POLICY ON PERSONAL DATA PROTECTION

1. Purpose and Scope

This Policy sets out the standards and principles followed by the company under the name "VITEX A.E.", with headquarters in Aspropyrgos, Attica, at "Imeros Topos", with G.E.M.I. No. 113357952000 (hereinafter referred to as the "*company*"), concerning the processing of personal data. The company, as the data controller, in the course of its business activities, which mainly consist of the industrial production and sale of building paints, insulation materials, and integrated external thermal insulation systems, in the domestic and international markets, processes personal data in accordance with the principles and the applicable legislation on data protection and takes necessary measures to ensure the confidentiality, integrity, and availability of these data.

This Policy applies to all natural persons whose data we process, including existing and potential customers, suppliers, collaborators in general, members of the Board of Directors, shareholders, employees, and visitors. It applies to all activities conducted in any department/section of our company involving the processing of information about natural persons. All employees and management staff are committed to i) protecting the privacy and personal data they process within the scope of their duties and ii) ensuring the confidentiality of personal data from the time they assume their duties and after the end of their employment. Also, they remain trained to comply with this Policy. We integrate data protection standards into our activities, technologies, and relationships with third parties using personal data, while designing relevant security controls for our processing activities and technologies that are consistent with data protection principles and applicable legislation.

2. Definitions

Data Protection Legislation: The General Data Protection Regulation (GDPR) EU 619/2016 (hereinafter referred to as the "*GDPR*") and the Greek Law No. 4624/2019 for the protection of individuals from the processing of personal data, as amended, as well as any secondary legislation / opinions / decisions / directions / guidelines issued by the Hellenic Data Protection Authority (hereinafter referred to as the "*Authority*") and any other competent Supervisory Authority for data protection.

Personal Data: Any information relating to an identified or identifiable natural person, including information that identifies the individual or can be used to identify, locate, track, or communicate with them. Specifically, personal data includes both direct identification information such as name, surname, or unique job title, as well as indirect identification information such as date of birth, mobile or landline phone number, and encoded data.

Special Categories of Data (also known as sensitive personal data): These pertain mainly to data related to religious, philosophical, political, or trade union views or activities, health, genetic or biometric information, racial or ethnic origin, and data relating to the sexual life or sexual orientation of an individual.

Processing: Any operation or set of operations performed on personal data, whether automated or non-automated, including, but not limited to, collection, recording, organizing, structuring, storage, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or any other form of making available, alignment or combination, restriction, erasure, or destruction of personal data.

Anonymization: The alteration, removal, deletion, or other restriction, or transformation of personal data, to make it impossible to use the data to identify, locate, or communicate with the data subject.

Data Subject: The natural person to whom personal data relates.

Data Controller: The legal entity that determines the purpose, means, content, and process of personal data processing.

Processor: The natural or legal person that processes personal data on behalf of the data controller.

Third Party: Any legal entity, organization, or subject that is not part of our company or for which our company does not have oversight or does not employ.

Transmission: The provision of access to personal data in any form.

Data Record: Any set of personal data structured in a way that allows identification of the relevant individual, e.g., any IT tool containing personal data.

Security Incident: Any accidental, unlawful, or unauthorized loss, destruction, alteration, access, use, disclosure, damage, or deterioration of personal data or any incident that may reasonably lead to accidental, unlawful, or unauthorized loss, destruction, alteration, access, use, disclosure, damage, or deterioration of personal data, or a reasonable suspicion that this has occurred.

3. Principles of Data Processing

When processing personal data, our company adheres to the following principles:

3.1 Lawfulness, Fairness, Transparency

We process personal data lawfully and fairly, based on the legal grounds outlined in the GDPR, which are explained below.

Before collecting and processing personal data, we inform data subjects through clear, distinct, and easily accessible data processing notices or similar means, about (i) the corporate entity/entities responsible for processing and the processor, (ii) the contact details of the Data Protection Officer, (iii) the types of personal data processed, (iv) the purposes of the processing, (v) categories of data recipients, including any requirements to disclose personal data to public authorities, (vi) the period of retention of data, (vii) the legal basis and purpose for processing the personal data, as applicable, (viii) details of any intended cross-border transfers, (ix) whether automated decision-making applies and the significance of processing for the data subject, (x) instructions regarding the data subject's rights.

