TravelPerk

Privacy

Whitepaper

TravelPerk

Table of Contents

Introduction

Customers' trust is TravelPerk's most valuable asset. Protecting customers' personal data is pivotal to upholding that trust.

The purpose of this document is to provide customers and potential customers with transparency as to the practical measures which TravelPerk takes to comply with global regulatory requirements.

Our Privacy Team

TravelPerk has a dedicated Privacy Team. The team comprises legal and operational specialists, focused on maintaining a word-class privacy compliance program for our customers, employees and everyone else who entrusts their data to our company. Our Privacy Team works closely with TravelPerk's Information Security team, ensuring our privacy and security operations are aligned towards keeping your personal data safe at all times.

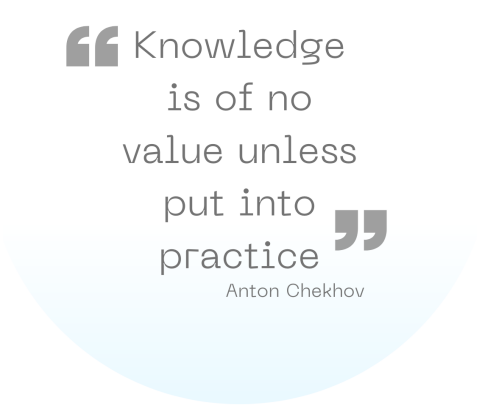
Our Data Protection Officer (DPO) is responsible for translating regulatory insights into actionable enhancements to our privacy culture, and acts as the contact point for supervisory authorities and customers for any privacy compliance questions.

Privacy by Design at TravelPerk

A great start

We pursue the principles of privacy by design and by default by understanding and focusing on the life cycle of customers' data. We apply technical, organisational and physical security measures from the moment personal data is entrusted to us up until the point it is securely destroyed.. We embed a privacy focused culture within TravelPerk through:

- Training and awareness;
- Support to operational teams; and
- Working collaboratively to bring about our trusted product and services.



Training starts from the moment our employees join TravelPerk. e assess understanding of learnings through standardised testing. Our employees understanding privacy is important to us, as it allows for a proactive approach to be taken with data protection. We also offer annual refresher training specialised to areas within the business.

Top-Down Leadership

Accountability for our privacy culture starts with 'tone at the top' - messages, endorsements and enthusiasm expressed by our leadership team as to the importance of maintaining customer trust through positive privacy behaviour.

Privacy Team

As direction comes down from leadership, our Privacy Team drives privacy by design and default by implementing structural and behavioural measures to drive positive privacy practice. These measures are led by our designated Data Protection Officer, whose core role is to monitor and assess our compliance with privacy laws.

People

Our employees work collectively on providing a seven star product and service to our customers. Provision of a seven star service requires a deep understanding of customer need, and an 'over and above' attitude towards anticipating and meeting it.

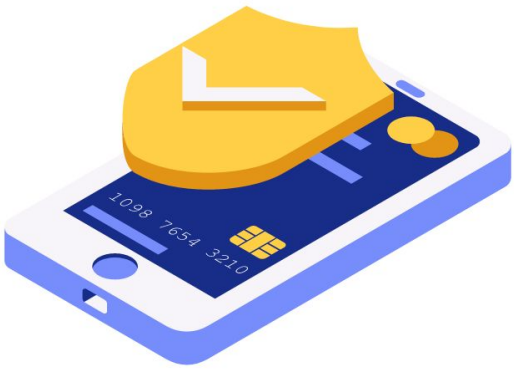
We adopt this same approach in relation to privacy and trust development, recognising that adequate technical, organisational and physical measures are not enough to drive a high level of customer trust. .

Transparency, for example, is embedded into our processing activities. From the moment we collect personal data, we provide you with the information needed to make an informed choice as to whether you want to entrust us with your data. Through data mapping, we know which

data we need for what purpose. We adopt data minimisation through the use of pseudonymisation for our customers' data. We provide further features for customers to add security to personal data provided to us within the TravelPerk platform, such as SSO sign-on integration and tiered access control management.

