Privacy Policy

This Privacy Policy explains how AhaPlay Bulgaria VCC ("AhaPlay", "we", "us", or "our") collects, uses, stores, shares, transfers, protects, and otherwise processes personal data in connection with the AhaPlay Platform, related applications, artificial intelligence (AI) functionalities, integrations, websites, communications, and related services (collectively, the "Platform").

This Privacy Policy forms part of the AhaPlay legal and operational framework and should be read together with the AhaPlay Terms of Service, the applicable Quote or Order Form, the applicable Service Level Agreement (SLA), the applicable Data Processing Agreement (DPA) where applicable, the Security Policy, the Acceptable Use Policy, the IP Policy, and other applicable AhaPlay policies and documentation. Capitalised terms used in this Privacy Policy, unless otherwise defined herein, shall have the meanings assigned to them in the AhaPlay Terms of Service.

AhaPlay is primarily a business-to-business (B2B) platform. Where Customer Organisations provide access to the Platform to their employees, contractors, representatives, participants, clients, members, or other authorised persons, the Customer Organisation acts as a separate data controller for employment-related and organisational data. Depending on the context and purpose of processing, AhaPlay may act as an independent controller (for platform operation, account management, billing, security, and similar activities), as a processor or service provider acting on behalf of a Customer Organisation (for workshop content, participation data, and similar activities), or in other legally recognised roles under Applicable Law. Your organisation's own privacy policy also applies where relevant.

Last Updated: [Effective Date]

Data Controller: AhaPlay Bulgaria VCC, 5 Rozova Dolina Street, Floor 4, Lozenets District, Sofia 1421, Bulgaria

Privacy Contact: privacy@ahaplay.com

Supervisory Authority: Commission for Personal Data Protection (CPDP), Bulgaria — cpdp.bg

Applicable Regulation: EU GDPR (Regulation 2016/679), UK GDPR, PECR

At a glance

This is a short, plain-language summary of how AhaPlay handles your personal data. It is not a substitute for the full Privacy Policy below, which is the legally binding version. Where the summary and the full policy differ, the full policy applies.

What we collect: account information you provide (name, email, password, optional profile details); workspace and organisational information from your employer or Customer Organisation; data generated when you participate in Sessions and Plays (responses, contributions, chat messages, engagement metrics); technical data (device, browser, IP); AI conversation data when you use AI features; and support communications when you contact us.

Why we process it: to deliver the Platform and the Sessions you participate in, to keep your account secure, to provide AI-assisted features, to operate and improve the service, and to comply with legal obligations.

Who sees it: your fellow Session participants, your Workspace Administrators and facilitators, AhaPlay personnel where reasonably necessary for support and security, and a defined list of sub-processors (see Section 5.4) under formal data processing agreements.

What we do not do: we do not sell your personal data, we do not use it for advertising, we do not train AI models on identifiable Customer Content without consent, we do not record video or audio Sessions unless all participants consent, and we do not make automated decisions with legal effect on you.

How long we keep it: retention periods vary by data category, from 7 days (AI conversations) to 3 years (Session activity). See Section 7 for the full retention schedule.

Your rights: you can access, correct, delete, restrict, or port your personal data, and you can object to processing or lodge a complaint with a supervisory authority. See Section 11 for how to exercise these rights, or contact privacy@ahaplay.com.

1. Who We Are

AhaPlay Bulgaria VCC is the entity responsible for operating the AhaPlay Platform and related services. Our legal name is AhaPlay Bulgaria VCC, our company registration number is UIC 208270875, and our registered address is 5 Rozova Dolina Street, Floor 4, Lozenets District, Sofia 1421, Bulgaria. For questions relating to this Privacy Policy or the processing of personal data, you may contact our Privacy Contact at privacy@ahaplay.com or by post at AhaPlay Bulgaria VCC, Attn: Privacy Contact, 5 Rozova Dolina Street, Floor 4, Lozenets District, Sofia 1421, Bulgaria.

2. Scope of This Privacy Policy

This Privacy Policy applies to personal data processed by AhaPlay in connection with the AhaPlay Platform and related applications; Workspaces, Programmes, Sessions, Plays, Templates, and related functionality; AI-assisted features and integrations; websites, onboarding flows, communications, and support services; and other services or functionality provided by AhaPlay from time to time.

