights

Under the GDPR, data subjects (in this context, travelers) possess specific rights regarding their data. These rights encompass access, rectification, erasure, restriction of processing, and data portability.

Should a traveler wish to exercise these rights, they should contact the Data Protection Officer of Schiphol Travel at gdpr@schipholtravel.com. Schiphol Travel commits to responding to such requests within three weeks, or if that is not feasible, to communicate the anticipated delay within that timeframe. If a request is deemed unfounded or excessive by the Data Protection Officer, it may result in the request's rejection or the imposition of costs by Schiphol Travel. Schiphol Travel may extend response times by two months if necessary.

In conclusion

Should you have any queries regarding Schiphol Travel's implementation of the GDPR, as outlined in this document, please feel free to contact the Data Protection Officer (DPO) via email at gdpr@schipholtravel.com.