Cost Control Privacy Policy — Web and Mobile Application

Version: 1.1

Last updated: 30 July 2026

1. Summary

Cost Control is an application for managing users, projects, contracts, business parties, invoices, costs, payments, and financial analytics. The service is available through a web interface and an iOS/Android mobile application.

This Policy explains which personal data is processed through Cost Control, why it is processed, how long it is retained, who may receive it, and which rights you have under Regulation (EU) 2016/679 (the “GDPR”) and applicable Romanian law.

Cost Control is intended for professional use by organisations. It is not intended for children or for personal consumer use.

2. Who is the data controller?

2.1 Data entered by your organisation

If your Cost Control account was provided by your employer, client, or another organisation (the “Organisation”), the Organisation is the controller of data relating to its users, contact persons, suppliers, customers, and other individuals whose data is entered into the application. The Organisation determines the purposes and means of processing, user access, retention periods, and instance configuration.

Cost Control uses a customer-controlled infrastructure model. The backend, database, and web interface run on a server, virtual machine, or cloud account selected, owned or leased, and administered by the Organisation. Operational data remains under the Organisation's administrative control and is not automatically transferred to Aegis Core Tech merely because the Organisation uses the software.

Requests concerning data entered into Cost Control should first be submitted to the Organisation that provided your account. Its identity and contact details are available in your account invitation or documents, your employer's/client's privacy notice, or from the administrator of your Cost Control instance. This product Policy supplements, but does not replace, the Organisation's own privacy notice as controller.

The Organisation's platform administrator manages user accounts, including creation, disablement, and deletion. The administrator or the Organisation's privacy contact is also the contact point for access, correction, and deletion requests concerning the Organisation's instance.

2.2 The role of Aegis Core Tech SRL

The application provider is:

Aegis Core Tech SRL
Romanian tax ID: RO52060129 • Trade Register number: J2025046995006
Calea Dorobanți 33A, 010553 Bucharest, Romania
Email: contact@aegiscoretech.com
Telephone: +40 741 131 505
Website: https://aegiscoretech.com

Aegis Core Tech supplies and licenses the software but does not host the production database and does not have standing or routine access to operational data in the customer's instance. Merely supplying the licence, updates, or documentation without access to personal data does not make Aegis Core Tech a processor of that data.

The roles are as follows:

- the Organisation is the controller of operational data processed in its Cost Control instance;
- Aegis Core Tech is a separate controller for its own data strictly required for contracting, licensing, invoicing, securing the commercial relationship, and administering support requests;
- if the Organisation requests support or maintenance that requires access to the instance or personal data, Aegis Core Tech will act as a processor for that access, solely on the Organisation's documented instructions and under an agreement compliant with Article 28 GDPR. Access must be authorised, time-limited, logged, and revoked after the intervention;
- external providers enabled or contracted by the Organisation, such as its cloud provider, Microsoft, Google/Firebase, OpenAI, or its email provider, may receive data according to the selected configuration. These disclosures are described in Sections 7 and 8 and do not constitute routine hosting of the production database by Aegis Core Tech.

The Organisation's control of the infrastructure does not limit Aegis Core Tech's obligations concerning product security and data protection by design. The Organisation provides users with its identity and contact details through the application, account invitation, contract, or its own privacy notice.

3. Personal data we process

Depending on the functions used and the configuration selected by the Organisation, the following categories may be processed.

3.1 Account, authentication, and authorisation data

- internal user ID, username, first and last name if configured by the backend, and professional email address;
- roles, permissions, project membership, and account status;
- cryptographically protected credentials; plaintext passwords must not be retained;
- session tokens, login and logout dates/times, and authentication events;
- for Microsoft Entra ID authentication: account identifiers and attributes supplied by Microsoft according to the tenant configuration, such as name, email address, and account ID;
- an account-disablement reason entered by an administrator.

3.2 Professional, contractual, and financial data

- project information and project membership;

- business-party names and tax identifiers; these constitute personal data where they identify an individual, sole trader, or representative;
- contact persons' names, email addresses, and telephone numbers;
- contract number, duration, value, payment terms, warranties, notes, and associated document or URL;
- invoices and invoice lines, including number, date, due date, description, amounts, business party, status, and history;
- payment amounts, dates, method, transaction reference, and description;
- costs, categories, project allocations, income, expenses, and financial indicators or forecasts;
- creation and modification timestamps and, where configured by the backend, the identity of the user who performed an operation.

