CUSTOMER DATA SECURITY POLICY

230 Route des Dolines, 06560 VALBONNE
Tel : +33(0)9 72 10 05 90 - E-mail : solutions@my-travelplanet.com
www.my-travelplanet.com
TRAVEL PLANET France SAS au capital de 3 000 000 €
SIRET 384 221 925 00116 - APE 7911Z - IM62100003

1. Data Security Governance
2. 1.1 A Committed Approach to Customer Data Security
3. Travel Planet is committed to taking all necessary measures to secure customer data.
4. In pursuit of excellence in cybersecurity, Travel Planet works with a specialized service provider, who carried out the following tasks in 2017:

- Security audit of the information system (staff working environment, datacenter infrastructure, application architecture)
- Compliance implementation
- Training of development leads in secure coding practices

1.1.1 GDPR Compliance

Compliance with the General Data Protection Regulation (GDPR) was formalized upon its entry into force.

1.2 Risk-Based Security Management

To ensure an effective and informed security approach, Travel Planet regularly conducts security audits of its information system.

In addition, security investment decisions are guided by a risk analysis based on the specific characteristics of Travel Planet's business. This risk analysis is reviewed every two years.

Overview of risk-based management:

- Mapping of digital assets
- ・IT systems in which data is stored or through which it transits
- Assessment of potential threats
- ・External and internet-based threats
- ・Evaluation of available resources
- Risk analysis
- ・Steering of security investments to address the most significant risks
- ・Systematic priority given to the security of customer data

230 Route des Dolines, 06560 VALBONNE
Tel : +33(0)9 72 10 05 90 - E-mail : solutions@my-travelplanet.com
www.my-travelplanet.com
TRAVEL PLANET France SAS au capital de 3 000 000 €
SIRET 384 221 925 00116 - APE 7911Z - IM62100003

1.3 Guidelines for Travel Planet Staff:

1.3.1 Data Access Restrictions

Each Travel Planet employee has one or more roles within the company. Depending on their role, an employee has access only to the information necessary to carry out their duties. Additionally, staff members are made aware of the importance of not responding to any internal or external requests for disclosure of customer information.

1.3.2 Securing Accounts and Access to the Information System

Access to Travel Planet's information system is assigned to individuals by name, ensuring access traceability. Employee accounts are deactivated when they leave the company or change roles.

No customer data is stored on employee workstations, which are used solely as access points to the web applications of the information system.

Security of privileged accounts (administrators) is reinforced with two-factor authentication.

1.3.3 Staff Training

The Travel Planet Academy is an internal training program that provides job-specific training to new employees. As part of this program, training on best practices in data protection and awareness of cyber hygiene is included.

We also conduct regular internal communication campaigns on data protection and cyber hygiene topics.

1. Storage and Use of Personal Data
2. 2.1 Storage of Customer Personal Data
3. Travel Planet never uses customer data, directly or indirectly, for any purpose other than fulfilling its role as a Travel Management Company (TMC). We never buy or sell customer data.

2.1.1 Stored Data

Travel Planet only stores the data necessary to execute the contract with the client. Regarding personal data, this mainly includes identity information essential for organizing travel. We do not store any payment information.

2.1.2 Printouts

Travel itineraries are processed entirely in digital format. We do not print

Only the processing of exceptional requests may occasionally require the creation of a paper file. In such cases, files are stored in locked cabinets at one of Travel Planet's secured sites, with access restricted by badge.

Furthermore, paper documents are destroyed before being disposed of as recyclable waste.

2.1.3 Cybersecurity Principles Related to Digital Storage of Personal Data

To ensure the security of personal data within the Travel Planet information system, we have implemented the architectural principles described in this section.

2.1.3.1 Personal Data Vault

All personal data of our clients is stored in a digital personal data vault.

This is a secure database that contains personal data. Here, we define personal data as any information that can easily identify a client, such as identity details (first name, last name, etc.) or contact information (phone number, postal address, etc.). Access to this vault is strictly limited, and data is stored and encrypted at the application level (an SQL query to the database will return encrypted information).

By default, our applications store and process anonymized data linked to a technical identifier. Only processes that require access to personal data can occasionally retrieve it using the correlation technical ID to query the vault.

2.1.3.2 Security of Our Web Application Development

All transactions with the web client are conducted within a time-limited application session. The session is managed using a standard self-generated cookie. As a result, all client-server transactions propagate the session identifier.

To protect against hacking attempts on our web client, we systematically perform access rights checks on all our server-side APIs using a secure token.

Any abnormal situation (timeout, multiple simultaneous connections, etc.) during a session results in the session being terminated, requiring the user to reconnect to restore normal conditions. In addition, we reserve the right to temporarily deactivate a user account that exhibits abnormal behavior suggesting it may have been compromised.

2.2 Processing of Personal Data

We do not carry out any processing of customer data beyond what is strictly necessary to perform our service. No data enrichment or other uses of personal data are carried out.

3.1.2 Advanced Filtering System

We use a filtering technology that applies to each machine individually. In other words, by default, even two machines (virtual or physical) within the same network zone cannot communicate with each other.

We define specialized filtering rules for each machine based on its role. Only the network traffic required for the proper functioning of the information system is allowed. The implementation of this technology enforces strict discipline in managing our network traffic.

3.2 Operational Maintenance and Security Reporting

3.2.1 Obsolescence and Patch Management

The development and IT operations teams work together to maintain the operational and security integrity of the information system. This process relies in particular on obsolescence management reporting (including patch management) for system components (infrastructure, OS, middleware, and application libraries).

3.2.2 Access to Administration Consoles

The production environment can only be accessed through administration consoles. To maximize their security, these consoles are ephemeral: they are created when an operator needs to perform a maintenance task and are destroyed once the task is complete. As a result, under normal conditions, there is no persistent access to the "administration interfaces" of production machines.

3.3 Intrusion Detection

We have implemented a logging policy to monitor activity on our information system. This allows us to collect both performance data (response times, etc.) and security data (access logs, etc.). These logs are processed using a business intelligence tool.

Some of these processes are designed to detect abnormal behavior that may indicate attempted intrusions or data exfiltration.

When abnormal behavior is detected...