

## Privacy Policy

### About Us

- Airline GEO SKY LLC is a dynamic and highly qualified aviation services provider company, certified by the Civil Aviation Agency of Georgia.
- Company's scope of activity includes cargo air transportation and freight services.
- Additional information about our main activities can be found at <https://airgeosky.com/ka>

**Company Address:** 2 Guram Meliva Street, 0144, Isani District, Tbilisi, Georgia

**Company Email Address:** [info@airgeosky.com](mailto:info@airgeosky.com)

**Data Protection Officer:** Legal & Data Security Center LLC (ID: 405771829)

**Data Protection Officer Contact Details:** [dpo@airgeosky.com](mailto:dpo@airgeosky.com)

### 1. Purpose of This Policy

- 1.1.** The Privacy Policy (hereinafter "Policy" or "Privacy Policy") of Airline GEO SKY LLC (hereinafter "Company", "We/Us/Our" or "Data Controller") is based on principles defined in accordance with the Law of Georgia "On Personal Data Protection" and fully complies with it. Company strictly protects the security and confidentiality of personal information and, in accordance with Georgian legislation, provides for the process of collecting and using personal information and data protection procedures.
- 1.2.** Company is committed to ensuring the protection of fundamental human rights and freedoms, including in terms of privacy, personal space, inviolability of communications, and protection of Personal Data. Company attaches particular importance to the protection of Personal Data of employees and all subjects in pre-contractual and contractual relationships. Therefore, when processing Personal Data, Company acts in accordance with the Law of Georgia on "Personal Data Protection", other legal acts, and Privacy Policy.
- 1.3.** This Policy document defines the principles, methods, and procedures by which Company is guided when processing Personal Data.

### 2. Legislation Underlying Privacy Policy

**2.1.** Personal Data is processed by Us in accordance with the Chicago Convention of 1944 on International Civil Aviation, International Civil Aviation Organization (ICAO) regulations (Annex 9 – Facilitation), International Air Transport Association (IATA) regulations, EASA/SAFA regulations, and the Law of Georgia "On Personal Data Protection". Your rights are protected in accordance with Georgian legislation and the European Data Protection Regulation (GDPR).

**2.2.** In the process of Data Processing, We are also guided by sector-specific regulatory legislation, including but not limited to:

**2.2.1.** "Air Code of Georgia".

**2.2.2.** Order N142 of the Director of LEPL - Civil Aviation Agency on approval of "Rules for Aircraft Operator Certification".

**2.2.3.** Order N196 of the Director of LEPL - Civil Aviation Agency on approval of "Safety Management System Rules".

**2.2.4.** Order N97 of the Director of LEPL - Civil Aviation Agency "On Approval of Rules for Aviation Event Reporting and Distribution of Information About Aviation Events".

**2.2.5.** Order N172 of the Director of LEPL - Civil Aviation Agency "On Approval of Rules for Certification of Aircraft Airworthiness Management Organizations".

**2.2.6.** Order N62 of the Director of LEPL - Civil Aviation Agency "On Approval of Aviation Security Training Program in Civil Aviation".

**2.2.7.** Order N70 of the Director of LEPL - Civil Aviation Agency "On Approval of Special Permit Issuance Rules".

**2.2.8.** Order N168 of the Director of LEPL - Civil Aviation Agency "On Approval of Working Time and Flight Time Standards for Civil Aviation".

**2.2.9.** Order N4 of the Director of LEPL - Civil Aviation Agency "Rules for Aviation Medical Centers, Certification of Aviation Medical Experts and Medical Certification of Aviation Specialists".

**2.2.10.** Law of Georgia "On Personal Data Protection".

**2.2.11.** Other legal acts in force during business operations.

When processing Personal Data, We take into account international and local recommendations and protocols, including those of the Personal Data Protection Service (from March 02, 2026 State Audit Office) (hereinafter "Service") of Georgia.

### **3. Definition of Terms**

The terms used in this Policy have the meanings defined by the Law of Georgia "On Personal Data Protection" and other legislative acts, specifically:

**3.1. Data Controller** - a person who, individually and/or jointly with others, determines the purposes and means of Personal Data processing, and carries out Data Processing directly or through a Data Processor.

**3.2. Personal Data (hereinafter "Data" or "Personal Data")** - any information relating to an identified or identifiable natural person. A natural person is identifiable when it is possible to identify them directly or indirectly, including by name, surname, identification number, geolocation data, electronic communication identifiers, physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics.

**3.3. Special Categories of Data** - Data connected to a person's racial or ethnic origin, political views, religious, philosophical or other beliefs, membership of professional unions, health, sexual life, status of an accused, convicted or acquitted person or a victim in criminal proceedings, conviction, criminal record, diversion, recognition as a victim of trafficking in human beings or of a crime under the Law of Georgia on the Elimination of Violence against Women and/or Domestic Violence, and the Protection and Support of Victims of Such Violence, detention and enforcement of his/her sentence, or his/her Biometric and Genetic Data that are processed to allow for the unique identification of a natural person.

**3.4. Data Concerning Health** - Data related to the physical or mental health of Data Subject, including the provision of health care services, which reveal information about his/her physical or mental health.

**3.5. Data Processing** - any operation performed on Personal Data, including collecting, obtaining, accessing, photographing, video monitoring and/or audio monitoring, organising, grouping, interconnecting, storing, altering, retrieving, requesting for access, using, blocking, erasing or destroying, and disclosing by transmission, publication, dissemination or otherwise making available.

