TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

INTRODUCTION

Outlined below are technical, organizational and physical measures implemented by TravelPerk to ensure the security of personal data processed. It covers TravelPerk's ability to ensure confidentiality, integrity, availability and resilience in the four areas of the business personal data is processed:

- Our platform
- Endpoint
- Network
- Software development

Alongside assessing the nature, scope, context and purpose for processing personal data within TravelPerk, the following is taken into account when implementing and maintaining security of processing: (as per Article 32 of the General Data Protection Regulation):

- Level of protection required with data transmission
- The ability to regularly test, assess and evaluate the security measures put in place
- Protection from accidental or unlawful destruction, loss, alteration, unauthorized disclosure and storage of personal data
- Ensure personnel accessing personal data do so in compliance with data protection laws

1. MEASURES TO PROTECT PERSONAL DATA DURING TRANSMISSION

Technical measures	
Encryption	Data is encrypted in transit and at rest with both the platform and at the endpoint within TravelPerk. This includes our website, workspace, email encryption, backups and use of TravelPerk's company-provided VPN for remote access.
Pseudonymization	This is practiced where deemed necessary for instances such as minimizing data processing and reducing duplication of personal data.
Web Application Firewall	Blocks attacks on traffic on our web application and APIs.
Network and Application Layer Firewalls	Blocks attacks on traffic on TravelPerk's network.

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

Organizational Measures	
IT Acceptable Use Policy	This policy includes restricting the use of public Wi-fi and media storage as well as encouraging the use of VPN. Also included is using the corporate machine for work related purposes only, along with the prohibition of installing third party tools with expressed approval.
Data Protection Policy	This policy is designed to provide clear rules and guidance to TravelPerk employees, contractors and external agents on how to handle and protect personal data processed within and associated with TravelPerk in compliance with the applicable regulation.
Encrypted file sharing platform	By providing a platform for documents to be shared securely with other parties, including those outside of the network, it reduces transmission of personal data.

Physical Measures	
Controlled mail space	Where personal data is transported in paper form, this is handled by a selected number of personnel in a defined space.
Secure media storage bins	TravelPerk facilitates secure disposal and destruction of removable media containing data.
Confidential waste bins	Personal data in paper format is disposed of within TravelPerk's confidential bins to be securely transported offsite and destroyed.

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

2. MEASURES TO REGULARLY TEST, ASSESS AND EVALUATE THE SECURITY MEASURES PUT IN PLACE

The security framework is aligned to the ISO27001 framework. Policies, procedures and processes are therefore reviewed annually or where a significant change takes place
External audits such as ISMS consultancy and penetration tests
Bug bounty programme allows us to continually test our security measures on the platform
Change management procedure for configuration changes helps us to visibly see and evaluate effectiveness of recent and potential changes
Security and Privacy teams are responsible for overseeing and managing data security processes. TravelPerk also has an Information Security Officer and a Data Protection Officer. Regular meetings, including cross meetings are conducted where topics on agendas are addressed
Evaluation stage in key processes such as incident management and data breaches
Static and dynamic application security testing tools integrated in our automated CI/CD pipeline
Security review of codes pre-release into production from CI/CD pipeline where required
Architecture reviews, with security considerations when introducing new systems or technologies into our environment
Threat modeling sessions conducted with our engineering squad

White-box 3rd party security assessment conducted every 6 months
Security guild and security champions program running
Backup procedures in place are tested twice a year
There is a Business Continuity and Disaster Recovery plan with the most common scenarios with solutions mapped out
Risk management

3. MEASURES TO PROTECT PERSONAL DATA FROM ACCIDENTAL OR UNLAWFUL DESTRUCTION, LOSS, ALTERATION, UNAUTHORIZED DISCLOSURE AND STORAGE

Additional technical, organizational and physical measures to the aforementioned include:

Technical measures
Separation of testing and production environments
Client systems logically separated within AWS
Enhanced mailbox security
Endpoint vulnerability management

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

Host-based Intrusion detection and prevention security tooling
SSO or Multi-factor Authentication on our application and internal systems used
Automatic device lock with reasonable idle timeout
Encryption within our AWS platform
Key Management Service with annual rotation
Audit logs with limited personnel access - Audit of access to applications, modification and deletion of data
Client data sits in AWS which has: ISO 27001, ISO 27017 and ISO 27018, SOC 1, SOC 2 and SOC 3, PCI DSS Level 1, and BSI's C5 certification
Regular network vulnerability scanning
VLAN Segmentation
Software Composition Analysis used to protect ourselves from supply-chain attacks
Data leakage controls in customer facing systems to restrict ability to send emails to wrong customers in error

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

Organizational measures
Authorisation procedures - access control management and procedures
Information Security Policy
Data Protection Policy
Third party management process - this includes security assessments with cyber score risk ratings provided; and due diligence questionnaires
Confidentiality agreements and Data Processing Agreements for all who access personal data processed within TravelPerk
Annual review of policies and procedures
Password management
Mobile Device/IT Acceptable Use Policy
Minimal Admins with access granted on a strictly need-to-know basis
Segregation of duties where possible
Policies and procedures govern data storage, downloading personal data onto mobile devices and minimizes duplication of data to allow for at a minimisation

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

Training and awareness programme which includes onboarding security and data protection training with testing and annual refresher courses
Minimal use of data storage media
Data retention policy and schedule
Asset management
OWASP led security training for developers

Physical measures
Access control in building
Visitors' procedure
CCTV in offices
Visitor's protocol
Employee/visitors' lanyards

4. ENSURE PERSONNEL ACCESSING PERSONAL DATA DO SO IN COMPLIANCE WITH DATA PROTECTION LAWS

Employee and contractors onboarding includes security and data protection training and awareness
Regular phishing simulation exercises
Centrally accessible written policies and procedures
All internal teams receive ongoing support from Security, Legal and Privacy teams
Annual refresher training

To ensure we adhere to the principles of the General Data Protection Regulation as per Article 6, we have the following measures in place:

Lawfulness, Fairness and Transparency
A Privacy policy which outlines what, how and why personal data is processed within TravelPerk as well as for how long and when it is transmitted externally. We make sure this policy is communicated at the first point of collecting or receiving the data
Publicly available documentation such as our Security Whitepaper, our Data Protection webpage and a GDPR Mailing List
Data Protection Agreements are in place with all third parties who access personal data within TravelPerk
Explicit and granular consent sought with a simple way to withdraw the consent at any time

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

Purpose Limitation
Data Flow map which allows TravelPerk to monitor when personal data is being collected and attributing it to a purpose already identified on the map. If it transpires as a new purpose then this is dealt with accordingly
Records of Processing register records TravelPerk's processing activities which is reviewed periodically or where a significant change takes place
Data Minimization
As well as the use of pseudonymization as mentioned above, the common use of API and other relevant connectors reduces data duplication
Project management for upcoming projects allows TravelPerk to assess what processing of data is required, enabling adequate information on individuals to be collected only
Periodic reviews on processes and data retention periods
Data Accuracy
Customers can themselves rectify their data on their travel accounts
Access control to systems is implemented where personal data is stored, with access and permissions to modify data granted on a need-to-know basis
Storage Limitation
Data retention and deletion policy and schedule in place with delegated owners of the process
Periodic review undertaken on retention schedules

TRAVELPERK | SECURITY MEASURES ADOPTED BY TRAVELPERK

Integrity and Confidentiality
Aforementioned within this Annex
Accountability
A DPO, ISO and dedicated teams overseeing privacy and security respectively
Top down approach is taken on data protection allowing for privacy by design and privacy culture to be successfully adapted