

StellarBlue P.C.

Privacy Policy

Version 1.0 — March 2026

1. Who We Are

StellarBlue P.C. (“StellarBlue”, “we”, “us”, “our”) is a software company incorporated in Greece, with registered address at Adrianoupoleos 14, 55133 – Kalamaria, Greece (VAT: EL802309756). We develop and operate the ATLAS ETRM platform, an Energy Trading and Risk Management (ETRM) system delivered as a Software-as-a-Service (SaaS) to energy companies in Greece, Cyprus, Belgium, and other European markets.

This Privacy Policy explains how StellarBlue processes personal data when you interact with us — whether as a user of the ATLAS ETRM platform, a representative of a client organisation, or a person who contacts us directly. We are committed to processing personal data lawfully, transparently, and in accordance with Regulation (EU) 2016/679 (“GDPR”) and applicable Greek data protection legislation.

For any questions regarding this policy or the exercise of your data protection rights, please contact us at: contact@stellarblue.eu

2. Data We Collect and Why

2.1 ATLAS ETRM Platform Users

When your employer or organisation subscribes to ATLAS ETRM and creates a user account for you, we process the following personal data in our capacity as data processor on behalf of your organisation:

- Full name and work email address — to identify you as an authorised user.
- Username and hashed password credential — where Single Sign-On (SSO) via Microsoft Azure Active Directory is not configured; raw passwords are never stored.
- Role and permission assignments — to enforce role-based access control (RBAC) across the platform’s modules.
- System audit log entries — recording your actions within the platform (deal creation, order submissions, configuration changes) with timestamp and session IP address, for traceability and regulatory compliance purposes.
- Email address for system notifications — used to deliver automated alerts triggered by platform events relevant to your assigned role.

The legal basis for this processing is the performance of the contract between StellarBlue and your organisation (Article 6(1)(b) GDPR), and our legitimate interest in maintaining secure, auditable access to the platform (Article 6(1)(f) GDPR). Your organisation, as the data controller, determines the purposes for which your data is used within the platform. StellarBlue processes this data only on your organisation’s instructions.

2.2 Back Office Contact Persons

Client organisations may enter the names and contact details of their counterparties, trading partners, and other business contacts into the ATLAS ETRM Back Office module. StellarBlue stores this data as a data processor on behalf of the client. The data collected may include name, work email, telephone number, role, and associated organisation. If you are a contact person whose details have been entered into the platform by one of our clients, you should direct any privacy queries to that client organisation directly, as they are the data controller for that data.

2.3 Client Representatives and Contract Counterparties

When your organisation enters into a commercial relationship with StellarBlue, we process personal data relating to you as our client contact in our capacity as data controller. This includes your name, work email address, telephone number, and contractual correspondence. We process this data on the basis of contract performance (Article 6(1)(b) GDPR) and compliance with legal obligations including Greek accounting and tax law (Article 6(1)(c) GDPR).

2.4 Enquiries and Pre-Sales Contact

If you contact us via email or other channels with an enquiry, we process your name, organisation, email address, telephone number (if provided), and the content of your message. We do this on the basis of pre-contractual steps or our legitimate interest in responding to business enquiries (Article 6(1)(b) and (f) GDPR).

3. Data We Do Not Collect

StellarBlue does not collect or process special categories of personal data (Article 9 GDPR), including health data, biometric data, genetic data, data concerning racial or ethnic origin, political opinions, religious beliefs, or sexual orientation. ATLAS ETRM is an energy trading platform; its data model is focused on market positions, financial instruments, and energy assets, not on individuals' personal characteristics.

We do not use personal data for automated decision-making or profiling that produces legal or similarly significant effects on individuals.

4. How We Protect Your Data

StellarBlue implements technical and organisational measures appropriate to the risks of the processing, including:

- Encryption in transit: all communications between users and the ATLAS ETRM platform are encrypted using TLS 1.2 or higher. HTTP connections are automatically redirected to HTTPS. Internal service communications are confined to private network segments.
- Encryption at rest: personal data stored in the platform database and backup repositories is encrypted at rest using AES-256 via Azure-managed encryption.
- Access control: access to personal data within the platform is enforced on a least-privilege, role-based basis using OAuth 2.0 / JWT authentication via Microsoft Entra ID. Unauthenticated API requests are rejected at the network gateway. The platform supports over 112 granular permission settings across modules.
- Network isolation: the production database is non-internet-facing and accessible only through private Azure Virtual Network (VNet) segments. Azure Private Endpoints are used for all database and storage services, ensuring data traffic never traverses the public internet.
- Secret management: credentials, API keys, and certificates are stored exclusively in Azure Key Vault and retrieved at runtime via managed identity; no secrets are hardcoded in configuration files or container images.
- Continuous security monitoring: the platform is monitored continuously via Azure Defender for Cloud. All application components are maintained on Long-Term Support (LTS) releases and patched promptly upon availability of security updates.
- Backups: daily automated database backups and weekly VM snapshots are retained in Azure Blob Storage with Geo-Redundant Storage (GRS). Backups are retained for a minimum of 30 days.