Security Measures

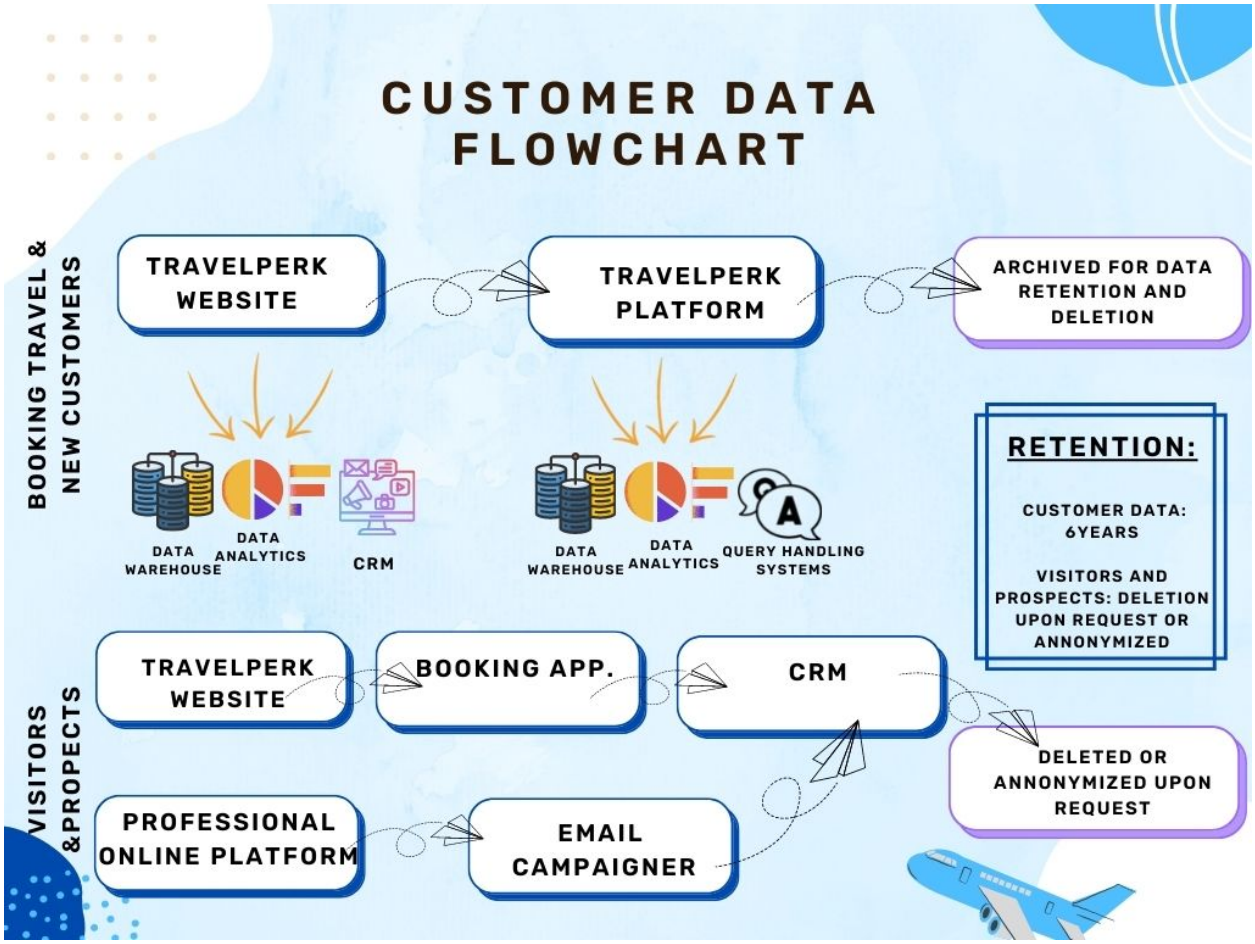
TravelPerk has implemented technical and organisational measures having assessed the level of necessity. In the process we risk-assess the rights and freedoms of individuals. To further demonstrate our compliance with the GDPR, specifically Article 32 of the regulation, we have put together a list of our implemented Technical, Organisational and Physical Security Measures. More information is included in our Security Whitepaper for more information.



