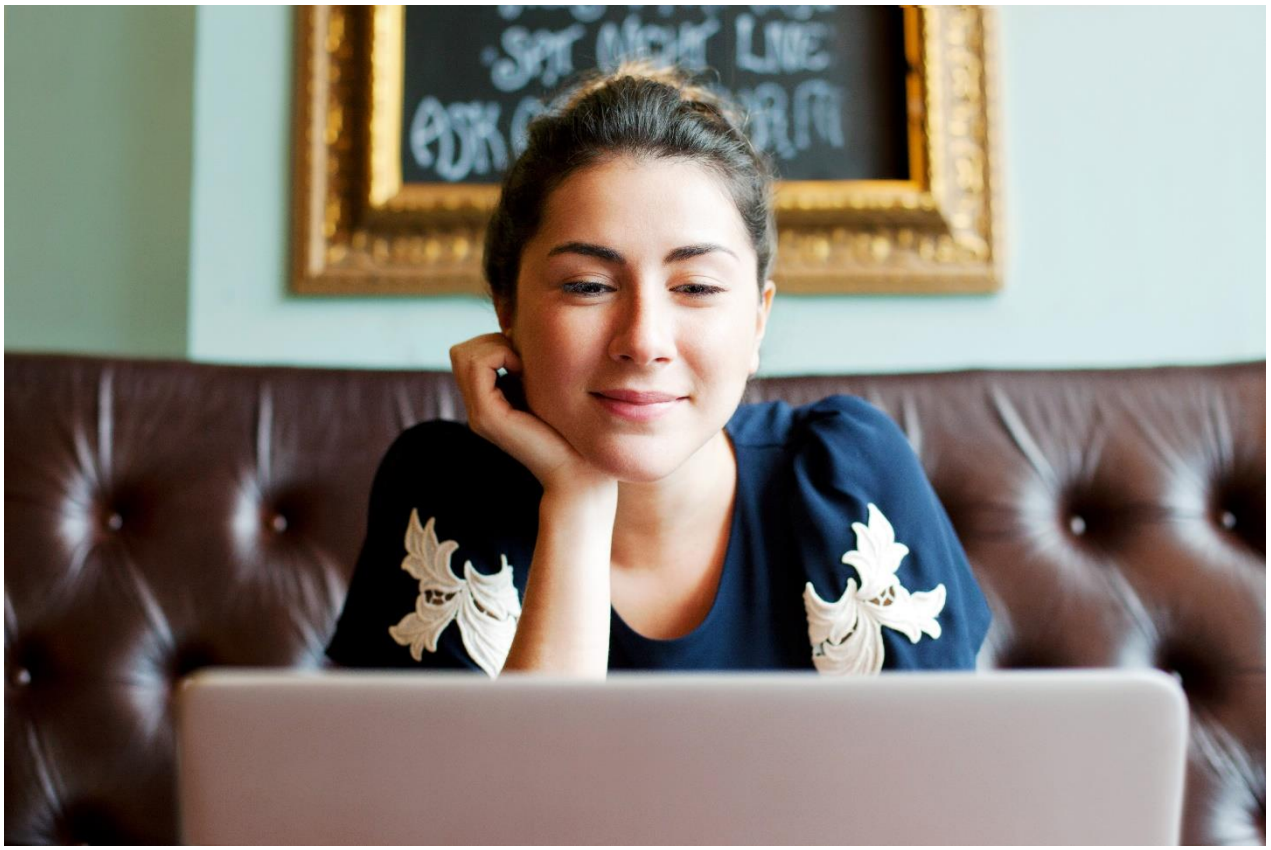
TRAVELPORT

TRAVELPORT COMPLIANCE AND ETHICS

Protecting Personal Data

Policy and Code Guidance



Version 10: August 2022

Protecting Personal Data

This Code Guidance outlines what is required of all Travelport employees and contractors who handle or may come into contact with personal data.

Why is the protection of personal data important?

Our company is obligated to ensure that personal data is collected, stored, used and disclosed in the appropriate way. This includes personal data from or about our customers, suppliers or employees. Any failure to meet this obligation could lead to possible legal action against the company and/or any individuals involved and/or substantial fines imposed by governmental authorities. In certain countries, failure to comply with data protection requirements may also be a criminal offence. Aside from the legal obligations imposed on us, our customers, suppliers, and fellow employees entrust us with their data. If that trust is breached, our reputation and the potential for future business could be severely damaged.

What is personal data?

Personal data is any information (in electronic or paper form) that can be used to identify a living individual, including for example, names, addresses (including in some countries, email addresses), credit cards, customer and supplier lists and contact details, employee candidate interview notes, salary information and bank details. Different countries and cultures around the world may use different definitions, or slightly different terminology (for example, in the US people may refer to personally identifiable information or PII), but generally the concept of what is personal data remains the same for the purpose of this Code Guidance.

What are your obligations as an employee?