This Privacy Policy applies to Customer Organisations, End Users and Workspace Administrators, participants in Sessions or Plays, visitors to AhaPlay websites, prospective customers, Partners, consultants, Thought Leaders, and business contacts, and other individuals whose personal data is processed in connection with the Platform or related services, regardless of whether access to the Platform occurs directly through AhaPlay, through a Partner, through an enterprise deployment, or through another authorised arrangement.

This Privacy Policy does not apply to third-party platforms, services, or integrations not controlled by AhaPlay; Customer Organisation policies or processing activities outside the Platform; or processing activities independently conducted by Customer Organisations, Partners, or other third parties outside AhaPlay's control. Third-party services and integrations may maintain their own privacy policies, terms, and processing practices.

Where you are invited to a Session, Programme, or other Platform experience by a Customer Organisation before you have an AhaPlay User Account, the Customer Organisation acts as the controller for that initial invitation and is responsible for providing you with information about how it uses your personal data in connection with the invitation. AhaPlay makes this Privacy Policy available to you at the time of your first interaction with the Platform (typically when you click the invitation link or otherwise first access Platform functionality). If you receive an invitation but do not access the Platform, your information is processed only by the inviting Customer Organisation and the email delivery sub-processor identified in Section 5.4, in each case for the limited purpose of delivering the invitation, until the invitation expires or is withdrawn.

3. Categories of Personal Data We Process

The categories of personal data processed by AhaPlay depend on the Platform functionality used, the configuration of the applicable Workspace, the role of the relevant End User, the integrations and AI features enabled, and the manner in which Customer Organisations and End Users use the Platform.

3.1 Account and Identity Data

When you register for or use an AhaPlay User Account, we process your full name (used for display name and identification in Sessions), email address (used for login, communications, and invitations), password in hashed form (used for authentication and never stored in plain text), profile photograph or avatar where voluntarily provided, professional bio or headline where voluntarily provided, language and localisation preferences, last login date, account status flags, and account creation timestamps. Legal basis: contract performance (Art. 6(1)(b) GDPR) for required account data, consent (Art. 6(1)(a) GDPR) for voluntarily provided profile elements such as photo and bio, and legitimate interest (Art. 6(1)(f) GDPR) for security and audit information such as last login date and account creation timestamps.

3.2 Workspace and Organisational Data

When an organisation deploys AhaPlay, we process organisation contact name and email address, organisation contact phone number where provided, email sender display name used in system emails sent on behalf of the organisation, Workspace identifiers, billing and subscription information, administrative contacts, Workspace configurations and settings, participant and membership structures, access permissions, enabled functionality and integrations, and customer support, onboarding, and operational configuration data relating to use of the Platform. Legal basis: contract performance (Art. 6(1)(b) GDPR).

3.3 Session and Play Activity Data

When you participate in AhaPlay collaborative experiences (Sessions and Plays), we process session attendance records including join timestamps and participation records; your responses, selections, rankings, reflections, and contributions to activities; activity progress including completion status, time in activity, and scores; alignment scores, divergence metrics, and aggregate team alignment indicators derived from group response patterns; chat messages sent within Sessions; endorsements you give or receive, with optional comments; commitments and acknowledgements you make during Sessions; post-Session satisfaction feedback and replay feedback where you choose to provide them; Programme Member status including join and completion dates and champion flags; facilitation actions where you act as a Session facilitator; and issue reports including name, email, and message if you submit a bug report. Legal basis: contract performance (Art. 6(1)(b) GDPR) for participation and engagement data necessary for service delivery, consent (Art. 6(1)(a) GDPR) combined with legitimate interest (Art. 6(1)(f) GDPR) for endorsements and feedback, and legitimate interest (Art. 6(1)(f) GDPR) for issue reports.

Your name, responses, and activity contributions may be visible to other participants in your Session and to designated Workspace Administrators and facilitators in accordance with the Platform configuration and applicable permissions. Contributions made during a Session, including responses, chat messages, endorsements, commitments, and generated content, persist within the applicable Workspace after the Session ends and remain accessible to authorised users in accordance with the retention periods set out in Section 7. See Section 5.3 for details on Workspace Administrator visibility and the scope of access.