Our Customer Personal Data Flow

Below is a basic illustration of how our customers' data flows during its life cycle with TravelPerk. As part of our privacy practices, we are constantly reviewing our data flow to ensure:

- We continue to process personal data in accordance with customer consents/ expectations;
- We update our Data Processing Agreement regularly to inform our customers (or our Privacy Policy for our website visitors and prospects) about any new forms of processing identified;
- We review, develop and (where appropriate) add more layers of security to personal data we are processing;
- We do not retain data longer than is necessary.



Data Subjects' Requests

We aim to provide data subjects with the ability to control how their data is used, at the time and in a manner which suits their needs.

Right to delete data: Data deletion requests can be fulfilled by us or customer admins within user accounts, providing flexibility and autonomy to our customers. Once a deletion request is made or carried out, we proceed to take the data out of live mode, delete by way of masking, and archive the information we are required to retain for legal reasons. After the applicable retention period lapses, we then delete the remaining data.

Right to rectify data: Users have the freedom to modify most of their data within their accounts on the platform. To protect the security of our customers, we retain the sole right to complete a small percentage of data operations.

Right to request access to data: Users requesting copies of their data, or who are asking specific questions around how their data is processed, are able to receive this information from us in .pdf; .csv and/or JSON format.

Right to object: Any user who is not satisfied with the way we process their data, may request that we cease processing activities. Users should be aware that contractual and legal limits apply to the extent we can comply with such requests. We aim to communicate these limits transparently wherever they constrain users' rights to object.

Right to lodge a complaint with a supervisory authority: If you think we are not doing enough to protect your data, or you have any complaint about how we process your personal data, we encourage you to contact our Privacy Team in the first instance. However, if our Privacy Team is unable to assist, you have the right to file a complaint with a supervisory authority in your country. More information can be found in our Privacy Policy.

Right to restrict the processing of your data: We can take data out of live mode and archive it, where asked to do so, provided that archiving does not infringe legal or contractual obligations.

TravelPerk primarily acts as the data processor. We have the obligation to notify our customer as the data controller so that they decide the desired course of action to respond to such requests. If we do not receive a response from the data controller in due time, we will proceed to carry out the request on behalf of the data controller. We have a robust procedure in place to facilitate requests within the calendar month of receipt and all employees are trained to identify and understand this procedure. As we continue to work on improving the service we provide to our customers, we are in the process of automating requests to restrict data processing.

Data Breaches

We have a formal procedure in place to deal with data breach. Additionally, we have backup external incident management assistance, where required, comprising legal, forensics and engineering expertise.

We will always notify our customers without undue delay to allow for you to assess next steps and whether to report to the supervisory authority within 72 hours of us making you aware. We offer continual assistance where needed so our customers as the data controller can make an informed decision on how to best act.

International Data Transfers (IDTs)

Sharing our approach to international data transfers with our customers is an essential part of an overall privacy program to identify privacy risks, document compliance with applicable laws and internal policies, and maintain customer trust.

This section is intended to provide our valued European customers and users with transparent information regarding TravelPerk's data transfer practices in light of the European Court of Justice's C-311/18 decision of 16 July 2020, frequently known as the "**Schrems II**" decision. It explains the measures we have adopted to ensure that an equivalent level of protection exists for personal data that is transferred out of the European Economic Area (**EEA**), Switzerland and the UK in connection with the use of TravelPerk services. We also provide a quick overview of the measures adopted by TravelPerk to protect our customers' data from inappropriate disclosure to law enforcement and intelligence agencies of third countries.

The CJEU "Schrems II" ruling

The Schrems II judgement is a reminder that the protection granted to personal data in the EEA must travel with the data wherever it goes. The CJEU made data exporters aware that the standard of protection afforded to personal data in third countries needs to be essentially equivalent to the standard guaranteed within the EEA.

Where we act as a processor and exporter of our customers' personal data, we are responsible for verifying, together with the importer and on a case-by-case basis, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards laid out in the transfer tools of Article 46 of the GDPR. In such cases, as mandated by the CJEU in Schrems II, we assess whether our suppliers have implemented supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law.