**3.6. Data Subject (hereinafter "Data Subject" or "You")** - any natural person whose Data is being processed;

**3.7. Consent** – will freely and unambiguously expressed by Data Subject after the receipt of the respective information, by an active action, in writing (including in electronic form) or verbally, to the processing of Data concerning him/her for specific purposes.

**3.8. Written Consent of Data Subject** - Consent signed by Data Subject or otherwise expressed in writing (including electronically) for processing of Data about them for a specific purpose after receiving appropriate information.

**3.9. Data Controller (hereinafter "Controller")** - a natural person, a legal person, or a public institution, who individually or in collaboration with others determines the purposes and means of the processing of Data, and who directly or through Processor processes Data.

**3.10. Data Processor (hereinafter "Processor")** - a natural person, a legal person, or a public institution, which processes Data for or on behalf of Controller. A natural person who is in labour relations with Controller shall not be considered as Processor.

**3.11. Third Party** - a natural person, a legal person, or a public institution, other than Data Subject, Service, Controller, Processor, a special representative and persons who, under the direct authority of Controller or Processor, are authorized to process Data.

**3.12. Data Protection Officer** - a person designated/appointed by Data Controller or Data Processor who performs functions provided for in Article 33 of the Law of Georgia "On Personal Data Protection".

**3.13. Biometric Data** - Data processed using technical means and related to the physical, physiological or behavioural characteristics of Data Subject (such as facial images, voice characteristics or dactyloscopic data), which allow the unique identification or confirm the identity of that Data Subject.

**3.14. Genetic Data** - Data relating to the acquired or inherited genetic characteristics of Data Subject which, through an analysis of a biological sample from that Data Subject, give unique information about his/her physiology or health;

**3.15. Flight Crew** - specially trained Flight Crew members, holding certificates for operation for a specific type of aircraft and its equipment in flight.

**3.16. Aircraft Crew** - persons (Flight Crew member and service crew member) who are responsible for aircraft operation and performance of specific service duties when carrying out a flight mission.

#### **4. Company Observes the Following Principles When Processing Any Personal Data**

**4.1. Principle of Legality and Fairness** - We process Personal Data according to procedures and grounds established by legislation. We comply with rules for processing Special Categories of Data in accordance with international and local regulatory body recommendations/protocols. We ensure protection of Data Subject rights and process Personal Data in compliance with the principle of equality (exclusion of discrimination).

**4.2. Principle of Transparency** - Data Processing process is transparent to Data Subject. Before starting Data Processing, Data Subject is provided with information about the purpose, scope of Data Processing, and Data Subject rights. Data Subject can contact Us at any time and receive information about Data Processing according to procedures and deadlines established by Georgian legislation. We notify Data Subjects about incidents related to Personal Data that may affect their rights.

**4.3. Principle of Purpose Limitation** - We process Personal Data only for the specific purpose for which it was obtained. For using Consent-obtained Data for other purposes, We request their Consent again.

**4.4. Principle of Data Minimization** - We process Personal Data only to the extent necessary to achieve the purposes stated in this document and/or established/legitimate purposes by legislation. When processing Data, We consider the proportionality of purpose and Data volume and the impact of Data Processing on human rights. Considering this, whenever possible, We pseudonymize Data.

**4.5. Principle of Data Accuracy** - We ensure that Personal Data stored with Us, obtained by Us, and provided by Data Subject is accurate and authentic. We immediately correct or delete inaccurate Data, both at Data Subject's request and when We discover an error. We inform Third Parties to whom We transmitted Data about Data corrections.

**4.6. Principle of Storage Limitation** - We store Data only for the period necessary to achieve the purpose (a specific period is defined for each Data category). For Personal Data storage, We define in advance a specific period or indicate criteria for determining the period, except when Data storage period is established by legislation.

**4.7. Principle of Data Security** - To protect Data security, when processing Data We take technical and organizational measures that adequately ensure Data Protection, including from unauthorized or illegal processing, accidental loss, damage, disclosure, and/or destruction. We observe the principle of confidentiality and, to protect this principle, define the circle of persons who, based on their functions, have access to Personal Data.

#### **5. Where We obtain Your Data**

##### **5.1. We receive information about You from You when:**

**5.1.1.** You contact Us with an application or notification and request to use Our services;

**5.1.2.** You notify Us about an incident related to Personal Data;

**5.1.3.** You contact Us with an application/complaint related to matters within Our competence;

**5.1.4.** You participate in a competition announced for a vacant position;

**5.1.5.** You are in an employment relationship with Us;

**5.1.6.** You enter into a service contract with Us;

**5.1.7.** You contact Us by phone or/and send Us a message via email;

**5.1.8.** You visit Our websites;

**5.1.9.** You contact Us with a request to exercise Your rights as Data Subject.

##### **5.2. We also obtain Your Data when:**

- 5.2.1. Information about You is indicated in an application submitted by another person;
- 5.2.2. You are a person authorized to represent/manage a legal entity that wishes to enter into a relevant service contract with Us.

## **6. Why and How We Use Your Data**

- 6.1. When You contact Us as an international air carrier and wish to receive Our services.
- 6.2. Based on the scope of activity, Personal Data is processed by Company on the basis of a relevant transaction/contract and/or legislative/regulatory act, for the purpose of concluding a contract to provide services of interest to You.

### **6.3. Where We Obtain Data**

Company, as an air carrier, obtains Data from the following sources:

- a) Directly from Data Subject

Data Subject (cargo air transportation customer) personally provides personal information in the following formats:

- ✓ When filling out an application;
- ✓ When providing necessary information.

- b) From the customer organization

Enterprise or organization representative orders air transportation from Company and provides:

- ✓ Requisites necessary for contract execution.