3.4 Device and Technical Data

We automatically collect technical data when you use the Platform, including device type and operating system information, browser type and version, IP address and approximate geolocation derived from technical or network data (typically at country or city level), authentication and session activity, access timestamps, camera and microphone permission status (capability check only — we do not record), network connection quality during Sessions, infrastructure and API activity, error reports and crash information, performance and latency metrics, operational logs and monitoring information, browser storage and session state information, and security events, anomaly detection signals, and fraud-prevention indicators.

Legal basis: legitimate interest (Art. 6(1)(f) GDPR) for platform security, troubleshooting, service delivery, and operational integrity.

3.5 Error Monitoring

We use a third-party error monitoring service for automated error and crash reporting on the AhaPlay Platform in production environments. When an error occurs, the service may capture the error message and stack trace, your User Account identifier and in some cases your email address as part of the error context, device type and browser name and version, the page or route where the error occurred, and recent actions leading up to the error (breadcrumbs). Error monitoring data is used exclusively for diagnosing and fixing software bugs and is not used for profiling, marketing, or any purpose beyond platform reliability. Retention period: 90 days maximum. Legal basis: legitimate interest (Art. 6(1)(f) GDPR) — maintaining platform stability and resolving technical issues affecting users.

3.6 Authentication and Security Data

To secure your User Account, we process authentication tokens (stored in your browser's local storage until you log out) used to maintain your authenticated session across page refreshes and cleared on logout; separate impersonation tokens used when AhaPlay personnel access your User Account for support purposes, with the access notification commitment described in Section 5.3; session validity, expiry, and revocation records; password reset and magic link tokens (temporary and expiry-limited); and administrative access records where your User Account is accessed by AhaPlay personnel for support purposes. Specific technical details regarding storage keys, token formats, and cryptographic standards are described in the Security Policy. Legal basis: contract performance (Art. 6(1)(b) GDPR) and legitimate interest (Art. 6(1)(f) GDPR) for security of your account.

3.7 AI Conversation Data

When you use AhaPlay's AI-assisted features (including AI Programme generation, recommendations, summaries, prompts, and chat-based Programme creation), the following data may be processed: your chat messages and prompts (retained for 7 days, then auto-deleted); team goals and work context you describe (retained for 7 days, then auto-deleted); documents you upload such as PDFs (retained for 7 days, then auto-deleted); organisation name (retained for 7 days, then auto-deleted); your User Account identifier and Workspace identifier (retained for 7 days as metadata only and NOT sent to AI model providers); generated Programme results (retained for 1 year — see Section 7); and AI execution traces used for quality and safety monitoring (retained for 90 days maximum by the AI tracing provider). Legal basis: contract performance (Art. 6(1)(b) GDPR) — AI features are core to the service you contracted for.

We do not send your email address, User Account identifier, or account credentials to any AI model provider. Only the content you type into AI-assisted features (your goals, team context,

uploaded documents, and organisation name) is processed by AI providers. AhaPlay shall not use Customer Content in identifiable form for the training, fine-tuning, optimisation, or development of artificial intelligence models or machine learning systems, irrespective of whether such systems are intended for internal or external use, without the express prior consent of the applicable Customer Organisation. AhaPlay maintains contractual safeguards with its AI sub-processors (including OpenAI, Anthropic, and AI tracing providers) under which Customer Content submitted via API is not used by those providers to train their general-purpose AI models, except where expressly authorised by the applicable Customer Organisation or End User. AhaPlay may use aggregated, anonymised, statistical, and non-identifiable data derived from the use of the Platform solely for the purposes of operating, maintaining, securing, improving, supporting, and developing the Platform and its AI systems. Customer Organisations and End Users should not upload to AI-assisted features or otherwise submit through the Platform special categories of personal data (as defined under Article 9 GDPR, including health, biometric, racial or ethnic, religious, political, trade union, or sexual orientation data), highly sensitive employment information, protected health information, government-issued identifiers, financial credentials, or other highly regulated or sensitive information, unless expressly permitted by AhaPlay in writing and appropriate safeguards have been implemented.

3.8 Video and Audio During Sessions

AhaPlay integrates with a third-party video conferencing service for live video conferencing during collaborative Sessions. When you join a video Session, your display name and role are shared with the conferencing service, your audio and video streams are transmitted via the conferencing infrastructure, other Session participants can see and hear you, and conference room identifiers are linked to your Session. AhaPlay does NOT record your video or audio Sessions. Real-time streams are transmitted via the conferencing infrastructure and are not stored by AhaPlay unless Session recording is explicitly enabled and consented to by all participants (see Section 3.9). The video conferencing API is loaded as an external script during Sessions and may set its own browser storage or cookies independently of AhaPlay's control. Please refer to the applicable conferencing provider's privacy policy for details on data they may collect. Legal basis: contract performance (Art. 6(1)(b) GDPR) — video conferencing is an integral feature of collaborative Sessions.