When personal data is collected from sources other than directly from the data subject, we ensure in writing that the data provider has informed the data subject about how and why the data will be used by our company, and we seek to ensure that our partners comply with data protection laws and this Policy.

We ensure that necessary transparency mechanisms are incorporated into our supporting technologies, including mechanisms to support individual rights requests, where applicable. All individuals whose personal data we process will have the right to a copy of this Policy upon request to the Data Protection Officer or directly to us at the addresses provided below.

3.2 Purpose Limitation

Personal data is collected and processed for specified, explicit, and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes. The data collected or stored is necessary for fulfilling the purpose of its processing. We ensure that the principle of purpose limitation is embedded in our supporting technologies.

If new reasonable business purposes arise for personal data already collected, we ensure that either the new business purpose is compatible with the original purpose of processing, as described in the data processing notice, or we obtain the data subject's consent for the new use of their personal data.

3.3 Data Quality

We ensure that the personal data we process is accurate, complete, and up to date. We take reasonable steps to promptly delete or correct personal data that is inaccurate or incomplete, in relation to the processing purpose. Personal data is validated as accurate and current before collection, use, or any other processing. When changes occur to personal data by our company or third parties working for us, we ensure that these changes are communicated promptly, where possible, to the required recipients.

3.4 Data Minimization and Retention Limitation

We process only the necessary, relevant, and adequate data for specific processing purposes. Before processing personal data, we determine and record the specific lawful purpose for which it is necessary and the retention period of the related data. We do not collect, use, or share more personal data than needed, nor retain personal data in an identifiable form for longer than necessary for the specified business purposes. We anonymize data when necessary to retain information about the activity or process for a longer period.

3.5 Security, Integrity, Confidentiality, and Availability

We implement technical and organizational measures to ensure that personal data is processed in a way that guarantees an appropriate level of security, including protection against unauthorized or unlawful processing and accidental loss, destruction, or damage, using appropriate technical and organizational measures. Our operational security policies include, among others, business continuity and disaster recovery standards, identity and access management to necessary data according to the duties and responsibilities of each individual, security and information breach incident management, network access control, physical security, vulnerability and penetration testing, and risk management. For example, we implement security measures on workstations (username, password, antimalware, antivirus, screen lock policy), store paper documents with personal data in locked drawers/cabinets, have a Personal Data Protection Policy, a Data Subject Request Management Procedure, and a Secure Data Destruction Procedure. We also ensure that appropriate contracts for data protection are signed with partners, suppliers, and employees. New third-party suppliers or partners are evaluated regarding the level of data protection they provide. Personal data is encrypted, pseudonymized, and anonymized when necessary and feasible.

4. Training and Awareness

Every employee of the company is trained on data protection and security upon starting employment and periodically during their employment.

5. Data Transfers

We transfer personal data applying the appropriate technical and organizational measures, only when necessary for fulfilling our purposes and activities, based on a specific legal ground, and when required by law or judicial decision. Personal data is provided anonymously when deemed appropriate.
If the role of the entity receiving personal data is to process it on behalf of our company, before receiving the personal data, we (a) conduct a legal data protection audit to assess the data protection practices and risks related to these entities, (b) obtain contractual guarantees from these entities under Article 28 of the GDPR, ensuring they process personal data in accordance with our instructions, this Policy, and data protection laws, that they will promptly notify us of any security incident, including any inability to comply with this Policy and applicable legislation, and that they will cooperate in the timely resolution of any documented security incident.

If personal data needs to be transferred outside the EU, it will be done following specific legal safeguards under Articles 44-50 of the GDPR. We use the necessary measures to ensure that personal data is only transferred to a jurisdiction that provides an adequate level of protection for the data subject's rights and freedoms.