EDPB Recommendations and TravelPerk's approach to IDTs

Assessing third countries and identifying appropriate supplementary measures where needed is a complex task. To help with that, the European Data Protection Board (**EDPB**) adopted the Recommendations 01/2020 (version 2.0 adopted on 18 June 2021) on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (the **EDPB Recommendations**). These recommendations provide exporters with a series of steps to follow and some examples of supplementary measures they may put in place.

Before transferring any customers' personal data to a supplier located in a third country, TravelPerk follows the steps outlined by the EDPB, as described below.

(1) Know your transfers

We perform a mapping of all transfers of personal data to third countries to ensure that it is afforded an essentially equivalent standard of protection wherever it is processed. The locations from which the services of our sub-processors may be provided and a description of their processing activities are set out in the Data Processing Agreement we enter into with our customers, as well as in TravelPerk's sub-processors page.

(2) Verify the transfer tool(s) on which the transfer relies

In the absence of an adequacy decision, we put in place the appropriate transfer tools (as per Article 46 GDPR), namely the Standard Contractual Clauses approved by Commission Implementing Decision (EU) 2021/914 of 4 June 2021 (**SCCs**). We execute the relevant Modules of the SCCs with both our (sub)processors and any independent controllers (e.g. travel service providers) which have access to our customers' personal data.

(3) Assess the laws of the third country

TravelPerk, as an EU-based company with its headquarters located in Barcelona (Spain) and data centres in Ireland, is not subject to regulations that may entail inappropriate disclosure to law enforcement and intelligence agencies in breach of the GDPR. But some of our suppliers are located outside of the EEA, and therefore we need to assess whether there is anything in the law and practices in force of those third countries that may impinge on the effectiveness of the appropriate safeguards contained in the SCCs. Our attention is drawn to any legislation and practices that might require our suppliers to disclose personal data to public authorities or law enforcement. The starting point for our assessment is the thorough Data Protection Questionnaire we send to all our suppliers, as described below.

(4) Identify and adopt supplementary measures

If our assessment reveals that the third country legislation and practices are an obstacle to the effectiveness of the relevant SCCs, we verify whether our suppliers have adopted supplementary measures aimed at bringing the level of protection of the data transferred up to the EU standards.

We also adopt supplementary measures on our end, both in the form of contractual safeguards (e.g. execution of the relevant SCCs, as well as additional contractual commitments regarding requests for disclosure of personal data to law enforcement or public authorities) and technical and organisational safeguards, as detailed in our Security Whitepaper.

(5) Adopt necessary procedural steps

In addition, we assess whether the adoption of supplementary measures may require certain formal procedural steps.

(6) Re-evaluate

The principle of accountability requires continuous vigilance of the level of protection of personal data. Accordingly, we re-evaluate at appropriate intervals the level of protection afforded to the personal data we transfer to third countries.

Data transfers to the USA

The Schrems II ruling has focused European attention on the breadth of law enforcement powers that permit US government agencies to engage in proactive surveillance. To address the uncertainty generated about the impact of such US laws on our international data transfers, we have set out specific processes and internal policies to make sure that any transfer of personal data to a US supplier is carried out safely and in full compliance with EU data protection standards.

Our attention has been drawn to the following US laws:

1) Section 702 of the Foreign Intelligence Surveillance Act (**FISA Section 702**)

2) Executive Order 12333 (**EO 12333**)

3) US Clarifying Lawful Overseas Use of Data Act (**CLOUD Act**)

As regards FISA Section 702, we have set up processes to proactively assess whether and to what extent our suppliers may be compelled to respond to targeted requests for customer data. We direct them to carefully review the lawfulness of any request for disclosure they may receive, notably whether it remains within the powers granted to the requesting public authority, and to exhaust all available remedies to challenge the request if, after a careful assessment, it concludes that there are grounds under the applicable laws to do so.

EO 12333 authorises and governs surveillance activities by US intelligence agencies. The main concern is the US government's ability to collect personal data while it is in transit to the US by intercepting data travelling over transatlantic cables. TravelPerk addresses this risk by encrypting Personal Data and only transferring data that is subject to strong protection. Please see our Security Whitepaper for more information about these technical measures. Our priority is to only engage suppliers that do not and cannot be ordered to take any action to facilitate the type of bulk surveillance sought under EO 12333.