### **6.4. What Data We Process**

To execute a relevant service contract, we require:

- ✓ Customer organization or/and individual Data - name/title, personal number/identification number, contact details, bank details;
- ✓ Required documents: air transport document (AWB), commercial invoice, product list, and necessary permits for restricted, dangerous, or special items.

### **6.5. Why We Use It**

Processing of the above Data serves clearly defined purposes:

- ✓ Transaction/contract execution;
- ✓ Fulfillment of obligations under the transaction/contract;
- ✓ Reporting to the Civil Aviation Agency or other authorized bodies and fulfillment of obligations defined by law;
- ✓ Internal analysis and statistics production, with Data anonymization.

### **6.6. Legal Basis for Processing**

When processing Data, We rely on the following grounds:

- 6.6.1. Article 5, Paragraph 1, Subparagraph "b" of the Law of Georgia "On Personal Data Protection" - to fulfill obligations under a contract with Data Subject or to conclude a contract at Data Subject's request;
- 6.6.2. Article 5, Paragraph 1, Subparagraph "c" of the Law of Georgia "On Personal Data Protection" - Data Processing is provided for by law;
- 6.6.3. Article 5, Paragraph 1, Subparagraph "d" of the Law of Georgia "On Personal Data Protection" – Data Processing is necessary to fulfill obligations imposed on Us by Georgian legislation;
- 6.6.4. Article 5, Paragraph 1, Subparagraph "i" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to protect significant legitimate interests of Us or Third Party, unless there is an overriding interest in protecting the rights of Data Subject (including minors);
- 6.6.5. Article 5, Paragraph 1, Subparagraph "j" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to consider Your application.

### **6.7. To Whom We Transfer Data**

Data transfer procedure is strictly controlled and carried out only in the cases specified below.

- ✓ We, as a service provider, transfer Personal Data only for clearly defined purposes permitted by law and international regulations.

#### **To state and regulatory bodies:**

- LEPL Civil Aviation Agency of Georgia - only to the extent necessary to fulfill legal obligations;

- Law enforcement and investigation structures - only in case of court decision or existence of appropriate legal grounds, with strict limitation of information volume;
- Border protection and security state agencies;
- Relevant aviation regulatory or security structures of the country in whose territory transit occurs;
- International and foreign state bodies.

**To public and private service providers:**

- Transport service providers - for service provision;
- IT service providers - within the framework of internal systems technical support, only to the extent necessary to provide the service.

- All such transfers are governed by agreement and Personal Data protection requirements.
- Company records each case of Data transfer to Third Parties.

## 7. Conducting Competitions for Vacant Positions

### 7.1. Where We Obtain Data

7.1.1. When submitting an application for participation in a competition announced for a vacant position, We receive information indicated in Your application and attached documents about You and other persons. In case of participation in subsequent stages of the competition, We obtain additional information provided by You within the framework of the relevant stage. Your Data may also be provided to Us through applications submitted by other persons. For example, if a candidate names You as a reference, or when You sign a document that the candidate submitted to confirm work experience.

### 7.2. What Data We Process

7.2.1. Within the framework of conducting competitions for vacant positions, We obtain:

From the candidate participating in the competition:

- Name and surname;
- Date of birth;
- Email address and phone number;
- Information about citizenship;
- Information about education and work experience;
- Information about declaration for subsequent stages of the competition;
- Information contained in works created when performing written or other types of assignments;
- Other information about the candidate and other persons indicated in the submitted application and attached documents. Parallel to the candidate's participation in different stages of the competition, information about assessments and results received by the candidate at each stage accumulates;
- Along with information about Your identity, date of birth, citizenship, and contact details, You should submit only Data that will be useful for assessing Your compliance with qualification requirements defined within the framework of a specific competition.

### 7.3. Why We Use It

Within the framework of conducting competitions, We process Data to assess candidates' compliance with established competition conditions, select the best among them, and inform each candidate about the decision made regarding them.

### 7.4. Legal Basis for Processing

When processing Data within the framework of conducting competitions for vacant positions, We rely on the following grounds:

- 7.4.1. Article 5, Paragraph 1, Subparagraph "c" of the Law of Georgia "On Personal Data Protection" - Data Processing is provided for by law;
- 7.4.2. Article 5, Paragraph 1, Subparagraph "d" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to fulfill obligations imposed on Us by Georgian legislation;
- 7.4.3. Article 5, Paragraph 1, Subparagraph "j" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to consider Your application.

### 7.5. To Whom We Transfer Data

**7.5.1.** We do not transfer documentation/information submitted by You within the framework of competitions to any Third Party, unless required by current legislation.

## **8. Personal Data Received Within the Framework of Employment Relationship**

### **8.1. Where We Obtain Data**

We, as an employer, collect Data within the framework of employment relationship only from the employed person. Also, Data may be verified with references provided by the employed person or/and with the relevant educational institution.

### **8.2. What Data We Process**

For the purpose of establishing an employment relationship, Company as an employer processes the following categories of Data:

- **Employee identification Data** - name, surname, citizenship, address, date of birth, place of residence, education, profession, workplace, employee's passport data;
- **Employee contact information** - address, phone number, email;
- **Documents confirming employee qualification** - qualification and professional certificates;
- **Financial and insurance information** - details related to employee insurance and provision of salary remuneration;
- **Special Categories of Data** - requirement established for pre-defined specific positions - certificate of criminal record, certificate of drug addiction registration, form N IV-100/a, periodic medical examination, which may include - alcohol/drug testing. Aviation specialist medical certificate which is a requirement established by legislation.