The Organisation must avoid entering data that is not necessary for its professional purposes. It must also provide the information required by Article 14 GDPR to contact persons and others whose data is obtained indirectly, unless a statutory exception applies.

3.3 AI assistant and voice messages

The AI function is inactive unless the Organisation's administrator configures it and supplies the required provider credentials. Where enabled, the function may process:

- questions, message text, a conversation identifier, and generated responses through OpenAI's chat service;
- audio recorded at the user's request and sent to OpenAI's transcription service;
- text supplied to OpenAI's text-to-speech service to generate an audio response;
- information retrieved by authorised tools from the Organisation's Cost Control database where necessary to answer the user's request, subject to the user's existing roles and permissions;
- filtered search keywords sent to Tavily when the assistant needs a current web search, together with technical request metadata processed by the provider.

The application is designed to remove confidential information from Tavily search terms before submission. A search term may nevertheless constitute personal data if it concerns or identifies an individual. Users must not ask the assistant to disclose secrets, special-category data, passwords, or other information that is not necessary for the requested task.

Microphone recording starts only following a user action and after permission has been granted through the operating system. Permission may be withdrawn in the device settings.

Cost Control does not persist AI conversations as conversation history in its backend. Messages are held in the mobile application's memory only while the chat is active and are discarded when the chat is closed or left. The backend processes prompts, relevant tool results, audio, transcripts, and responses transiently to complete the request. OpenAI and Tavily process data under the account, API configuration, contract, and data controls selected by the Organisation, as described further in Sections 7–9.

3.4 Mobile application and push notifications

- Firebase Cloud Messaging (“FCM”) token and Firebase Installation ID;
- platform (Android/iOS), application version, Firebase/device metadata, Android operating-system build identifier (`Build.ID`), or Identifier for Vendor (“IDFV”) on iOS;

- notification title, technical content, and internal route (“deep link”);
- locally on the device: authentication token, user profile, selected language, saved backend URLs, and the measurement-unit cache;
- temporarily, an audio file created to send a voice message.

Notifications are optional at operating-system level. Refusing them must not prevent the use of the application's core functions. We avoid including sensitive personal or financial data in content displayed on a locked screen.

3.5 Technical and security data

The server and infrastructure may process an IP address, request date and time, URL or endpoint, device type, browser and operating system, response code, session identifiers, security events, and technical errors. These data are used for operation, diagnostics, abuse prevention, and security.

The Organisation administering the infrastructure determines log content and retention subject to data minimisation and storage limitation. The Organisation must separately inform you if it enables an external monitoring or crash-reporting service.

4. Sources of personal data

Personal data may come:

- directly from the user;
- from the Organisation and its administrators;
- from other authorised users who enter contact or commercial-document data;
- from Microsoft when Entra ID authentication is used;
- from the device, operating system, and Firebase for notifications;
- from OpenAI when the AI assistant returns text, transcripts, or generated speech;
- from Tavily and public web sources when the AI assistant performs a web search;
- from financial or accounting systems imported or integrated by the Organisation. The Organisation is responsible for informing individuals about the integrations it enables.

Where data is not obtained directly from the individual, the controller must provide the information required by Article 14 GDPR unless a statutory exception applies.

5. Purposes and legal bases

Purpose	Main data categories	Usual legal basis
Creating and administering accounts, authentication, roles, and sessions	account, profile, roles, tokens	Article 6(1)(b) GDPR for a contract with an individual user where applicable; normally Article 6(1)(f) for operation of the B2B service and security; for employees, the legal basis is determined by the employer
Managing projects, contracts, invoices, costs, and payments	professional and financial/accounting data	Article 6(1)(b), (c), and/or (f) GDPR, depending on the relationship with the individual and applicable accounting or tax obligations
Accounting records and responding to public authorities	supporting documents and financial transactions	Article 6(1)(c) GDPR, including Romanian Accounting Law No. 82/1991 and applicable tax legislation
Security, fraud prevention, auditing, and legal claims	logs, IP address, events, timestamps	Article 6(1)(f) GDPR; Article 6(1)(c) where a statutory obligation applies
Microsoft Entra ID authentication	account identifiers and attributes	Article 6(1)(b) or (f) GDPR, depending on the relationship and Organisation configuration
Text/voice AI assistant and AI web search	prompts, authorised database results, audio, transcripts, responses, and filtered search terms	Article 6(1)(b) or (f) for the requested function; microphone access and the required prominent disclosure are separately controlled in the mobile flow. Consent will be relied upon as the GDPR legal basis only where the implemented flow allows consent to be freely given and withdrawn without unjustified consequences
Push notifications	FCM token, device ID, platform, version	Article 6(1)(f) or (b) for requested operational communications; operating-system permission is separate. Any future promotional communications require a separate legal basis and opt-out mechanism
Technical support	contact data, request content, supplied logs	Article 6(1)(b) and/or (f) GDPR

Legitimate interests are relied upon only after assessing necessity and balancing those interests against the individual's rights. You may request information about the legitimate-interest assessment and object under Article 21 GDPR.

