Privacy Policy

English Version (Primary for Stores / USA) · Version 2026-10-15-r2

Part I. Controller, scope and data we process

1. Controller

The controller of your personal data is Affinity Intelligence sp. z o.o., Al. Krakowska 61A, 05-090 Sękocin Nowy, Poland, KRS 0001091878, NIP 5342676045, (the "Controller", "we"). In all matters concerning personal data, including the exercise of your rights, you may contact us at kontakt@affinity-intelligence.com or by post at the address above.

2. Scope

This Policy applies to the BridgeCoach mobile application, its backend services and the account functions of the bridge-coach.ai website (together, the "App"). Capitalised terms not defined here have the meaning given in the Terms of Service. The App is intended only for persons aged 18 or over.

3. Key information in brief

(a) The App processes special categories of personal data, in particular data concerning health (addiction, sobriety, mental and emotional state), on the basis of your explicit consent. (b) In Shared Conversations you interact with an AI system (the "Coach"); the text of recent messages is sent to an external AI model provider in order to generate responses. (c) Selected content is encrypted at rest with AES-256-GCM and all connections use TLS/HTTPS; encryption is applied on the server and is not end-to-end, because the AI Mediator must read the content to provide the Service. (d) We do not sell your data, do not show advertising, do not use third-party advertising or analytics trackers in the App and do not use your content to train our own AI models. (e) Your data are stored in the European Union (Frankfurt, Germany). (f) You can delete individual content and your entire Account directly in the App.

4. Account and contact data

E-mail address, display name (first name), account role (Seeker, Supporter, Sponsor), password (stored only as an Argon2id hash), optional profile photo, e-mail verification status, account creation and update times, declaration of being 18+, and records of accepted consents and document versions. Source: you.

5. Onboarding and preference data

Area of work (addiction and recovery, relationship, mental health), optional free-text answers about your situation and expectations, relationship to the supported person and duration of support (Supporters), years of recovery experience (Sponsors), AI style and support-level preferences, notification settings, crisis-resources region, sobriety tracking settings, and optional crisis contact name and telephone number. Source: you.

6. Content and health data (special categories)

(a) Messages in Shared Conversations, including captions, photos, voice notes and videos; (b) emotion journal entries, moods and tags, and attachments; (c) sobriety start date, day logs (sober, struggled, relapsed) with notes, milestones and ceremony reflections; (d) tasks and goals; (e) letters to your future self; (f) guided-step and twelve-step answers; (g) supporter wellbeing check-ins (energy, resentment, needs); (h) personal timeline entries, including crisis support episodes; (i) reports of content you file. These data may reveal information about your health, addiction, emotional state, sex life or relationships and other special categories of data. Source: you.

7. Data generated by the AI Mediator (inferred data)

Per person and conversation: a running emotional valence score, a running crisis-risk score, affect labels; AI-generated public and private coach messages; session summaries visible to both Bridge members; step summaries; and, only with your consent, a short AI summary of how you are doing shown to your Bridge partner. These inferences may constitute data concerning health. Source: automated analysis of your messages.

8. Technical and usage data

Push notification token, device platform and time zone, a log of push notifications sent (type, priority, time), read markers, session tokens (stored as hashes), request identifiers, server logs containing user identifiers and technical counters, and IP addresses recorded transiently in access logs. The App does not collect your precise location, contacts, advertising identifier or health data from Apple Health or Health Connect.

9. Data of third parties

(a) E-mail address of a person you invite to a Bridge (used once to send the invitation); (b) name and telephone number of a crisis contact you enter; (c) information about other persons you mention in your content. If you provide data of third parties, you must have a legal basis to do so and inform them where required. The Controller obtains such data from you; the invited person is informed by the invitation e-mail and this Policy.

10. Device permissions

The App may request access to: notifications (to deliver messages, reminders and crisis alerts), camera and photo library (only when you take or attach a photo or video), and microphone (only when you record a voice note). Permissions are optional and may be withdrawn in the device settings; refusing them limits the related functions only.