Lastly, the CLOUD Act foresees that US law enforcement authorities may request personal data from US-based technology companies when there is a suspicion of a crime by issuing warrants or court orders, regardless of the location of the data. To minimise the risk for customer personal data under our custody, TravelPerk's assessment of its US suppliers aims at ascertaining to what extent they may be compelled to respond to such a law enforcement requests for customer data, and, should a supplier be subject to the CLOUD Act, we direct them to carefully review any request they may receive to verify that it is lawful and appropriate, and, when necessary, to challenge the request in accordance with GDPR principles and their contractual commitments towards TravelPerk on government access requests.

Privacy assessment of our suppliers

Before engaging a new supplier, we direct them to respond to a questionnaire carefully and thoroughly drafted by our Privacy Team. The questionnaire addresses all relevant data protection concerns, ranging from the implementation of robust security measures to protect personal data, to the supplier's internal data protection policies, its handling of data subject requests, prevention from potential data breaches, mechanisms put in place for international data transfers and onward transfers, and any additional safeguards to guarantee the effectiveness of such measures, especially as regards potential requests for disclosure of personal data by public authorities and law enforcement in the vendor's country.

Our dedicated Privacy Team then reviews the responses to the questionnaire and assesses the trustfulness of the supplier. Where we have any concerns that the personal data may not be protected enough against disclosure to public authorities and law enforcement, we direct the supplier to implement additional safeguards. If we still believe the transfer of personal data to that supplier is not safe, we will seek to engage a more GDPR-compliant alternative.

TravelPerk's Privacy Role as a Data Processor

As a business travel service provider, TravelPerk processes customer data as a data processor. This means that TravelPerk handles personal data on the customer's behalf and under its instructions, and only for the purposes allowed by the customer as defined in the Data Processing Agreement.

The role of Travel Suppliers

Neither our customers nor TravelPerk determine the means and purposes for the processing of personal data by travel suppliers, which is why they are not data processors of customer data. Airlines, hotels, car rentals, and other suppliers of travel inventory define the purposes and means for processing your data on their own for booking a flight, hotel room, or vehicle.

Such autonomy in defining how and why the data will be processed position travel suppliers as **independent data controllers** of the customer data shared by TravelPerk, so they provide the travel service requested through our platform.

TravelPerk is not responsible for the acts or omissions of travel suppliers. Once the service is booked, all terms and conditions and other contractual terms of the travel supplier will apply to the customer and, where applicable, its affiliate companies. TravelPerk will not be liable for any breach, delay, default or deficiency during the provision of services by those travel suppliers.

Lastly, data sharing agreements between customers and travel suppliers are not required as the data will be shared by TravelPerk on the customer's behalf. TravelPerk has data sharing agreements in place with those suppliers to ensure they comply with their respective obligations under the applicable privacy laws in relation to customer personal data.

DPIA (TravelPerk's process for customers)

Article 35 of GDPR states the circumstances in which data controllers should carry out a Data Protection Impact Assessment (**DPIA**). These include types of processing using new technologies and any activity which, taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons.

As a data processor, TravelPerk will support its customers in complying with their data controller obligations, which also applies to the reasonable information required by the customers to perform their own DPIA prior to sharing the personal data with us.

Conclusion

The protection of personal data is of paramount importance for us to operate effectively as your trusted business travel partner. We've gone to great lengths to maintain a word-class privacy compliance program within TravelPerk and to secure your data through technical and organisational measures, both while the data are under our custody and where we need to share your data with suppliers.

We're sharing this Privacy Whitepaper to return the trust you've placed in us, providing a level of transparency that we hope provides you with assurance and confidence in our partnership. We hope this document has given a useful insight into how we approach privacy at TravelPerk and as we grow further, we intend to continue expanding our privacy compliance program with the same transparent approach.

Should you have any further questions on how we approach privacy or how we handle customers' personal data entrusted to us, please don't hesitate to contact our Privacy Team at personaldata@travelperk.com.