We do not make core functions conditional on consent to unnecessary processing. Where processing is based on consent, it may be withdrawn at any time without affecting the lawfulness of earlier processing.

6. Special-category data and national identifiers

Cost Control is not designed to request health data, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data about sex life or sexual orientation, or genetic or biometric data used for identification. Voice is processed as an audio recording, not for biometric identification.

Do not include such information in free-text fields, documents, or AI conversations. If the Organisation decides that it is strictly necessary, it must identify a condition under Article 9 GDPR, document necessity, and implement additional safeguards.

Romanian personal identification numbers, identity-document series and numbers, and other national identifiers must not be entered unless they are necessary and a legal basis under Article 6 GDPR exists. Where legitimate interests are relied upon, the special safeguards in Article 4 of Romanian Law No.

190/2018 apply: data minimisation, security and confidentiality, retention and deletion periods, and periodic staff training.

7. Recipients of personal data

Access is limited to authorised users of the Organisation according to their roles and permissions, and to personnel or providers with a legitimate need for access.

Depending on the configuration, recipients or processors may include:

Provider/category	Role and data	Notes
Infrastructure controlled by the Organisation and, where applicable, its contracted cloud provider	database, API, and web hosting	The Organisation owns, leases, or administers the environment and informs users of the applicable provider and country/region
Google Firebase Cloud Messaging	notification delivery; FCM token, technical identifiers, message/device metadata	Active in the mobile application; Google's/Firebase's privacy terms apply to the service it supplies
Microsoft Entra ID	optional authentication; account identifiers and attributes	Only where the Organisation enables Microsoft sign-in
OpenAI	chat responses, voice transcription, and text-to-speech; prompts, relevant data returned by authorised Cost Control tools, audio, transcripts, and responses	Only where the Organisation enables AI and manages the OpenAI API key, contract, project, data controls, and available processing region. OpenAI states that API data is not used to train its models by default unless the customer opts in. Its API data controls and privacy policy apply
Tavily	current web search for the AI assistant; filtered search keywords and technical request metadata	Only where the Organisation enables the AI web-search tool and manages the Tavily API key and contract. Cost Control is designed to exclude confidential information from search terms before transmission. Tavily's privacy policy and the applicable commercial terms govern its processing
Email provider selected by the Organisation	system messages and password resets; Aegis may use its own provider for support responses submitted directly to Aegis	The specific provider depends on the Organisation's configuration
Advisers, auditors, authorities, and courts	compliance, auditing, legal claims, and statutory obligations	only where there is a need and legal basis

We do not sell personal data. We do not use the Organisation's operational data for behavioural advertising.

The controller must maintain an up-to-date list of processors and subprocessors and, where applicable, notify the Organisation about changes in accordance with the Article 28 agreement.

8. International transfers

The main instance is hosted on infrastructure selected and controlled by the Organisation. The Organisation informs users of the hosting country/region and is responsible for ensuring that its selection complies with the GDPR. Information applicable to your deployment is available from its administrator. Use of Microsoft, Google/Firebase, OpenAI, Tavily, or other providers may involve access to or transfers of personal data outside the European Economic Area.

The location of the Organisation or creation of a provider account from the European Union does not by itself guarantee that all API processing occurs in the EU. The actual processing region depends on the provider's service availability, API endpoint, account/project configuration, and contract selected by the

Organisation. The administrator must document these settings before enabling the provider.

Such a transfer will take place only under a mechanism permitted by Chapter V GDPR, such as:

- a European Commission adequacy decision, including the EU–US Data Privacy Framework for certified entities and covered data categories;
- the European Commission's Standard Contractual Clauses, together with a transfer impact assessment and supplementary measures where necessary;
- another applicable statutory safeguard or derogation.

You may request information about the mechanism used and a copy of the safeguards, subject to the removal of confidential information.

9. Data retention

The controller must establish a documented retention policy. Unless longer retention is required, data is deleted or anonymised when no longer necessary.