Part II. Purposes, legal bases and AI processing

11. Purposes and legal bases

We process personal data for the following purposes: (a) creating and maintaining your Account and providing the App under the Terms of Service – Art. 6(1)(b) GDPR (performance of a contract); (b) processing data concerning health and other special categories of data contained in your content and generated by the AI Mediator, in order to provide the App's functions (Shared Conversations, AI mediation, journal, sobriety tracker, tasks, letters, guided steps, check-ins) – Art. 9(2)(a) GDPR (your explicit consent) together with Art. 6(1)(a) and (b) GDPR; (c) operating the Crisis Protocol – Art. 9(2)(a) GDPR, and in exceptional situations where you are physically or legally incapable of giving consent, Art. 9(2)(c) and Art. 6(1)(d) GDPR (vital interests); (d) showing your wellbeing summary to your Bridge partner – Art. 9(2)(a) and Art. 6(1)(a) GDPR (separate consent); (e) sending transactional e-mails and push notifications – Art. 6(1)(b) GDPR; (f) ensuring the security and integrity of the App, preventing abuse, moderating content and handling notices under the Digital Services Act – Art. 6(1)(c) GDPR (legal obligation) and Art. 6(1)(f) GDPR (our legitimate interest in a safe service); (g) handling complaints, enquiries and data subject requests – Art. 6(1)(c) and (f) GDPR; (h) establishing, exercising or defending legal claims – Art. 6(1)(f) GDPR and, for special categories, Art. 9(2)(f) GDPR; (i) sending an invitation to a person you indicate – Art. 6(1)(f) GDPR (the legitimate interest of the inviting User and the Controller in enabling the Bridge function); (j) complying with obligations under accounting, tax and other laws and with orders of authorities – Art. 6(1)(c) GDPR; (k) maintaining the records of consents and demonstrating compliance – Art. 6(1)(c) GDPR in connection with Art. 5(2) and Art. 7(1) GDPR.

12. Explicit consent to the processing of health data

12.1. During registration we ask for your explicit, separate and informed consent to the processing of data concerning health and other special categories of data, including their automated analysis by the AI Mediator and their transmission to the AI model provider. We record your User ID, the date and time, and the version of the consent text and documents.

12.2. Consent is voluntary. However, because the processing of such data is essential to the App's core functions, the App cannot be used without it.

12.3. You may withdraw your consent at any time by deleting your Account in the App or by e-mail. Withdrawal does not affect the lawfulness of processing carried out before withdrawal. Following withdrawal, we cease processing special categories of data and delete them in accordance with section 21, except where another legal basis applies (e.g. the defence of legal claims).

13. AI Mediator – transparency (EU AI Act, Art. 50)

13.1. When using Shared Conversations and guided functions you interact with an artificial intelligence system and not with a human; AI messages are labelled "Coach".

13.2. The AI Mediator analyses the text of messages to assess the emotional dynamics of the conversation (sentiment and affect analysis, running emotional and crisis-risk indicators) and, on that basis, generates suggested, de-escalating responses, private hints and summaries. The analysis is based on text only; no biometric data (face, voice characteristics) are used, and photos, voice notes and videos are not sent to the AI model. Although in our assessment this text analysis does not constitute an emotion recognition system within the meaning of Article 3(39) of the AI Act, we voluntarily inform you of it in accordance with Article 50(3) of the AI Act.

13.3. On each coaching turn we send to the AI model provider: the text of up to the 20 most recent messages of the conversation (participants are identified by numbered role labels, without names, e-mail addresses or user IDs; however, names or other data you type inside a message are transmitted as written), the running emotional and crisis-risk indicators, preparation answers of an active guided step, and the regional helpline list. Session summaries, milestone ceremonies and step summaries use up to 40–60 recent messages. Journal entries, letters, tasks, sobriety notes, check-in texts and onboarding answers are not sent to any AI model.

