Personal Data Protection Policy

Definition of terms:

- **Personal data:** Any information relating to an identified or identifiable natural person.
- A natural person is identifiable when he/she can be identified, directly or indirectly, by name, surname, identification number, geolocation data, electronic communication identifying data, or physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics.
- **Special category data:** Data relating to a natural person's racial or ethnic origin, political opinions, religious, philosophical, or other beliefs; trade union membership; health; sex life; or status as an accused, convicted, acquitted, or victim in criminal proceedings. It also includes data about criminal convictions, criminal history, diversion, and recognition as a crime victim in accordance with the Law of Georgia "On Prevention of Violence Against Women and/or Domestic Violence, Protection and Assistance to Victims of Violence." Additionally, it encompasses imprisonment, the execution of sentences, biometric data, and genetic data processed for the unique identification of a natural person.
- **Data processing:** Any action performed on, about, or against data. This includes collection, obtaining, accessing, photographing, video and/or audio monitoring, organizing, grouping, interconnecting, storing, modifying, retrieving, blocking, deleting, or destroying data. It also covers disclosing data by transmission, dissemination, distribution, or making it available in other ways.
- **Data subject:** Any natural person in relation to or about whom the data is processed.
- **Incident:** A breach of data security that results in improper or accidental damage, loss, unauthorized disclosure, destruction, modification, access to, collection/obtaining, or other unauthorized ways of data processing.

Introduction

TAV Urban Georgia LLC strictly adheres to the Georgian Law on Personal Data Protection and local and international regulations in the field of personal data protection. Protecting personal data stored and maintained by the company and ensuring its proper processing is a crucial priority.

TAV Urban Georgia ensures the protection of fundamental human rights and freedoms in every way, including the protection of privacy, personal space, personal communication, and personal data. The company takes all necessary measures to protect the personal data of passengers, employees, and individuals in contractual relationships with the company, implementing all reasonable technical and organizational measures for this purpose.

Purposes of data processing

Data is processed to serve passengers, provides them with services that meet international standards for their departure and arrival, offer luggage storage services, hire employees, and enter into contracts.

Principles of data protection

The company processes data following these principles:

- Lawfully, fairly, and transparently, ensuring processing doesn't harm the dignity of the data subject.
- Data collection/retrieval is solely for clearly defined, legitimate purposes.
- Data is processed only to the extent necessary to achieve the purpose of processing.
- Relevant technical and organizational measures are in place to minimize the risk of damage, alteration, or loss of data during processing.
- Data is processed and stored only until the purpose of processing is achieved. Afterward, the data is destroyed or anonymized, except in cases specified by law.

Legal grounds for data processing

The company processes data based on:

- The consent of the data subject.
- The fulfillment of contractual obligations.
- Compliance with legal requirements.
- Reviewing and responding to inquiries from data subjects.

Categories of processed data

The company processes the following categories of data:

- Special category data
- Data of minors
- Data related to health status/conditions

The company processes data such as name, surname, personal number, email address, residential address, employee salary, employee health status report, and employee conviction report for legitimate purposes. It also processes other data necessary for achieving the legitimate purposes described in the company's personal data protection policy.

Data subjects and protection of their rights

The company's data subjects are:

- Airport passengers
- Company applicants and employees
- Persons in a contractual relationship with the company

Protecting the rights of data subjects is a key priority for the company and a core value for international and local legislation on personal data protection.

Data subjects have the following rights:

1. To obtain information about whether their personal data is being processed by the company.
2. To know what data about them is processed by the company and to request a copy of this data.
3. To request information about the storage period of their data.
4. To know the legal basis for processing their data.
5. To understand the purpose of data processing.
6. To revoke any consent given for data processing.
7. To find out if their data has been transferred to any third party.
8. In the case of data transfer to a third party, to know which data was transferred, when, and on what legal basis.
9. To request information about the source(s) of collection/obtaining his/her data

This information can be requested in writing. The company is obliged to provide the requested information free of charge within 10 days of the request. This period may be extended in the event of objective circumstances.

The data subject has the right to request the updating, modification, deletion or destruction of data about him/her if his/her data is incomplete, outdated, incorrect, there is no longer a reason for their storage, or they had been obtained through illegal means.

The right given in clauses 6 and 7 or any other right can be restricted only in the case provided for by the legislation, in cases provided by article 13, part 3 and article 21 of the Law of Georgia on Personal Data Protection

If an incident occurs and there is a high likelihood that it will cause significant damage and/or pose a significant threat to basic human rights and freedoms, the company will immediately notify the data subject, except in cases specified by Article 30, Part 3 of the Law of Georgia on Personal Data Protection.