5. Sub-Processors and Third-Party Recipients

StellarBlue uses Microsoft Ireland Operations Limited (“Microsoft Azure”) as its sole cloud infrastructure sub-processor. Microsoft Azure provides hosting, storage, key management, and security monitoring services. Microsoft processes data in EU data centres (West Europe and North Europe regions) under its Data Processing Agreement and EU Standard Contractual Clauses.

We do not sell, rent, or share personal data with third parties for marketing, analytics, or any commercial purpose. Personal data may be disclosed to our accountants or legal advisors where strictly necessary and subject to professional confidentiality obligations.

6. International Transfers

Personal data processed through ATLAS ETRM and in connection with our business relationships is stored and processed exclusively within the European Economic Area (EEA), specifically within Microsoft Azure’s EU data centre regions. We do not transfer personal data to countries outside the EEA. Should this change, we will ensure an appropriate transfer mechanism (such as EU Standard Contractual Clauses or an adequacy decision) is in place before any transfer occurs.

7. Retention Periods

We retain personal data only for as long as necessary for the purpose for which it was collected, and in accordance with applicable legal obligations:

Data Category	Retention Period	Basis
Platform user accounts	Duration of client subscription + 30 days post-termination	Contract performance
Audit log entries	12 months active / 36 months archived [to confirm]	Regulatory / contractual
Notification records	90 days	Operational necessity
Client contract and invoice records	10 years from contract expiry	Greek accounting law (Law 4308/2014)
Client representative contact data	Duration of commercial relationship + 2 years	Legitimate interest
Pre-sales enquiry data	24 months from last contact	Legitimate interest

8. Your Rights

You have the following rights under GDPR with respect to personal data that StellarBlue processes as data controller (primarily client representatives and enquiry contacts). Where StellarBlue acts as data processor, you should exercise your rights through the client organisation that controls your data, and we will assist that organisation in responding.

- Right of access (Article 15): you may request confirmation of whether we hold personal data about you and a copy of that data.
- Right to rectification (Article 16): you may request correction of inaccurate personal data.
- Right to erasure (Article 17): you may request deletion of your personal data where there is no lawful basis for continued processing.
- Right to restriction of processing (Article 18): you may request that we limit processing of your data in certain circumstances.

- Right to data portability (Article 20): where processing is based on consent or contract and carried out by automated means, you may request your data in a structured, machine-readable format.
- Right to object (Article 21): you may object to processing based on legitimate interests.
- Right to lodge a complaint: you have the right to lodge a complaint with the Hellenic Data Protection Authority (HDDPA) at www.dpa.gr, or with the supervisory authority of your country of residence.

To exercise any of these rights, please contact us at contact@stellarblue.eu. We will respond within one calendar month of receipt of your request. We may ask for proof of identity before processing a request.

9. Cookies and Website

StellarBlue's primary product interface (ATLAS ETRM) is a browser-based SaaS application delivered to client organisations. It uses session cookies and authentication tokens strictly necessary for login and session management. No third-party advertising, tracking, or analytics cookies are deployed within the platform.

If StellarBlue operates a public website (stellarblue.eu), a separate cookie notice will be published on that site in accordance with the ePrivacy Directive and applicable Greek law.

10. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our processing activities, applicable law, or best practice. Material changes will be notified to client organisations via email. The current version is always available upon request from contact@stellarblue.eu. The version date at the top of this document indicates when it was last revised.

11. Contact

For any questions, requests, or concerns regarding this Privacy Policy or our data protection practices, please contact:

Organisation:	StellarBlue P.C.
Address:	Adrianoupoleos 14, 55133 – Kalamaria, Greece
Email:	contact@stellarblue.eu
Privacy contact:	George Tsoumalis

This document is the Privacy Policy of StellarBlue P.C. and is effective as of March 2026.