13.4. Neither we nor, under their contractual terms, our AI providers use your content to train AI models.

14. Crisis Protocol – processing

14.1. Each message in a Shared Conversation is automatically checked against a list of keywords indicating explicit self-harm or suicidal intent and assessed by the AI Mediator.

14.2. If a crisis signal is detected: (a) a crisis message with helplines for the relevant regions is displayed to all members of the Bridge; (b) the other member(s) of the Bridge receive an in-app alert and a high-priority push notification that their partner may need support (the notification does not contain the content of your message); (c) a crisis support entry is recorded on your timeline. A journal mood marked as "crisis" may, if your partner has enabled supporter alerts, result in a notification to your partner after 30 minutes.

14.3. No data are disclosed to emergency services, healthcare providers, the Controller's staff or any other person outside the Bridge as part of the Crisis Protocol, and the system does not place calls or send messages on your behalf.

14.4. The partner alert constitutes a disclosure of information that may concern your health; it is covered by your explicit consent given during registration and cannot be disabled while you use Shared Conversations.

15. Wellbeing summary for the Bridge partner

A short AI-generated summary of how you are doing is shown to your Bridge partner only if you give a separate consent for the given Bridge. You may revoke this consent at any time in the conversation settings; revocation stops the generation of new summaries, and you may request deletion of summaries already generated.

16. Automated decision-making and profiling

The App does not take decisions based solely on automated processing which produce legal effects concerning you or similarly significantly affect you within the meaning of Article 22 GDPR. The emotional and crisis-risk indicators constitute an automated evaluation of personal aspects (profiling) used only to adapt AI responses and to trigger the display of helplines and partner alerts; they are not used for marketing, scoring or access decisions. Moderation decisions concerning your Account are always taken by a human.

17. Voluntary nature of providing data

Providing data is voluntary, but the e-mail address, password, age declaration and the consents referred to in section 12 are necessary to create an Account and use the App. Other data (profile photo, onboarding free-text answers, crisis contact, journal content) are optional.

Part III. Recipients, transfers, security, retention and deletion

18. Recipients of data

18.1. We share personal data only to the extent necessary, with the following categories of recipients acting as our processors under data processing agreements (Art. 28 GDPR): (a) hosting and infrastructure – DigitalOcean, LLC (servers, database and media storage located in the Frankfurt, Germany region); (b) AI model providers – depending on the configuration of the Service, Anthropic, PBC (USA) and/or Mistral AI SAS (France), which receive the data described in section 13.3 solely to generate AI Output; (c) transactional e-mail – Postmark (ActiveCampaign, LLC, USA) – e-mail address, display name and content of verification, password-reset and invitation e-mails; (d) push notifications – Google Ireland Limited / Google LLC (Firebase Cloud Messaging) – device token and notification content, which for new-message notifications may include an excerpt of up to 160 characters of the message; (e) test distribution – Google (Firebase App Distribution) – e-mail addresses of testers during the test phase; (f) IT service providers supporting the development, maintenance and operation of the App, bound by confidentiality.

18.2. Other recipients: (a) members of your Bridges, to whom your messages, summaries and alerts are displayed as described in this Policy; (b) Apple and Google as operators of the App Store and Google Play, acting as independent controllers with respect to data processed in connection with downloading

the App; (c) legal, tax and audit advisers bound by professional secrecy; (d) public authorities, courts and law enforcement, where required by law.

18.3. We do not sell, rent or share personal data for advertising purposes.

19. Transfers outside the EEA

19.1. Your data are stored in the EEA. Some processors (in particular Anthropic, PBC, ActiveCampaign, LLC (Postmark), Google LLC and DigitalOcean, LLC) are established in the United States or may access data from there.

19.2. Such transfers take place only on the basis of: (a) the European Commission's adequacy decision of 10 July 2023 on the EU-U.S. Data Privacy Framework, where the recipient is certified under it; or (b) the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914, together with supplementary measures where required (encryption in transit, data minimisation, removal of names and identifiers from AI requests).