Category	Retention period or criterion
Account and profile	until an administrator deletes the account and for any additional period required for statutory obligations or legal claims. Cost Control does not automatically delete an account after inactivity
Device session token	until logout, revocation, expiry, or deletion of the application/local data
FCM token and device identifiers	the current device registration is removed on logout, and server-side registrations are deleted when the account is deleted or an administrator removes them. There is currently no automatic expiry process for other inactive or invalid FCM tokens, so they may remain until account deletion or manual administrative cleanup
Temporary device audio recording	stored in the operating system's temporary application directory while it is recorded and transmitted. It is not added to Cost Control conversation history. A temporary file may remain until it is overwritten by a later recording, cleared by the operating system, or removed with the application's local data
AI conversation in Cost Control	held in mobile application memory only while the chat is active and discarded when the chat is closed or left; the Cost Control backend does not save conversation history
Data processed through OpenAI	governed by the API endpoint and controls selected by the Organisation. Under OpenAI's standard API controls, customer content may be included in abuse-monitoring logs retained for up to 30 days, unless a different approved control or legal requirement applies. Some endpoints have separate application-state periods; the administrator must document the endpoints and controls it enables
Tavily web-search queries	governed by the Organisation's Tavily contract and configuration. Tavily's general privacy policy states that query data is retained as needed for the service and that portions may be used to improve responses unless the customer contract specifies otherwise. The Organisation must verify the retention terms applicable to its plan
Technical and security logs	for the period necessary for operation, security, and incident investigation; logs associated with an investigation may be retained until it and any related legal proceedings are completed
Financial/accounting documents covered by Romanian Law No. 82/1991	five years calculated from 1 July of the year following the end of the financial year in which they were created, under Articles 23 and 25, unless a longer special period applies
Contracts and evidence needed for legal claims	for the contract term and applicable limitation periods; the general Romanian limitation period is normally three years under Article 2517 of the Civil Code, although special periods may apply

Category	Retention period or criterion
Backups	until the end of the rotation cycle configured for the specific customer deployment. The exact cycle is available by email from the Organisation's administrator or privacy contact. Deleted data is not restored to the active system unless restoration is required for continuity or statutory obligations

Deletion from the active system may not immediately remove data from isolated backups. Backups must expire through rotation and must not be reused for unrelated purposes.

10. Cookies, web storage, and mobile storage

10.1 Web interface

Cookies or similar technologies that are strictly necessary for authentication, security, load balancing, or remembering requested preferences may be used without consent only within the limits of the applicable statutory exception. Any optional analytics, personalisation, or marketing cookie or identifier must be blocked until informed, specific, and withdrawable consent is obtained, in accordance with Article 5(3) of Directive 2002/58/EC and Article 4(5) of Romanian Law No. 506/2004.

The Organisation administering the instance is responsible for maintaining an inventory of cookies and similar technologies in its environment. If the Organisation adds optional analytics, personalisation, or marketing technologies, it must offer equally accessible “Accept”, “Reject”, and granular settings before activation and publish each technology's name, provider, purpose, and duration.

10.2 Mobile application

The application locally stores the data described in Section 3.4 for session, configuration, and functional purposes. Notification and microphone permissions are managed through iOS or Android. Deleting the application will normally remove its local data, but it will not automatically delete server-side data; the account-deletion procedure in Section 13.1 must be used for server-side data.

11. Security

We implement or require risk-appropriate measures such as:

- role- and permission-based access control and least privilege;
- authentication, session expiry/revocation, and account disablement;
- TLS encryption for communications in production;
- protection of credentials and secrets, security logging, and monitoring;
- backups, tested restoration, updates, and vulnerability management;
- confidentiality commitments, staff training, and Article 28 agreements;
- incident response processes and periodic assessments.

No system can guarantee absolute security. Where a personal-data breach is likely to result in a risk, the controller will notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it (Article 33 GDPR). Affected individuals will be informed where a high risk is likely (Article 34 GDPR).

The mobile application connects to the backend address configured for the relevant deployment. The Organisation must provide and configure an HTTPS/TLS endpoint for production. An unencrypted HTTP

endpoint must be used only in an isolated development environment because data sent to such an endpoint would not be protected in transit.

12. AI, forecasts, and automated decision-making

Cost Control may generate AI responses and financial forecasts or indicators. Results may be inaccurate and must be checked by a competent person. The system is not intended to make decisions without human involvement that produce legal effects or similarly significantly affect an individual.