3.9 Optional Session Recording (Consent Required)

AhaPlay may allow Session recording. Recording is ONLY enabled when explicit consent is obtained from ALL participants before the recording begins, a visible recording indicator is displayed throughout the recording, and the recording is stopped immediately if any participant withdraws consent. If you do not consent, you will not be recorded, and your ability to participate in the Session is not affected by declining to be recorded. Legal basis: consent (Art. 6(1)(a) GDPR) — explicit, specific, and freely given consent from all participants.

3.10 Browser Storage Technologies

AhaPlay does not use cookies on its marketing website or Platform for tracking, advertising, or analytics purposes. We use browser local storage exclusively to store functional and session data, including authentication tokens, administrative impersonation tokens, language code, cached UI strings for performance, UI layout preferences, and Session-specific UI state (such as timeline state and column visibility). Specific local storage key names and technical details are described in the Security Policy. You can clear all local storage data at any time via your browser settings; clearing this data will log you out of the Platform.

3.11 Heatmap and Session Replay Analytics (Consent Required)

Heatmap and session replay analytics functionality is only active on the AhaPlay Platform (not the marketing website). It is enabled only when (a) your Workspace Administrator has activated heatmap analysis at the Workspace level, AND (b) you have personally given explicit opt-in consent via the consent prompt. It is never activated automatically. Your individual consent overrides any Workspace-level setting. When you consent, the analytics provider collects mouse movements, clicks, and scroll behaviour, interactions with buttons and form fields, IP address (masked to city level by the provider's anonymisation), and device and browser information. The provider does NOT collect passwords, payment card data, or full text entered into sensitive fields (these are automatically masked). Legal basis: consent (Art. 6(1)(a) GDPR). You can withdraw consent at any time via your Account Settings, and the analytics provider will stop immediately.

3.12 Support Communications and In-Platform Messaging

When you interact with AhaPlay support, use in-platform messaging functionality, or engage with AI-assisted support features, we process the content of your support messages and conversations; attachments, screenshots, or files you submit in connection with a support request; identifiers needed to associate the request with your User Account (name, email, User Account identifier, Workspace identifier); contextual information about the issue (page or feature where the issue occurred, browser and device information, error messages); and metadata relating to the interaction (timestamps, response times, ticket status, assigned support personnel).

AhaPlay's in-platform support chat is self-hosted within AhaPlay's own infrastructure (AWS eu-central-1, Frankfurt) and support communications are not transmitted to or stored by external hosted support-chat providers. Where AI-assisted support functionality is used to triage, suggest responses to, or otherwise assist with your support interaction, the content of your message and relevant context may be processed by AhaPlay's AI sub-processors (OpenAI and Anthropic, as listed in Section 5.4) under the same safeguards described in Section 3.7, including the contractual prohibition on those providers training their general-purpose AI models on the submitted content.

Support communication content is retained for the period necessary to resolve your request and maintain support continuity, subject to the retention periods in Section 7. Legal basis: contract

performance (Art. 6(1)(b) GDPR) for support necessary to deliver the Services, and legitimate interest (Art. 6(1)(f) GDPR) for support quality improvement, fraud and abuse prevention, and operational continuity.