The data subject has the right to apply to the court or to the Personal Data Protection Service. In order to exercise his/her rights and for other issues the data subject may also lodge a request with the company's Personal Data Protection Officer (e-mail: mirian.petriashvili@tav.aero)

The Company's Personal Data Protection Officer will review the application within 10 days. Depending on the complexity of the investigation of the circumstances contained in the application or other objective circumstances, this period may be extended for a reasonable period, and in such cases, the party will be notified as soon as possible, but no later than within 10 days.

Sources from which data is obtained

The company receives personal data from:

- Airlines operating at Tbilisi International Airport
- Applicants and/or employees

- Natural and legal persons with whom the company has contracts within the scope of its activities
- Public bodies

Data transmission and recipients

The company shares data only as permitted by law or with the data subject's consent for transferring data to a third party. Data subjects receive explanations about why their data is being transferred.

Data recipients are:

- Public bodies
- Airlines
- Audit companies
- Legal entities with which the company has agreements for receiving various services

For example, the company sends its employees' data, with their consent, to a commercial bank to open a salary account and issue a bank card.

When transferring data abroad, it is sent to countries included in the list of countries with adequate data protection guarantees.

Data storage

Data is stored until the purpose of processing is achieved. Afterward, the data is anonymized or deleted/destroyed.

Data may be stored after the purpose is achieved in cases specified by law. For example, the company is legally obliged to maintain financial and accounting documentation for 6 years. Information about aviation occurrences must be kept for 7 years. After these different storage periods expire, the data is destroyed.

The company has an agreement with the airport's owner, the state-owned United Airports of Georgia LLC, on airport operation (BOT agreement). This agreement requires the company to provide certain information related to the airport's operation to United Airports of Georgia LLC. Such information will be stored for the duration stipulated in the agreement or as requested by United Airports of Georgia LLC, based on the agreement.

Personal Data Protection Officer

As required by law, the company has a Personal Data Protection Officer. The officer coordinates and monitors the process of data processing within his/her competence; provides appropriate recommendations and instructions to improve the data procession process in the company;

participates and develops in accordance with the legislation of Georgia regulations that are necessary for the company for data procession. In the event of a legislative change, they make appropriate changes in the internal regulations so that they are fully consistent with it.

If there are any complaints and statements received in relation to the procession of personal data in the company, consider them, perform a complete investigation of the issue and if a violation is discovered, act in response to the same. Together with the relevant officials/authorities, it determines appropriate preventive measures and measures for elimination of defects.

Personal Data Protection Officer monitors the process of compliance with the requirements of the law; this document and other internal regulations related to data procession.

During data processing, in the event of an incident, the Personal Data Protection Officer notifies the Personal Data Protection Service on the same in accordance with the law, unless the incident is unlikely to cause any significant harm and/or pose a significant threat to fundamental human freedoms and rights.

Data Security and Employee Responsibilities

The secure storage of protected data is of utmost importance to the company, which is why appropriate technical and organizational measures are in place.

The possibility of losing, damaging, altering, or gaining unauthorized access to electronically available data is minimized, as the company's relevant department has taken all necessary technical measures. The company's internal regulations contain clear instructions and obligations for processing and storing electronic materials. Any violation of these rules will subject the relevant employee to disciplinary action as provided for in the company's bylaws.

Security and control systems, including access restrictions and limitations, are in place to protect against unauthorized access and other improper actions. The company continually takes measures to improve the IT service's technical infrastructure and software year after year, as this unit is responsible for ensuring the company's information security.

When determining the amount, category, storage period, and access to data, the company ensures that organizational and technical measures are in place to allow data processing only to the extent necessary for the specific purpose of processing

Data in material form is stored with a designated data processor who is obligated to store these materials properly and ensure their confidentiality. This duty is outlined in the company's internal regulations. The company has designated areas for storing material documents, where appropriate measures are taken to ensure the safety and security of the stored materials.

Company employees sign a commitment document related to personal data protection, which forms an integral part of the employment agreement. Violations of this commitment will result in appropriate consequences for the employee.

Employees of the company are obliged to protect personal data of passengers, ensure their proper procession in accordance with the legislation and the internal regulations of the company and to protect them from disclosure, modification, deletion and loss.

Employees of the company are obliged to not transfer the personal data received within the scope of their job-related duties to any other person and to protect confidentiality thereof. The mentioned obligation remains after/even in case of the employees' resignation (leaving the company). In case of any violation of this requirement, the employees will be held responsible accordingly.

Other provisions

1. Issues of data processing not defined in this document are regulated by the company's internal regulations and legislative requirements.
2. The company may change the personal data protection policy document at any time.