6. Rights of Data Subjects

Each data subject has the following rights under the conditions of the GDPR:

a) **Right to Information**: You have the right to receive clear, transparent, and understandable information about how we use your personal data and what your rights are. To this end, we provide this information in this Privacy Policy and encourage you to contact our Data Protection Officer (DPO) at the contact details provided below for any additional clarifications.

b) **Right of Access**: You have the right to access your personal data held by the company.

c) **Right to Rectification**: Data subjects have the right to correct inaccurate personal data. The rectification may include completing incomplete personal data, for example, by providing a supplementary statement of data from the data subject. When such a request is made, unless there is an exception, we will rectify the personal data without undue delay.

d) **Right to Erasure**: You have the right to request the deletion of your personal data.

e) **Right to Restriction of Processing**: You have the right to request the restriction of processing your personal data.

f) **Right to Data Portability**: In certain cases, data subjects have the right to obtain the personal data they have provided to us in a structured, commonly used, and machine-readable format, and to transfer it to another data

controller. When such a request is made, unless there is a legal exception, we will provide the personal data without undue delay.

g) **Right to Object**: Among other things, where personal data is processed for direct marketing purposes (e.g., promotional emails), data subjects have the right to object at any time to further processing of their personal data for such purposes. If a data subject raises such an objection, we will stop processing their personal data for these purposes.

h) **Rights Regarding Automated Individual Decision-Making and Profiling**: In certain cases, you have the right not to be subject to a decision based solely on automated processing, including profiling, which has legal or similarly significant effects on you. Specifically, you have the right to human intervention, to express your opinion, to receive an explanation about the decision that was made after an assessment, and to challenge that decision. Please note that our company does not use personal data to create "profiles" as defined under the GDPR.

i) **Right to Withdraw Consent**: If you have given your consent for the processing of your personal data, you have the right to withdraw your consent at any time by contacting us at the details provided in this document.

Any individual whose personal data we process under this Privacy Policy may exercise the above rights, ask questions, file complaints, or express concerns by contacting our Data Protection Officer using the methods provided below. Additionally, our employees and partners are obligated to inform the Data Protection Officer promptly about any requests, questions, complaints, or concerns related to the processing of data and the procedures applied by our company to protect such data.

In case you exercise any of the above rights, we will take every possible measure to address your request within a reasonable period, and at the latest within one (1) month from the identification of your request, informing you in writing about the satisfaction of your request or the reasons preventing the exercise of the relevant right. In certain cases, it may not be possible to fulfill your request, such as when complying with the right contradicts a legal obligation or conflicts with a contractual legal basis for processing your data.

If you believe that any of your rights have been violated, or that the company has failed to meet any legal obligation regarding the protection of personal data, you may file a complaint with the competent supervisory authority, which is the Hellenic Data Protection Authority (DPA), located at 1-3 Kifisias Avenue, 115 23, Athens, Greece, email: complaints@dpa.gr.

7. How Personal Data are Collected

We may collect personal data from various sources, specifically:

i. **Directly from Data Subjects** for one of the following reasons:

- Information provided during the establishment, development, and termination of our contractual relationship.

- Information provided during participation in the company's training seminars or at professional exhibitions and events.

- Information provided when you communicate with us or submit a request.

- Information provided when you subscribe to our newsletter.

ii. **Indirectly, from Other Sources**, based on our legitimate interest, in the following cases:

- Information obtained during a credit check of individuals or entities dealing with us, provided that the related legal process is followed.
- Information collected through closed-circuit television (CCTV) systems at the company's external premises for the protection of persons, goods, and property.
- Information collected and stored through cookies and tracking technologies when interacting with our websites or when the user's browser accesses our websites or other content displayed by the company or on its behalf on third-party websites. Please note that when you visit any of our company websites, we collect basic data related to your interaction with the website and the installation of cookies (see the detailed Cookies Policy posted on each website owned by our company). Third-party websites

generally apply their own privacy statements and terms of use, which we recommend you read before using these sites. The official websites owned by our company are currently:

- www.vitex.gr
- www.vitextherm.gr
- www.hermes-ins.gr
- www.trapezachromatos.gr

8. What personal data are collected?

Due to the nature of its activities, as previously mentioned, our company primarily collects the following personal data, categorized by type of subject:

Employees: Personal data related to their employment relationship with the company, including, but not limited to, identity and contact details, job position, evaluation records, financial information, health data about themselves or additional family members (as necessary for compliance with applicable labor and social security laws), and data related to work accidents or complaints (e.g., name, address, phone number, email, ID/passport copy, tax and social security details, work contracts, performance level, bank account details for payroll, medical certificates, and work suitability certificates, including maternity leave and working hours details).