4. Purposes of Processing and Legal Bases

We only process your personal data where we have a lawful basis to do so. The principal purposes of processing and the corresponding legal bases are: creating and managing your User Account using name, email, and password under contract performance (Art. 6(1)(b) GDPR); delivering collaborative Sessions and Plays using session data, responses, presence, and video/audio under contract performance (Art. 6(1)(b) GDPR); AI Programme generation and AI-assisted features using chat messages, team context, organisation name, and documents under contract performance (Art. 6(1)(b) GDPR); sending invitations and Session reminders using name, email, and participation status under contract performance (Art. 6(1)(b) GDPR); User Account authentication and session security using authentication tokens, IP address, and session data under contract performance (Art. 6(1)(b) GDPR) combined with legitimate interest (Art. 6(1)(f) GDPR) for security; Platform security and fraud prevention using IP address, device data, audit logs, and login patterns under legitimate interest (Art. 6(1)(f) GDPR) — protecting Platform and users; service performance monitoring and debugging using error logs, crash reports, and technical data under legitimate interest (Art. 6(1)(f) GDPR) — maintaining platform quality; measuring team alignment and engagement using alignment scores and activity completion under contract performance (Art. 6(1)(b) GDPR); improving Platform features and UX using anonymised or aggregated usage patterns under legitimate interest (Art. 6(1)(f) GDPR) — product development; sending marketing communications using name, email, and organisation under consent (Art. 6(1)(a) GDPR) — only with your explicit opt-in; heatmap and session replay analytics using interaction data under consent (Art. 6(1)(a) GDPR) — only when you explicitly opt in; calendar integration using attendee emails, names, and event data under consent (Art. 6(1)(a) GDPR) — only when you connect the integration; and compliance with legal obligations using relevant data as required by law under legal obligation (Art. 6(1)(c) GDPR).

4.1 Legitimate Interests Balancing Test

Where we rely on legitimate interests (Art. 6(1)(f) GDPR), we have conducted a balancing test to ensure our interests do not override your fundamental rights. The principal legitimate interests we rely upon are:

Platform security and fraud prevention — our interest in protecting all users from security threats outweighs the minimal privacy impact of processing technical and log data, which users reasonably expect in a SaaS environment. We minimise data collection to what is necessary to identify and respond to threats, apply access controls, and retain security data only for the periods set out in Section 7.

Service monitoring and debugging — maintaining Platform reliability benefits all users, and error data is technical in nature and processed with access controls and PII minimisation. Error reports exclude payload content where possible and identifiers are kept to the minimum necessary to diagnose issues.

Product improvement and Platform development — we use anonymised or aggregated data only for general product improvement, and individual-level behavioural data is not used for profiling without consent. Where we use AI-assisted functionality data to improve those features, we apply the AI training restrictions described in Section 3.7.

Audit, governance, and abuse prevention — we retain audit logs, administrative access records, and operational records to support security investigations, lawful compliance, and protection of the Platform and its users. Access to these records is limited to authorised personnel with a legitimate operational, security, or compliance need.

Customer relationship management and support quality — we process limited identity and interaction data to manage customer relationships, deliver support, improve support quality, and maintain operational continuity. This processing is proportionate to the support context and limited to information reasonably necessary for the interaction.

Business protection and legal claims — we may process and retain data where necessary to establish, exercise, or defend legal claims, enforce contractual rights, or respond to legitimate business protection needs. Retention periods are aligned with applicable limitation periods.

In each case, we have weighed our legitimate interest against the rights and freedoms of data subjects and concluded that our interest does not override those rights, particularly given the safeguards applied (access controls, data minimisation, retention limits, and the absence of behavioural-advertising or third-party profiling activities). You have the right to object to processing based on legitimate interests; see Section 11 for how to exercise this right, and we will cease such processing unless we demonstrate compelling legitimate grounds that override your interests.

4.2 Controller and Processor Allocation

Where AhaPlay acts as a processor on behalf of a Customer Organisation, the Customer Organisation determines the purposes and means of processing. Activities for which the Customer Organisation acts as controller and AhaPlay acts as processor include Workspace configuration; participant management and Programme Member administration; the design and configuration of Programmes, Sessions, and Plays; participation visibility and organisational access settings; Customer Content uploaded to the Platform; AI-assisted workflow usage initiated by the Customer Organisation; and engagement and collaboration initiatives configured at the Workspace level. For these activities, processing is governed by the applicable Data Processing Agreement (DPA) and the Customer Organisation's instructions.

AhaPlay acts as an independent controller for activities where it determines the purposes and means of processing, including User Account management and authentication; subscription management and billing; customer relationship management; security, fraud prevention, and abuse prevention; operational monitoring and infrastructure management; Platform improvement and product development (using aggregated and anonymised data); AI-assisted functionality development and improvement; support and troubleshooting; and legal compliance and lawful business operations.

Where AhaPlay processes the same personal data for both controller and processor purposes (for example, an End User's name appears in both the User Account that AhaPlay manages as controller and the Session participation records that AhaPlay processes on behalf of the Customer Organisation), AhaPlay applies the appropriate role to each processing purpose.