19.3. You may obtain a copy of the safeguards applied by contacting us.

20. Security measures

20.1. We apply technical and organisational measures appropriate to the risk (Art. 32 GDPR), in particular: (a) encryption in transit using TLS/HTTPS for all connections between the App, our servers and processors; (b) application-level encryption at rest using AES-256-GCM with a unique random nonce per value for message content, coach messages, journal content, letters to the future, check-in needs, ceremony reflections, sobriety notes and guided-step answers and summaries, and provider-level encryption of database volumes and media storage; (c) password hashing with Argon2id and storage of session and e-mail tokens only as cryptographic hashes; (d) short-lived access tokens (JWT) with rotating refresh tokens and reuse detection; (e) isolation of secrets and API keys in protected infrastructure configuration, separated from the source code; (f) access control limiting each query to the data of the authorised User and Bridge; (g) removal of names, e-mail addresses and user IDs from requests sent to AI models.

20.2. Because the AI Mediator, crisis detection and summaries require the content to be read in plain form on the server, encryption is not end-to-end. Authorised personnel and processors may technically access data only where necessary for maintenance, security, moderation of reported content or legal obligations, subject to confidentiality.

20.3. We maintain a personal data breach procedure and will notify the supervisory authority within 72 hours and affected Users without undue delay where required by Articles 33–34 GDPR.

20.4. No method of transmission or storage is completely secure. You are responsible for securing your device and credentials (see section 23).

21. Retention periods

(a) Account data and content: for the lifetime of the Account, until you delete it or individual content; there is no automatic deletion due to inactivity; (b) deleted messages: content is erased immediately; a technical record without content (identifier, author, time) may remain in the conversation; (c) push notification log: 7 days; (d) request identifiers with replies: 24 hours; (e) unused invitation codes: expire after 30 days; (f) server and access logs: until rotation, typically a few days; (g) database backups: up to 7 days (rolling); (h) data at the AI model provider: according to its retention terms, for Anthropic up to 30 days (longer only for content flagged for abuse), for Mistral AI in accordance with its applicable terms; (i) e-mail provider: up to 45 days; (j) undelivered push notifications at Google: up to 28 days; (k) data necessary to establish, exercise or defend legal claims, or required by law: only for the period necessary, up to the expiry of the limitation period.

22. Account deletion (Right to Erasure) and data export

22.1. You may delete your Account directly in the App (Settings → Delete Account) or by sending a request from your Account e-mail address to kontakt@affinity-intelligence.com. Deletion in the App is irreversible and carried out immediately; e-mail requests are executed without undue delay, no later than within one month.

22.2. Account deletion results in the permanent removal (hard delete) of the Account and all data associated with it from our production databases and media storage, including credentials, preferences, onboarding answers, journal entries, tasks, letters, sobriety data, check-ins, timeline entries, emotional indicators, consents, push tokens and your media files.

22.3. To protect the integrity of conversations of the other User, Shared Conversations are closed and remain readable for your Bridge partner: the text of messages you sent remains without your name or identifier, AI messages and session summaries already displayed to your partner remain on their side, and your photos, voice notes and videos are deleted.

22.4. Residual copies may persist for a limited time: in rolling backups (up to 7 days), with processors under section 21, and on the devices of other Users.

22.5. You may also delete individual content at any time: your own chat messages, journal entries, tasks, calendar entries and attachments; closing and removing a Bridge deletes the conversation once all members have removed it.

22.6. You may request a copy of your data in a structured, commonly used, machine-readable format (JSON) via the App, where available, or by e-mail; we will provide it within one month.

23. Data stored on your device

To enable offline use and faster loading, the App stores a local copy of conversations, journal entries and media on your device; login tokens are stored in the device's secure storage. Notifications may display message excerpts on your lock screen. We recommend using a screen lock, disabling lock-screen previews in the notification settings, and not sharing your device. Uninstalling the App removes the local

copy from the device; copies included in device backups are governed by your operating system's backup settings, which are outside our control.