### **8.3. Why We Use It**

We, as an employer, process Data within the framework of employment relationship for clearly defined, legal, and proportional purposes, which include:

- Ensuring the start, implementation, and completion of employment relationship, including:
  - Identification of person, contact with them, information;
  - Assessment of candidate's suitability for a specific position;
  - Agreement and execution of employment contract terms;
  - Inclusion of employee in internal registration systems;
  - Definition of necessary rights and obligations for the employee.
- Ensuring legally provided and internal organizational services for employees, including:
  - Salary remuneration payment;
  - Administration of taxes and other payments and mandatory contributions provided for by Georgian legislation;
  - Administration of health insurance, social packages, or other compensation mechanisms.
- Fulfillment of labor and social security requirements, including:
  - Monitoring employee health status (e.g., periodic medical examination);
  - Ensuring criminal record, drug addiction registration status, or alcohol/drug testing necessary for specific positions, in accordance with relevant legislation and organizational standards.
- Management of information provided for by labor legislation and internal regulations, specifically:
  - Ensuring communication with employee - in writing, by phone, or electronically;
  - Managing internal structural changes, position changes, or transfer processes;
  - Creating user accounts in internal corporate programs for them;
  - Optimization of internal administrative and organizational processes.
- Risk prevention, control, and security management, including:
  - Using employee Data for access control, entry into workspace, or defining special access;
  - Using Personal Data necessary to ensure technical or infrastructure security.

- Fulfillment of legal obligations and regulatory requirements, including:
  - Supporting legally established reporting, audit, or inspection processes;
  - Cooperation with relevant state bodies within the framework of legal disputes, investigation processes, or administrative proceedings.
- Ensuring measures necessary for business trips and other support processes, specifically:
  - Processing Data necessary to manage employee visa, travel documentation, and other related procedures;
  - Ensuring employee professional competence and presentation in other companies or partner organizations, including abroad.

#### **8.4. Legal Basis for Processing**

When processing Data within the framework of employment relationship, We rely on the following grounds:

- Article 5, Paragraph 1, Subparagraph "b" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to fulfill obligations under a contract with You;
- Article 5, Paragraph 1, Subparagraph "c" of the Law of Georgia "On Personal Data Protection" - Data Processing is provided for by law;
- Article 5, Paragraph 1, Subparagraph "d" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to fulfill obligations imposed on Us by Georgian legislation;
- Article 5, Paragraph 1, Subparagraph "j" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to consider Your application.

When processing information containing Special Categories of Data obtained during the establishment of employment relationship, We rely on the following grounds:

- Article 6, Paragraph 1, Subparagraph "b" of the Law of Georgia "On Personal Data Protection" - processing of Special Categories of Data is directly and specifically regulated by law and their processing is necessary and proportional measure in a democratic society;
- Article 6, Paragraph 1, Subparagraph "h" of the Law of Georgia "On Personal Data Protection" - processing of Special Categories of Data is necessary based on the nature of labor obligations and relationships, including to make employment decisions or to assess employee work abilities.

#### **8.5. To Whom We Transfer Data**

Data transfer procedure is strictly controlled and carried out only in the cases specified below.

We, as an employer, transfer Personal Data only for clearly defined purposes permitted by law and international regulations. Data may be transferred to **state and regulatory bodies**:

- Civil Aviation Agency of Georgia - only to the extent necessary for aviation safety, certification, admission, or fulfillment of legal obligations;
- Tax authorities, Social Service Agency, and other state agencies - within the framework of providing information established by law (e.g., salary Data, information about social contributions);
- Law enforcement and investigation structures - only in case of court decision or existence of appropriate legal grounds, with strict limitation of information volume;
- International and foreign state bodies, only in cases provided for by legislation and international agreements;
- In cases when an employee travels abroad (on business trip or as Crew Member) and visa, travel documentation, security, or registration procedures are necessary, Data transfer is carried out to:
  - ❖ Embassies and consulates of specific countries;
  - ❖ Border protection and security state agencies;
  - ❖ Relevant aviation regulatory structures of the country in whose territory transit occurs.

#### **To public and private service providers:**

- To the extent necessary for effective management of employment relationship or provision of services to employees:
  - ❖ Insurance companies - for health, life, or other types of mandatory or voluntary insurance processes;
  - ❖ Banking and financial service providers - for salary remuneration transfer;
  - ❖ Travel agencies, transport service providers - for organizing business trips;

- ❖ IT service providers - within the framework of internal systems technical support, only to the extent necessary to provide the service.

All such transfers are regulated by contracts and taking into account Personal Data protection requirements.

#### **To educational and training institutions:**

As necessary, transferred Data aims to verify employee professional qualification, to ensure certification or accreditation processes.

➤ Company records each case of Data transfer to Third Parties.

## **9. Recording Visits to Our Website**

### **9.1. Where We Obtain Data**

When visiting Our websites, We record information about Your visit.

### **9.2. What Data We Process**

When entering the website, We collect the following Data from You:

- Date and time of website entry;
- Internet Protocol (IP) address;
- Type of device used;
- Name of web browser used;
- Visitor location.

### **9.3. Why We Use It**

We use Data obtained within the framework of recording website visits to detect and respond to possible information security incidents, which is necessary, among other things, to ensure the integrity of Our electronic systems and maintain business continuity. Also, to offer You an acceptable working language through which You can receive information from the website.

### **9.4. Legal Basis for Processing**

When processing Data within the framework of recording website visits, We rely on the following ground:

- 9.4.1. Article 5, Paragraph 1, Subparagraph "i" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to protect Our legitimate interests.