Travelport maintains data protection and privacy measures to minimize our exposure to loss of personal data and legal risk. As employees, by observing a few simple protocols, we can avoid or minimize such exposure. The following protocols draw on the key data protection and privacy principles ("Privacy Principles"):

Data collection: When gathering personal data, you must:

- Know, and be able to justify, why you need to collect, store and maintain the personal data. Under GDPR Article 6, Travelport is required to process data only on certain lawful bases, such as consent, performance of a contract, compliance with a legal obligation, or a legitimate interest.
- Know the time for which you can store the data collected, when it must be deleted and take steps to ensure its deletion is scheduled to comply with applicable laws.
- Where possible, inform the individual whose personal data you are collecting that you will retain the data and why.
- Gather no more personal data than is reasonably required for the purpose it was collected for.
- Only use the personal data for the specific purpose that it was collected.
- Check whether the personal data is "sensitive data" and if so, be sure to comply with the additional security or legal requirements that may exist. Personal data is generally "sensitive" where it refers to an individual's race, religion, ethnic origin, health, genetic or biometric data, sex life or sexual orientation, political beliefs, criminal convictions, or trade union membership; and in some jurisdictions, such as the European Union under GDPR Article 9, explicit consent must be obtained prior to processing such data. If you are uncertain whether certain personal data is sensitive, you should contact the Legal Department.

- Be aware that a Data Protection Impact Assessment is required if you are planning on engaging in a new or altered processing activity that could be considered to pose a “high risk” to the rights and freedoms of the individual whose personal data you are collecting. “High risk” activities include, but are not limited to, systemic surveillance; automated decision-making using personal data, including profiling, that produces legal or other similarly significant effects (e.g., employment discrimination) on the person; use of new, unproven data processing technologies; large-scale data processing; and processing of data concerning vulnerable data subjects (e.g., children, elderly, etc.). Should you be uncertain as to whether the processing activity you are considering may be categorized as “high risk,” contact the Legal Department.

Data storage: When storing personal data, you must:

- Ensure that the personal data is protected by appropriate information security measures in line with Travelport information security policies, and that access is restricted on an authorized need-to-know basis.
- Make no unnecessary or unauthorized copies of the personal data.
- Ensure that you hold the personal data no longer than is necessary, and always in line with our Records Management Policy.
- Depending on the type of personal data being stored, use reasonable measures to ensure that it continues to be accurate and, where necessary, kept up to date.
- Be aware that individuals may have the right to erase, port or otherwise restrict the processing of their personal data under certain circumstances, and such rights must be accounted for in the storage of the data.

Data usage: When using or processing personal data you must:

- Only use the personal data for the purposes it was originally collected for.
- Be aware that any unauthorized use of personal data – for example, using the personal data of a customer for non-work-related purposes – is a potentially serious matter that could result in criminal prosecution and/or disciplinary action.
- Not use the personal data for marketing or other reasons unless you have written authorization to do so.

Data disclosure: When considering whether to disclose personal data you must be aware that:

- Individuals may have a right of access to their personal data that is held by Travelport.
- Individuals may have a right to say “no” to their personal data being stored and disclosed.
- You may generally only disclose personal data to third parties if the individual (whose personal data it is) was informed that you would do so when their personal data was collected and gave consent or had the opportunity to “opt out”. There are some exceptions; please contact the Legal Department for further information.
- Any third party that you share personal data with must adhere to the same data protection principles as Travelport and should enter into a contract with Travelport for that purpose before any data is disclosed. Please contact the Legal Department for further information.

In the **European Union (EU)** there are specific laws that restrict the transfer of personal data to a country outside the European Economic Area unless that country has been recognized by the European Commission as ensuring an adequate level of protection in relation to the processing of personal data. There are some exceptions. As Travelport relies on the transfer of subscriber personal data from its European operations to its data center in the United States, a country that has not been recognized as ensuring an adequate level of protection, Travelport relies on these exceptions, including the use of standard contractual clauses **(Model Clauses)** between relevant group companies. Other jurisdictions that have similar restrictions on international data transfers include Argentina, Australia, Chile, Malaysia, New Zealand, Russia, and Quebec (Canada). **When working with any third-party company, where we may be required to transfer personal data (subscriber or otherwise) outside of the local jurisdiction, you should contact the Legal Department to verify if the recipient of that personal data is subject to adequate legal protections, under the Model Clauses or other arrangements.**

Where can you find out more?

- Various privacy policies that Travelport uses on its own websites (e.g. http://www.travelport.com/privacy).
- Further information on the practical measures that must be taken to protect such data from unauthorized access can be found in the Travelport Code of Business Conduct and Ethics and Travelport information security policies.
- Travelport Legal Department.
- Travelport Data Protection Officer – Kathryn Heath, at kathryn.heath@travelport.com or Travelport, Axis One, Axis Park, 10 Hurricane Way, Langley, Berkshire, SL3 8AG, United Kingdom. Attention: Data Protection Officer.
- Specific privacy questions can be emailed to privacy@travelport.com.

Who is responsible for this Code Guidance?

The Travelport Data Protection Officer is responsible for this Code Guidance. Any changes to it must be approved by the Travelport Data Protection Officer. If you have any questions about this Code Guidance, please contact the Travelport Data Protection Officer or send an email to privacy@travelport.com.

Are there any situations where the Privacy Principles do not apply?

The Privacy Principles do not apply in specific situations where required or permitted by legal or compliance obligations. The Travelport General Counsel shall make such determinations on a case by case basis in consultation with the Travelport Data Protection Officer and the Travelport Legal Department.