If the Organisation later configures such a use, it must first conduct a legal assessment and, where required, a data protection impact assessment (DPIA). It must provide information about the logic involved and likely consequences and ensure the rights to human intervention, to express a point of view, and to contest a decision, in accordance with Articles 22 and 35 GDPR.

13. Your rights

Subject to the conditions of the GDPR, you have the right:

- to be informed (Articles 12–14);
- to access your data and receive a copy (Article 15);
- to rectify inaccurate data (Article 16);
- to erasure where the statutory conditions are met (Article 17);
- to restriction of processing (Article 18);
- to data portability for data you provided, where applicable (Article 20);
- to object to processing based on legitimate interests (Article 21);
- not to be subject to a solely automated decision under the conditions of Article 22;
- to withdraw consent where consent is the legal basis, without affecting earlier processing (Article 7(3));
- to lodge a complaint and seek a judicial remedy.

Submit your request to the controller identified in Section 2. Where Aegis Core Tech acts only as a processor, it will forward the request to the Organisation or assist the Organisation in responding. We may request reasonable information to verify identity without collecting excessive data.

The controller will respond without undue delay and normally within one month. This period may be extended by a further two months for complex or numerous requests, provided that the individual is informed within the first month. Requests are normally free of charge, subject to the exceptions in Article 12(5) GDPR.

Erasure may be refused or limited where retention is necessary to comply with an accounting, tax, or other statutory obligation, or for the establishment, exercise, or defence of legal claims. In that situation, data will be restricted to permitted purposes.

13.1 Account-deletion procedure

Cost Control accounts are created and managed by the Organisation's platform administrator; the application does not provide self-service account deletion. To request deletion, email the administrator or the Organisation's privacy contact using the address provided in the account invitation, contract, the Organisation's privacy notice, or the contact information displayed for the relevant Cost Control deployment. The Organisation must make that exact contact channel readily available to its users.

The Organisation verifies the requester's identity and decides the request as controller. It will respond without undue delay and normally within one month. Where deletion is approved, the administrator will delete the active user profile without undue delay and normally within 30 days after verification, unless a statutory exception applies.

Deletion of the account includes the user's profile and settings, name, email address, authentication and login information, roles and permissions, and server-side push-notification device registrations and FCM tokens associated with that account. Sessions must be revoked. References in audit trails may be anonymised or retained where necessary for security, accountability, statutory obligations, or legal claims.

Deleting an account does not automatically delete invoices, contracts, payments, project records, or other business records belonging to the Organisation or concerning other individuals. Personal identifiers in those records must be deleted, anonymised, restricted, or retained by the Organisation according to its legal basis and retention obligations. Residual copies in isolated backups expire under the deployment-specific rotation cycle described in Section 9.

There is no automatic account-deletion mechanism based solely on a period of inactivity.

14. Complaints to a supervisory authority

We encourage you to contact the controller first. You may also lodge a complaint with the supervisory authority in the Member State where you live or work or where you believe an infringement occurred.

In Romania:

National Supervisory Authority for Personal Data Processing (ANSPDCP)
B-dul G-ral Gheorghe Magheru no. 28–30, Sector 1, 010336 Bucharest, Romania
Website: https://www.dataprotection.ro/
Complaints page: https://www.dataprotection.ro/?page=Plangeri_pagina_principala

15. Mandatory data and consequences of not providing it

Fields marked as mandatory are required for the relevant account or selected commercial operation. If you do not provide authentication data, we cannot create a session. If you do not provide the mandatory fields for an invoice, payment, contract, or configuration, that function cannot be completed. Microphone access, notifications, and Microsoft authentication are optional where alternative methods remain available.

16. Children

Cost Control is a B2B service intended for individuals authorised by an organisation. It is not offered directly to children, and we do not knowingly seek to collect children's personal data. If you become aware that such data has been entered without a valid legal basis, contact the controller.

17. Changes to this Policy

We may update this Policy to reflect legal, technical, or operational changes. The current version, date, and a summary of changes will be made available in the application and/or on the public page. For material changes, users will be notified through an appropriate channel before the changes take effect where required by law.

18. Contact

For data controlled by the Organisation, contact the administrator of your Cost Control instance or use the details in your account invitation, contract, or the Organisation's privacy notice.

For Aegis Core Tech's own processing or questions about the provider:

- Email: contact@aegiscoretech.com
- Address: Calea Dorobanți 33A, 010553 Bucharest, Romania
- Telephone: +40 741 131 505