5. How We Share Your Personal Data

5.1 Within Your Organisation

If you access AhaPlay through your employer or organisation, Workspace Administrators can view participation records, engagement metrics, and Session attendance; aggregate team alignment scores and commitment records are visible to organisational administrators; individual Session responses and activity contributions are visible to your Session facilitator and fellow participants during and after your shared Sessions; and your name, role, and profile photo are visible to members of your Workspace.

Where a Session, Programme, or collaborative experience involves participants from outside your Customer Organisation — including external guests, invited participants, Partners, consultants, or facilitators authorised by your Customer Organisation — your name, role, profile photo, responses, and contributions visible during the Session will be visible to those external participants on the same basis as to other Session participants. Workspaces are otherwise logically separated environments, and cross-Workspace visibility occurs only where explicitly configured by an authorised Workspace Administrator, enabled through applicable Platform functionality, or required for shared collaborative experiences, authorised invitation flows, or operational integrations.

5.2 Session Participants

During a live Session, the following data is shared in real time with all participants in your Session: your display name and profile photo, your responses and contributions to activities (which form part of the group alignment exercise), your presence status (online/offline), and chat messages you send within the Session.

5.3 Workspace Administrators and Operational Access

Designated Workspace Administrators can access Session state data for Plays within their Workspace, including participant names, responses, chat messages, and alignment scores. The scope of this access is determined by the Workspace configuration and role-based permissions set by the Customer Organisation. AhaPlay implements technical and organisational access controls to ensure only authorised administrators have administrator-level access, and all such access is logged in our audit trail. Customer Organisations remain responsible for ensuring that Workspace Administrator visibility is configured proportionately, that End Users and participants are informed of applicable visibility settings, and that organisational use of participation data complies with Applicable Law (including applicable workplace monitoring, labour, anti-discrimination, and works council requirements).

AhaPlay personnel authorised for platform-level operations and support may access Customer Workspaces solely to the extent reasonably necessary to provide the Services, respond to support requests, investigate security incidents, or fulfil legal obligations. Where reasonably practicable and not inconsistent with the purpose of the access, AhaPlay shall notify the applicable Workspace Administrator of such access. Audit trails of such access shall be maintained and may be made available to the applicable Customer Organisation upon reasonable request.

5.4 Third-Party Service Providers (Sub-Processors)

We share data with carefully selected third-party service providers who process data on our behalf. All sub-processors are bound by Data Processing Agreements (DPAs) complying with Article 28 GDPR. Our current sub-processors are:

- **Amazon Web Services (AWS)** — cloud infrastructure (hosting, databases, storage, monitoring). Data shared: all platform data including databases, files, and logs. Location: EU (eu-central-1, Frankfurt). Transfer safeguard: intra-EU, no transfer mechanism required.
- **SendGrid (Twilio)** — transactional email delivery. Data shared: name, email, security tokens in URLs, calendar ICS files. Location: US. Transfer safeguard: Twilio DPA with Standard Contractual Clauses (SCCs).
- **Sentry** — error monitoring and crash reporting. Data shared: error context, device data, User Account identifier. Location: US. Transfer safeguard: SCCs (EU-US).
- **LangSmith (LangChain)** — AI execution tracing and quality monitoring. Data shared: AI prompts, responses, run metadata (NOT User Account identifiers or email addresses). Location: US. Transfer safeguard: SCCs (EU-US).
- **OpenAI** — AI language model processing. Data shared: user prompts, team context, uploaded documents. Location: US. Transfer safeguard: OpenAI DPA with SCCs.
- **Anthropic** — AI language model processing. Data shared: user prompts, team context, uploaded documents. Location: US. Transfer safeguard: Anthropic DPA with SCCs.
- **Jitsi / 8×8 (JaaS)** — video conferencing infrastructure (may independently set browser storage during video Sessions). Data shared: display name, role, audio and video streams. Location: US/Cloud. Transfer safeguard: SCCs (EU-US).