Job Candidates: Personal data related to their evaluation as candidates and the recruitment process, including identity and contact details, as well as their professional resume data (e.g., CV details, name, address, phone, email, education, experience).

Board Members & Shareholders: Personal data and necessary documents for the execution of essential company operations (e.g., home address, phone, email, ID/passport, tax and social security details, tax statements, etc.).

Customers (current, past, potential): Personal data related to their current or potential contractual relationship with the company, credit assessments, debt management, complaint handling, or communication with the company (e.g., name, company address, phone, email, tax ID, transaction data, and bank account details for billing).

Suppliers (product/service suppliers, contractors, subcontractors, and other collaborators): Personal data related to the fulfillment of our cooperation and contractual relationship (e.g., name, company address, phone, email, tax ID, billing data, and bank account details).

Trainees: Personal data of individuals (employees, collaborators, or third parties) participating in company training programs (e.g., name, tax ID, social security number, date of birth, contact details, and evaluations).

Recipients of newsletters, promotional emails or messages (e.g., SMS, Viber), and other updates: Personal data of individuals who are interested in receiving information about the company's products and activities (e.g., name, contact details, professional activity type, and past transaction details).

Visitors to company premises: Personal data related to the identification and entry time of individuals entering the company premises, such as name, vehicle details, and reason for the visit. This information is recorded in the company's visitor logbook. Additionally, images of these individuals are captured through the legal operation of CCTV in external areas and entrances, for security purposes.

We emphasize that we do not collect special categories of personal data, except for limited health data as stated in this Policy.

Specifically, regarding children's personal data: Personal data of children may be collected in exceptional cases as part of the employment relationship with employees, solely for the purpose of complying with the company's obligations under applicable tax or social security legislation (e.g., birth certificates or family status certificates).

9. Purpose of processing personal data

The purpose of processing personal data varies depending on the type of relationship between the company and the data subjects. Specifically:

- **Employees' data**: Processed by the company's Human Resources Department and, where applicable, by the Accounting Department for the purpose of creating, executing, or terminating the employment contract and employee training. The company's occupational physician processes health data to manage employee medical records and to confirm their fitness for specific jobs. Employee data is also processed for handling workplace accidents, reports, and complaints.
- **Candidates' data**: Provided during the stages of selection and evaluation, this data is communicated to the company's Human Resources Department and Management for the purpose of recruitment and contract signing.
- **Customers, suppliers, contractors and other partners' data**: Provided to the Commercial and Financial Departments for the purpose of managing sales, executing contracts, ensuring legal compliance, and communication with clients, suppliers, and other partners.
- **Visitors' data**: For the purpose of managing entry to the company's premises, including security reasons and compliance with legal obligations.

10. Legal bases for data processing

The collection and processing of personal data are based on the following legal grounds:

- **Article 6(1)(b) GDPR**: Processing necessary for the performance of a contract to which the data subject is a party, or for the taking of steps at the request of the data subject prior to entering into a contract.
- **Article 6(1)(c) GDPR**: Processing necessary for compliance with a legal obligation to which the company is subject.
- **Article 9(2)(b) GDPR**: Processing necessary for the performance of obligations and the exercise of specific rights under labor law and social security law.
- **Article 9(2)(h) GDPR**: Processing necessary for preventive or occupational medicine, to comply with legislation protecting health and safety at the workplace.
- **Article 6(1)(f) GDPR**: Processing necessary for the purposes of the legitimate interests pursued by the company, such as ensuring the security of company premises through CCTV.
- **Article 6(1)(a) GDPR**: Consent of the data subject, as per Article 7 of the GDPR, is obtained for certain purposes like sending newsletters or participating in promotional campaigns.
- **Article 9(2)(f) GDPR**: Processing necessary for the establishment, exercise, or defense of legal claims.
- **Article 9(2)(g) GDPR**: Processing necessary for reasons of public interest in the area of public health, such as protection against serious cross-border health threats.