Part IV. Your rights and additional information

24. Your rights (GDPR)

Subject to the conditions laid down in the GDPR, you have the right to: (a) access your data and obtain a copy (Art. 15); (b) rectify inaccurate data – you can edit your display name, e-mail address and preferences in the App (Art. 16); (c) erasure ("right to be forgotten") (Art. 17); (d) restriction of processing (Art. 18); (e) data portability – receive the data you provided in JSON format and transmit them to another controller (Art. 20); (f) object to processing based on our legitimate interests, on grounds relating to your particular situation (Art. 21); (g) withdraw any consent at any time, without affecting the lawfulness of processing before withdrawal (Art. 7(3)); (h) not be subject to decisions based solely on automated processing (Art. 22); (i) lodge a complaint with a supervisory authority – in Poland the President of the Personal Data Protection Office (Prezes UODO), ul. Stawki 2, 00-193 Warsaw, uodo.gov.pl – or with the authority of your Member State of residence or work.

25. Exercising your rights

Requests may be submitted via the functions available in the App or by e-mail to kontakt@affinity-intelligence.com. We respond without undue delay and in any event within one month; this period may be extended by two further months where necessary, of which you will be informed. To protect your data, we may ask you to confirm your identity, in particular by sending the request from the e-mail address assigned to your Account. Exercising your rights is free of charge, except for manifestly unfounded or excessive requests.

26. Adults only

The App is not directed at persons under 18. We do not knowingly collect data of minors. If we learn that an Account belongs to a person under 18, we will delete it together with its data. If you believe a minor is using the App, please contact us.

27. App Store and Google Play disclosures (App Privacy / Data Safety)

(a) Data collected and linked to your identity: contact info (e-mail address, name), user content (messages, photos, voice notes, videos, journal and other in-app content), health and fitness / sensitive information (sobriety, mood, mental and emotional wellbeing, crisis indicators), identifiers (user ID, push token), usage data (notification log, interactions needed to provide the functions), diagnostics (server error logs); (b) data used for tracking or advertising: none; (c) data shared with third parties: processed by service providers on our behalf as described in section 18, not sold and not shared for advertising; (d) data encrypted in transit: yes; (e) data deletion: you can delete your Account and data in the App and

request deletion by e-mail; (f) purposes: App functionality, account management, communication with you, security and fraud prevention.

28. Additional information for users outside the EEA (including the United States)

28.1. Regardless of your place of residence, we apply the standards described in this Policy.

28.2. We do not sell personal data, do not share personal data for cross-context behavioural advertising, do not engage in targeted advertising and do not use personal data for profiling in furtherance of decisions producing legal or similarly significant effects.

28.3. Consumer health data: the health-related data described in sections 6 and 7 (including data about substance use, sobriety, mental and emotional health and crisis indicators) are collected directly from you or inferred by the AI Mediator, solely to provide the App's functions; they are shared only with the recipients listed in section 18 and with members of your Bridges as described in this Policy, and only with your consent; we do not sell consumer health data.

28.4. Depending on your place of residence, you may have rights to know, access, correct, delete and obtain a portable copy of your data, to withdraw consent, to opt out of certain processing, and to appeal our decision on your request. You may exercise these rights by e-mail to kontakt@affinity-intelligence.com; if we refuse your request, you may appeal by replying to our decision, and we will respond within the period required by applicable law. You may designate an authorised agent where permitted by law.

28.5. We will not discriminate against you for exercising your privacy rights.

28.6. We do not respond to "Do Not Track" signals because the App does not track users across third-party services.

29. Website

The bridge-coach.ai website uses only a strictly necessary, encrypted session cookie and loads fonts from Google Fonts, which involves transmitting your IP address, browser information and the referring page to Google. The website does not use analytics or advertising cookies.

30. Changes to this Policy

We may update this Policy, in particular in the event of changes in the law, in the App's functions or in our processors (including AI providers). We will inform you of material changes in the App and/or by e-mail before they take effect and, where a change requires your consent, we will ask for it again. The current version and date are always available in the App.