- **Hotjar (Contentsquare)** — heatmap and session replay analytics (platform only, consent-gated). Data shared: interaction data, IP (anonymised), device info. Location: EU (Malta). Transfer safeguard: intra-EU, no transfer mechanism required.
- **Synthesia** — AI video generation. Data shared: Template data, video titles (no User PII normally). Location: UK. Transfer safeguard: UK Adequacy Decision.
- **Tavily** — web search for AI features. Data shared: search queries derived from team context. Location: US. Transfer safeguard: SCCs (EU-US).
- **Google Cloud / Google Workspace** — Google Calendar integration and Pub/Sub. Data shared: calendar attendee emails, names, event data. Location: EU/US. Transfer safeguard: Google DPA with SCCs.

An up-to-date sub-processor list, including any additions or substitutions made since the Last Updated date of this Privacy Policy, is also maintained at ahaplay.com/sub-processors. AhaPlay shall provide Customer Organisations with at least thirty (30) days' advance notice of any material change to its sub-processor list in accordance with Section 10.6 of the Terms of Service, with an objection mechanism as described therein.

5.5 Other Disclosures

We may also share personal data in the following circumstances: where required by law, court order, regulatory authority, or law enforcement; where reasonably practicable and legally permitted, AhaPlay will notify the affected Customer Organisation before disclosing Customer Content in response to governmental, judicial, regulatory, or law-enforcement requests, and where individual personal data is the subject of such a request the affected individual where legally permitted; in the event of a merger, acquisition, investment, financing transaction, corporate restructuring, change of control, sale of assets, strategic partnership, joint venture, or other corporate transaction involving AhaPlay, in which case personal data may be disclosed to potential or actual successors, acquirers, investors, advisors, or transaction participants — disclosures during due diligence shall be subject to confidentiality obligations, access restrictions, and commercially reasonable security safeguards, and any successor entity receiving personal data shall be expected to process such information in accordance with Applicable Law and protections substantially equivalent to those set out in this Privacy Policy. Nothing in this provision permits the sale, licensing, or transfer of identifiable personal data for third-party behavioural advertising or unrelated commercial exploitation purposes; to protect the vital interests of any person; and with your consent, for any other purpose where you have given explicit consent.

We do not sell your personal data. We do not share personal data with advertisers, use it for advertising targeting on third-party platforms, engage in cross-platform behavioural advertising profiling, or participate in advertising data brokerage. We do not use identifiable personal data processed through the Platform for advertising-targeting activities unrelated to the operation of the Platform and related services.

5.6 Public Content and User-Directed Sharing

Certain Platform functionality may allow Customer Organisations, Workspace Administrators, End Users, or authorised participants to intentionally publish, share, distribute, embed, export, or otherwise make content available to other users or the public — including public Templates, Programmes, Sessions, or Plays; public showcase pages or shared experiences; community content and shared resources; public galleries or discovery areas; shared links or embedded experiences; or other content intentionally made visible outside a private Workspace environment.

Customer Organisations and End Users remain responsible for ensuring that content intentionally shared, published, exported, or made publicly accessible through the Platform does not violate Applicable Law; does not infringe third-party rights; does not disclose confidential or sensitive information without authorisation; and is appropriate for the intended visibility and audience. Content intentionally made public or shared externally may become accessible to third parties and may remain visible, cached, copied, indexed, or redistributed outside AhaPlay's control. AhaPlay is not responsible for third-party use, republication, copying, indexing, or redistribution of content intentionally shared or made public by Customer Organisations or End Users.

5.7 Integrations and User-Authorised Third-Party Services

The Platform supports integrations with third-party services that Customer Organisations or authorised users may choose to connect — including calendar integrations (such as Google Calendar), authentication and single sign-on providers, productivity and collaboration tools, and other services enabled from time to time. Where an integration is activated, AhaPlay may exchange personal data with the integrated service to the extent necessary to provide the integration functionality (for example, sending Session schedules to a connected calendar service).

Integrations that you or your Customer Organisation choose to connect operate under the third party's own privacy policy, terms of service, and security practices, which are independent of this Privacy Policy. Customer Organisations and End Users are responsible for reviewing the appropriateness of connected services, managing applicable permissions (including OAuth authorisations), and ensuring lawful use of integrations. AhaPlay is not responsible for the processing activities, operational practices, or independent actions of third-party services or integrations outside AhaPlay's reasonable control.

Distinct from these integrations, AhaPlay's sub-processors (Section 5.4) process personal data on AhaPlay's behalf under Article 28 GDPR Data Processing Agreements and are AhaPlay's responsibility.