11. To whom personal data may be disclosed

The data are accessible to the authorized persons mentioned in paragraph 9 above, as well as to any other authorized person who needs to process the data of the data subjects as part of their work duties.

In principle, the company does not disclose personal data to third parties. However, for the purposes mentioned above, personal data may be further transferred (even to third countries) and specifically to: Authorities, public bodies, social security organizations (e.g. KEPEK, EFKA, Police, Ministry of Labor) as well as financial and credit institutions. Also, to third-party partners providing specific supply chain services to the company, such as external consultants and partners, providers of management, sales promotion, and customer and supplier relationship services, tax and social security consultants, insurance service providers, educational service providers, providers of CV management services, and the company's security services provider. Furthermore, data may be disclosed to representatives, distributors, business partners, suppliers of the company, third parties, and their consultants in cases of extraordinary operations (mergers and acquisitions, business/unit transfers, etc.), legal recipients of announcements as required by laws or regulations, such as family members and other relatives of employees, the occupational doctor and/or certain other doctors. Additionally, in cases where technical support is required for the company's electronic and information systems, an external partner

who provides technical support and IT services to the company may have access to the data of the data-subjects.

In each case, the above individuals/legal entities will act as data controllers, processors, or persons authorized to process personal data, for the same purposes mentioned above and in accordance with applicable law. We emphasize that, in these cases, our partners have access only to the personal data necessary for fulfilling their contractual obligations and are prohibited from using the data for any other purpose. Additionally, they have previously committed contractually to process personal data in compliance with the GDPR.

12. Retention period of your personal data

Personal data are retained for the period necessary to fulfill the company's purposes, comply with legal obligations, and establish, exercise, and support legal claims and rights in case of disputes. After the required retention period has passed, personal data are deleted by the company. Specifically and indicatively:

- **Employee data** are retained for the duration of the employment relationship and up to twenty (20) years after the termination/cessation of the employment relationship, during which time any legal matter involving the employee, such as a tax audit, civil rights claims, or criminal investigations, may arise.
- **Candidate data** are retained for six (6) months after the completion of the selection/recruitment process.
- **Customer, supplier, and other partner data** are retained as long as the contractual relationship lasts. After the termination of the relationship, for any reason, the data is retained for a maximum of twenty (20) years (indicative period for the limitation of any related legal claims), during which time any legal or tax-related matter may arise, such as judicial proceedings or tax audits.
- **Personal data related to promotional campaigns** aimed at individuals without a contractual relationship with the company are retained for ten (10) years.
- **Video surveillance data** collected from the company's surveillance system, including at external building facilities, the entrance, and the entrance gatehouse, are retained for fifteen (15) days, after which they are automatically deleted. If an incident is identified within this period, the video is isolated and retained for up to one (1) additional month for investigation purposes and the initiation of legal proceedings to protect our legitimate interests. If the incident involves a third party, the video will be retained for up to three (3) additional months. After the specified period, the company may retain the data for a longer period only in exceptional cases where the incident requires further investigation or if requested by the competent authorities.

13. Data Controller Information

You can contact our company as the Data Controller using the following details:

Company Name: VITEX A.E.
Address: Imeros Topos, P. O. Box 139, P.C. 19300, Aspropirgos, Attica
Telephone-Fax: 00302105589400 – 0030215597859
E-mail: info@vitex.gr

14. Data Protection Officer (DPO) Information

The company has appointed a Data Protection Officer to monitor compliance with the provisions of this Personal Data Protection Policy and the company's adherence to the GDPR and other relevant legislation. Data subjects may contact the Data Protection Officer regarding matters related to this Policy and other personal data protection issues using the following contact details:

Company Name: "ADVANCED QUALITY SERVICES A.E."
Address: 1A Tirnavou & Sarantaporou str. Agios Stefanos, Attica, P.C. 14565
Telephone-Fax: 00302106216997
E-mail: dpo@vitex.gr

15. Updates - Revision of this Personal Data Protection Policy Statement

Any changes and updates to this Policy will include a revision date and will be published on the official websites of our company.

Aspropyrgos, February 25th , 2025
For VITEX A.E.

Armodios Yannidis
C.E.O.