### **9.5. To Whom We Transfer Data**

We transfer Data about website visitors to Our Data Processor for storage. Information about IP address is stored on the Cloudflare platform for no more than 7 (seven) days from the visit.

In case of signs of crime, Data may be transferred to authorized investigation body.

## **10. Consideration of Data Subject Requests**

### **10.1 Where We Obtain Data**

When You contact Us with a request to exercise any Data Subject right provided for by the Law of Georgia "On Personal Data Protection".

### **10.2. What Data We Process**

Within the framework of considering applications submitted with requests to exercise Data Subject rights, We obtain:

- 10.2.1. Data indicated in Your application and materials attached to it about You and other persons;
- 10.2.2. Additional information, if We need it to properly identify You or/and properly verify representative authority transferred to You.

### **10.3. Why We Use It**

We process Data obtained within the framework of considering applications submitted with requests to exercise Data Subject rights in order to respond to them according to the procedure established by law and inform You of Our decision.

### **10.4. Legal Basis for Processing**

When processing Data within the framework of considering applications submitted with requests to exercise Data Subject rights, We rely on the following grounds:

- 10.4.1. Article 5, Paragraph 1, Subparagraph "d" of the Law of Georgia "On Personal Data Protection" - Data Processing is necessary to fulfill obligations imposed on Us by Georgian legislation;
- 10.4.2. Article 5, Paragraph 1, Subparagraph "j" of the Law of Georgia "On Personal Data Protection" – Data Processing is necessary to consider Your application.

#### **10.5. To Whom We Transfer Data**

Data obtained within the framework of considering applications submitted with requests to exercise Data Subject rights may be transferred to:

- Data Processor providing postal services;
- Persons defined by law in case of decision to correct, update, supplement, stop processing, delete, or destroy Data;
- Court, in case of appealing Our decision.

### **11. Video Monitoring of Our Buildings**

#### **11.1. Where We Obtain Data**

We have video cameras installed at the entrance and external perimeter of Our administrative buildings. Accordingly, if You move in this territory, We will receive video recording containing Your image.

#### **11.2. What Data We Process**

Through video monitoring system, We obtain only video recording containing images. We do not conduct audio monitoring through the system.

#### **11.3. Why We Use It**

We use Data obtained as a result of video monitoring for the following purposes:

- To protect the safety of Our employees and visitors;
- To protect Our, employees', and visitors' property;
- To protect confidential information available to Us.

#### **11.4. To Whom We Transfer Data**

Recordings obtained through video surveillance system may be transferred to law enforcement body or court, if this is necessary for the above-mentioned purposes, or to fulfill obligations imposed on Us by legislation.

### **12. Audio Monitoring**

#### **12.1. Where We Obtain Data**

12.1.1. Audio monitoring takes place on Company's hotline (+995 032 2 777 400) through a call made by Data Subject, based on prior warning and awareness about recording by audio signal before starting audio monitoring for Data Subject;

12.1.2. When using Company's hotline (telephone communication), Data Subject expresses Consent to processing of Their Personal Data;

12.1.3. Audio monitoring takes place throughout the telephone communication period, except for the existence of obstructive circumstances.

#### **12.2. What Data We Process**

Within the framework of recording telephone calls, We store the following information:

- Telephone numbers of call initiator and addressee;
- Call initiation time;
- Call duration;
- Conversation.

#### **12.3. Why We Use It**

Within the framework of recording telephone calls, We process Data in order to accurately record facts of contact by telephone and ensure appropriate response to appeals.

#### **12.4. Legal Basis for Processing**

When processing Data within the framework of recording telephone calls, We rely on the following ground:

**12.4.1.** Article 5, Paragraph 1, Subparagraph "i" of the Law of Georgia "On Personal Data Protection" – Data Processing is necessary to protect Our legitimate interests.

### **13. Organization and Conducting of Information and Educational Events**

#### **13.1. Where We Obtain Data**

**13.1.1.** During registration (both mandatory and voluntary) for attending an information or educational event organized by Us, We obtain Data submitted by You through the registration form;

**13.1.2.** We obtain Data from You to record Your attendance at the event and determine needs based on Your qualifications;

**13.1.3.** In addition, We obtain Your Data when taking photos and videos during the ongoing event.

#### **13.2. What Data We Process**

During the registration process for attending the event, We obtain from persons wishing to attend:

- Name and surname;
- Email address and phone number;
- Other Data indicated in the registration form.

When recording Your attendance at the event, We obtain:

- Name, surname, and signature;
- Other Data indicated in the attendee registration form;
- In case of Your photo-video recording at the event, We will warn You in advance about this and, if necessary, obtain Your Consent.

#### **13.3. Why We Use It**

**13.3.1.** Within the framework of registration and attendee recording, We process Data in order for this to be stored in employees' personal files to confirm their qualification improvement;

**13.3.2.** We publish photo-video materials recorded at events on Our website and social networks to provide information about Our activities.

#### **13.4. Legal Basis for Processing**

When processing Data within the framework of registration and attendee recording of persons wishing to attend events, We rely on the following grounds:

- Article 5, Paragraph 1, Subparagraph "a" of the Law of Georgia "On Personal Data Protection" – We have Your Consent; Article 5, Paragraph 1, Subparagraph "b" of the Law of Georgia "On Personal Data Protection" – Data Processing is necessary for the performance of a contract entered into with You; Article 5, Paragraph 1, Subparagraph "d" of the Law of Georgia "On Personal Data Protection" – Data Processing is necessary to fulfill obligations imposed on Us by Georgian legislation.

When taking photos and videos at events and placing prepared materials on Our website and social networks, We rely on the following grounds:

- Article 5, Paragraph 1, Subparagraph "a" of the Law of Georgia "On Personal Data Protection" - We have Your Consent.

#### **13.5. To Whom We Transfer Data**

Photo-video materials showing persons attending events, which We place on Our website and social networks, become accessible to any person who visits Our website and pages created on social networks.

### **14. International Data Transfer**

**14.1.** Company, within the framework of international air transportation specifics for the purposes of International Data Transfer, is obliged to act in accordance with the Georgian legislation, as well as:

- According to requirements of the "Convention on International Civil Aviation" (Chicago Convention, 1944);
- According to International Civil Aviation Organization (ICAO) regulations, including: o Annex 1 – Personnel Licensing;
- Annex 9 – Facilitation; o Annex 13 – Aircraft Accident and Incident Investigation; o Annex 17 – Security;

- According to International Air Transport Association (IATA) regulations and standards;
- According to European Aviation Safety Agency (EASA) norms and Safety Assessment of Foreign Aircraft (SAFA) standards;
- According to requirements provided for by internal legislation of relevant states, including:
- Advance Cargo Information (ACI);
- API/EAPIS systems;

**14.2.** International transfer of Your Personal Data may be necessary to provide You with the service You requested. Company takes appropriate measures that are necessary in relation to recipients of Your Personal Data to ensure an adequate level of protection defined by current law on Personal Data Protection. Data recipient ensures an adequate level of Data Protection if they use standard contractual clauses issued by the European Commission or there is a European Commission decision stating that the country to which Personal Data is transferred ensures an adequate level of Data protection.

**14.3.** If it is impossible to ensure an adequate level of Personal Data protection in connection with Data transfer abroad, then We will request Your express Consent in connection with such transfer of Data abroad.

## **15. How Long We Store Your Data**

**15.1.** We store Data received by Us only for the period necessary to achieve the above-mentioned purposes or/and to fulfill obligations imposed on Us by legislation in connection with Data storage.

**15.2.** Data storage periods existing with Us are regulated according to the procedure established in Company.

**15.3.** Storage of Personal Data by Company is carried out in a secure place.

**15.4.** Company determines Personal Data storage periods for each individual Data category, based on law, its interests, and legitimate purposes.

**15.5.** Company is guided by the following criteria regarding Data storage periods:

- Periods provided for by legislation;
- Periods provided for by contract;
- Periods based on statute of limitations, except for exceptional cases;
- Control body inspection periods;
- Existence of legitimate purpose and/or interest;
- Service provision specifics/scope.

## **16. Third Party Websites**

**16.1.** Company's website may offer You links to other websites for Your convenience and information. Please note that these sites may be owned and operated by other companies and organizations and have different security and privacy policies. Company has no control over and assumes no responsibility for information, materials, products, or services placed or accessible through these web pages.

## **17. Which Data Processors We Use**

**17.1.** Your Personal Data may be transferred only to persons authorized by Company to process Personal Data, including contractor companies that provide relevant services.

**17.2.** Transfer of Personal Data to Data Processor is carried out on the basis of law or/and contract, which defines processing grounds and purposes, categories of Data to be processed, Data Processing period, and rights and obligations of Data Controller and Data Processor.

**17.3.** Data Processor is obliged to comply with Personal Data protection legislation and ensure confidentiality of information in their possession.

**17.4.** Data Processor is obliged to process Data within Their competence and based on legal purpose, which is necessary in accordance with current legislation and existing contractual relationships to provide relevant services, for employees' rights and their realization, for employee information management, for fulfillment of obligations imposed by legislation, and for other needs.

**17.5.** Data Processor is obliged not to disclose and not to transfer Personal Data to Third Parties.

**17.6.** Data Processor is obliged to protect Personal Data, including Special Categories and health-related Personal Data (if any), to process them fairly, legally, transparently, without violating Data rights.

**17.7.** Data Processor who, based on contractual relationship, processes Personal Data, is responsible for disclosure of Personal Data, illegal use, loss, illegal obtaining, alteration, illegal destruction, and other illegal actions.

**17.8.** Every Data Processor is obliged to process Data for the purpose defined by Company and maintain confidentiality of received information. Additionally, Data Processor must have implemented organizational and technical security measures. For violation of these obligations, Data Processor is fully liable for damage/harm caused to Company or/and any Third Party.

**17.9.** In case of termination of contractual relationship, Data Processor is obliged to immediately ensure return of Personal Data to Data Controller, cessation of Data Processing, and deletion of Personal Data from their own database, at the request of Data Controller.

**17.10.** Data Processors may include, among others and not limited to:

- Information technology (IT) service providers;
- Postal service providers;
- Medical insurance companies (for administration of insurance claims);
- Telephone and communication service providers;
- International or/and local training companies;
- Hotels;
- International or/and local airports.

## **18. What Rights You Have**

**18.1.** You have the following rights regarding Your Data held by Us:

- Right to receive information about Data Processing;
- Right to access Data and receive copies;
- Right to correct, update, and supplement Data;
- Right to cease Data Processing, delete, or destroy Data;
- Right to block Data;
- Right to Data transmission;
- Rights related to automated individual decisions;
- Right to withdraw Consent;
- Right to appeal.

Specifically:

### **➤ Right to Receive Information About Data Processing**

You have the right to request Company to confirm whether Data about You is being processed and whether it is justified. Also, to receive other information related to processing free of charge.

You have the right to receive the above information no later than 10 (ten) working days from Your request. This period may be extended in exceptional cases with proper justification by no more than 10 (ten) working days.

### **➤ Right to Access Data and Receive Copies**

You have the right to access Personal Data about You held by Company and receive copies of this Data free of charge, except when Georgian legislation provides for a fee or Company has established a reasonable fee.

You have the right to access this Data or/and receive their copies no later than 10 (ten) working days from the request (unless another period is established by Georgian legislation). This period may be extended in exceptional cases with proper justification by no more than 10 (ten) working days.

### **➤ Right to Correct, Update, and Supplement Data**

You have the right to request Company to correct, update, or/and supplement false, inaccurate, or/and incomplete Data about You.

No later than 10 (ten) working days from submission of the request (unless another period is established by Georgian legislation), Data must be corrected, updated, or/and supplemented, or You must be informed of the grounds for refusing the request and explained the procedure for appealing the refusal.

#### **> Right to Cease Data Processing, Delete, or Destroy Data**

You have the right to request Company to cease processing (including profiling) of Data about You, delete, or destroy Data.

No later than 10 (ten) working days from submission of the request (unless another period is established by Georgian legislation), Data Processing must be ceased or/and Data must be deleted or destroyed, or You must be informed of the grounds for refusing the request and explained the procedure for appealing the refusal.

#### **> Right to Block Data**

You have the right to request Company to block Data, i.e., temporarily suspend Data Processing (except storage). This can be implemented when one of the circumstances provided for by law exists.

You have the right to receive information about the decision made regarding Data blocking or grounds for refusing Data blocking immediately upon making the decision, but no later than 3 (three) working days from the request.

#### **> Right to Data Transmission**

You have the right, on grounds provided for by law, in case of automatic Data Processing, if technically possible, to receive from Company in a structured, commonly used, and machine-readable format the Data You provided, or to request transfer of this Data to another Data Controller.

For example, You have the right to request Company to transfer Your Personal Data (as a person participating in training) to another educational institution.

In each case mentioned above, according to Your request, Company will take appropriate measures to protect Your rights, freedoms, and legitimate interests, including by involving human resources in the decision-making process, giving You the opportunity to express Your opinion and appeal the decision.

#### **> Right to Withdraw Consent**

You have the right, at any time, without any explanation or justification, to withdraw Consent You have given. This must be done in the same form in which Consent was declared.

You have the right to request and receive information about possible consequences of withdrawing Consent before withdrawing Consent from Company.

According to Your request, Data Processing must be ceased or/and processed Data must be deleted or destroyed no later than 10 (ten) working days from the request, unless there is another legal basis for Data Processing.

#### **> Right to Appeal**

You have the right, in case of violation of rights and established procedures provided for by the Law of Georgia “On Personal Data Protection” or/and this Policy, to contact Service or/and court according to the procedure established by law.

#### **18.2. Your rights may be restricted if their implementation may pose a threat to:**

- State security, information security and cybersecurity, or/and defense interests;
- Public security interests;
- Crime prevention, crime investigation, criminal prosecution, administration of justice, execution of imprisonment and deprivation of liberty, execution of non-custodial sentences and probation, operational-investigative activities;
- Detection of violation of professional ethics norms, including regulated professions, and imposing liability;
- Your or other persons' rights and freedoms, including freedom of expression;
- Justification of legal claim or objection;
- Implementation of functions and powers of regulatory or/and supervisory bodies in the above-mentioned areas;
- Protection of state, commercial, professional, and other types of secrets provided for by law.

In case of need to restrict Your rights, We will use the restriction only to the extent necessary to achieve the purpose of the restriction.

### **19. Data Security**

#### **19.1. Company ensures secure processing of Personal Data and for this purpose We apply all necessary technical and organizational measures.**

**19.2.** In Company We protect Personal Data from unauthorized or illegal access, accidental loss, damage, disclosure, or destruction.

**19.3.** After achieving the purpose of Personal Data Processing, We regularly delete and destroy Personal Data with observance of specified periods without possibility of recovery, or We store them in depersonalized form for analytical and statistical purposes.

**19.4.** Our employees are bound by confidentiality obligations, both by employment contracts concluded with them and by internal regulations. Our employees maintain the obligation to protect confidentiality even after completion of their employment contract.

**19.5.** When processing Personal Data, for Data security Company ensures consistent implementation of the following appropriate software, electronic, digital measures:

- **Data Protection:** A multi-layered approach is used that combines physical, technological, and administrative measures;
- **Digital and Physical Asset Security:** Security protocols are activated on electronic devices, digital files, and physical warehouses, so that systems are protected from unauthorized access, and Data integrity is ensured;
- **Access and Control Mechanisms:** Security control systems and access restrictions are used;
- **Strict Compliance and Training:** Personnel are trained and required to comply with Privacy Policy, which complies with both legislative and internal regulations;
- **Confidentiality:** Personal Data confidentiality is strictly protected in Company. Only those employees who need Data Processing to perform their assigned duties have access to them. Documentation existing in material form is stored in specially designated rooms for this purpose, whose security is ensured by technical and organizational security measures taken by Company. A non-disclosure agreement has been signed with all employees who have access to Confidential Information, according to which the obligation to maintain confidentiality remains in effect even if the aforementioned agreement is terminated for any reason.

## **20. Data Processing Control**

**20.1.** Compliance with this Policy and current legislation in the field of Data Protection is checked and controlled regularly. Verification and control are carried out by employees of Company's structural units equipped with appropriate authority and/or Data Protection Officer.

**20.2.** Company is obliged to ensure periodic training for employees to achieve unwavering fulfillment of requirements of this Policy and legislation related to Personal Data protection.

**20.3.** Company and any of its employees participating in Data Processing are obliged not to exceed the limits of authority granted to them. Additionally, they are obliged to maintain Data confidentiality, including after termination of their official authority.

## **21. Incident**

**21.1.** An incident constitutes a breach of Data security, which causes unlawful or accidental damage to Data, loss, as well as unauthorized disclosure, destruction, alteration, access to them, their collection/obtaining, or other unauthorized processing.

**21.2.** Data Processor and Data Controller are responsible for detecting an incident.

**21.3.** Information about any incident is submitted immediately, but no later than 72 (seventy-two) hours, to Service:

- At the request of Service;
- On own initiative (when the severity of consequences for Data Subjects' rights as a result of the incident is medium or high).

**21.4.** The procedure for incident management and notification is defined by Company's relevant internal document.

## **22. Company Personnel Obligations**

**22.1.** Each employee of Company is obliged to comply with Company's Privacy Policy.

**22.2.** Based on employment-legal relationship, Company employee who has access to Personal Data for official purposes and within their competence, including processes it and stores relevant documentation electronically or

materially, is obliged to comply with proper documentation procedures, confidentiality of records existing in documentation, and store this documentation in a secure place specially designated for this purpose in Company, where documentation will be protected from damage/destruction and Third-Party access.

**22.3.** Based on employment-legal relationship, Company employee who stores relevant documentation for official/legal purposes and processes Personal Data of a person within their competence is responsible for protecting documentation and disclosing Personal Data existing in documentation, illegal use, loss, illegal obtaining, alteration, and illegal destruction.

**22.4.** Company personnel are obliged to comply with Georgian legislation on Personal Data Protection and ensure protection of confidentiality of information about Data Subject in their possession.

**22.5.** When the issue concerns transfer of Personal Data about Data Subject to Third Parties/authorized bodies, each employee of Company is obliged to first verify the legality of such request with Company's legal department and/or Data Protection Officer, provide them with necessary information/documentation, and only on this basis, after receiving consultations and confirmation, provide information on behalf of Company.

**22.6.** Company employees are prohibited from leaving documents and files containing Personal Data unattended.

**22.7.** Company employee is obliged not to disclose and not to transfer other persons' Personal Data to Third Parties. The obligation to protect Personal Data remains in force even if the person is no longer in employment-legal relationship with Company. In case of violation of these requirements, Company is authorized to demand, and in this case the employee is obliged to compensate for damage/harm incurred.

**22.8.** Each employee of Company is obliged not to allow disclosure of their username and password used to access their work computer or/and Company's software to Third Parties, including other employees.

**22.9.** Each employee of Company is obliged to take all necessary measures that adequately ensure Data protection from accidental or illegal destruction, alteration, disclosure, obtaining, illegal use in any other form, and accidental or illegal loss.

### **23. Disciplinary Liability**

**23.1.** In case of violation of requirements of relevant Georgian legislation and Privacy Policy, Company is authorized to apply disciplinary liability measures defined by Company's internal regulations against the relevant employee.

**23.2.** Company decides on application of disciplinary liability measures according to the established procedure regarding disciplinary liability, for each individual case, based on assessment of actual circumstances and severity of violation.

### **24. Data Protection Officer**

**24.1.** Data Protection Officer is obliged to:

- Inform Data Processor, Data Controller and its employees on issues related to Data protection, including the adoption or amendment of regulatory legal norms, provide them with consultation and methodological assistance;
- Participate in developing internal regulations related to Data Processing and Data protection impact assessment documents, as well as monitoring the compliance of Data Controller or Data Processor with Georgian legislation and internal organizational documents;
- Analyze applications and complaints received in connection with Data Processing and issue appropriate recommendations;
- Receive consultations from Service, represent Data Controller and Data Processor in relations with Service, submit information and documents at its request, and coordinate and monitor the implementation of its tasks and recommendations;
- Provide information about Data Processing processes and rights of Data Subject upon request;
- Ensure performance of other functions by Data Controller or Data Processor in order to raise the standards of Data Processing.

**24.2.** Company has Data Protection Officer in compliance with requirements and deadlines provided for by Personal Data protection legislation.

**24.3.** Data Protection Officer represents an independent entity who provides consultations to Company and its Data Processors, gives expert advice on compliance with Personal Data protection requirements, and performs other functions from the perspective of Personal Data protection.

**24.4.** Company's Data Protection Officer is **Legal & Data Security Center LLC (ID: 405771829)**.

## **25. Final Provisions**

**25.1.** In case any point may be interpreted vaguely, or a conflict arises during application, Company undertakes to give priority to the high standard of Personal Data protection, align its action with current Georgian legislation, and decide in favor of Personal Data protection.

**25.2.** Issues reflected in this Policy do not mean and do not confirm that Company processes Data. This Policy defines rules that must be complied with when processing Data, if such exists.

## **26. Changes to the Privacy Policy**

**26.1.** Company reserves the right to update this Policy at any time. Information about changes to this Policy will be available both on Company's website and to any interested person at Company.

**26.2.** Issues not fully regulated by this Policy may be regulated by additional documents, as well as by introducing changes to this Policy or/and supplemented with provisions defined by current Georgian legislation.

## **27. Exercise of Rights**

**27.1.** Data Subject is authorized at any time to contact Company to receive information necessary for them in connection with this Policy, at the address: 2 Guram Meliva street, 0144, Isani District, Tbilisi, Georgia, by email: [info@airgeosky.com](mailto:info@airgeosky.com), or contact Company's Data Protection Officer, **Legal & Data Security Center LLC (ID: 405771829)** at the following email: [dpo@airgeosky.com](mailto:dpo@airgeosky.com).