6. International Data Transfers

Some of our service providers are located outside the European Economic Area (EEA). When we transfer your personal data outside the EEA, we ensure that appropriate safeguards are in

place as required by Chapter V of the GDPR. The transfer mechanisms we use include Standard Contractual Clauses (SCCs) under Commission Decision 2021/914 for transfers to processors where no adequacy decision applies; the EU-US Data Privacy Framework (DPF) adequacy decision where the US processor is certified under DPF (verify at dataprivacyframework.gov); the UK Adequacy Decision (Art. 45 GDPR) for transfers to the United Kingdom; processor-specific DPAs incorporating SCCs where applicable; and no transfer mechanism is required for processing that remains within the EEA. Where the validity of an adequacy decision (including the EU-US DPF) is suspended, withdrawn, or substantially modified, AhaPlay will rely on SCCs or other valid transfer mechanisms in place with the applicable sub-processor as the operative safeguard, without requiring a change to this Privacy Policy.

6.1 Transfer Impact Assessments

For transfers to jurisdictions outside the EEA, we have conducted Transfer Impact Assessments (TIAs) considering the nature of the data transferred (typically technical, operational, or business content — not sensitive categories), the legal framework of the destination country and any applicable government access laws, supplementary measures in place (encryption in transit, pseudonymisation, access controls), and the practical likelihood of access to the specific data by third parties. Copies of our SCCs or TIA summaries are available upon written request to privacy@ahaplay.com.

7. Data Retention — How Long We Keep Your Data

We keep your personal data only as long as necessary for the purposes described in this Policy, to comply with legal obligations, resolve disputes, and enforce our agreements. The principal retention periods are: User Account profile (name, email, preferences) — duration of active User Account plus 2 years after closure for dispute resolution; authentication sessions (database) — until token expiry plus automated cleanup within 30 days; authentication sessions (cache) — up to 24 hours via TTL controls; security tokens (password reset, magic links) — until use or expiry plus 30 days cleanup; Session activity data (Plays, responses, alignment scores) — 3 years from Session date, then anonymised or deleted; real-time Session state (cache) — 30 days TTL from Session end; AI conversation data — 7 days from conversation end (automatic deletion); AI Programme results — 1 year from creation; AI execution traces — 90 days maximum; profile photos and uploaded files — tied to User Account lifecycle, deleted with the User Account; audit logs (Platform activity) — 1 year, then anonymised; application logs — 90 days; error reports — 90 days; access logs (ALB / CDN) — 90 days lifecycle policy; email delivery records — 90 days; heatmap session recordings (if consented) — maximum 1 year; calendar integration data — duration of integration plus 30 days after disconnect; endorsement data — 3 years or until you request deletion; support communication records (tickets, messages, attachments) — duration of active User Account plus 2 years after closure, or 3 years from last interaction for prospects and non-account holders, whichever is shorter; invitation and participation records — 3 years from invitation date.

We operate automated data cleanup processes that enforce the above retention periods. At the end of the applicable retention period, data is either permanently deleted or irreversibly anonymised (where deletion would affect other users' records, such as aggregate scores). Anonymised data no longer constitutes personal data and may be retained, used, analysed, or disclosed for analytics, benchmarking, research, product development, and other lawful business purposes. AhaPlay applies commercially reasonable technical and organisational measures to reduce the likelihood of re-identification of anonymised or aggregated data. Aggregated, anonymised, de-identified, pseudonymised, statistical, benchmarking, operational, and analytical information that does not identify Customer Organisations or identifiable individuals shall not constitute Customer Content or Confidential Information of the applicable Customer Organisation for the purposes of this Privacy Policy, the Terms of Service, or the applicable contractual framework.

8. How We Protect Your Data — Security Measures

We implement technical and organisational security measures proportionate to the risk, in compliance with Article 32 GDPR. AhaPlay maintains ISO/IEC 27001:2022 certification covering the AhaPlay platform and related information security management systems, and we undergo regular security assessments. Our security programme includes measures relating to encryption at rest and in transit using industry-standard cryptographic algorithms; authentication and access control including role-based access control (RBAC) and multi-factor authentication for administrative access; network segmentation with controlled access to production environments via VPN; vulnerability management including regular security updates, dependency scanning, and penetration testing; monitoring and alerting via automated security monitoring with anomaly detection; incident response procedures; backup and disaster recovery; and AI security governance. Detailed technical specifications, including specific encryption standards, cryptographic algorithms, network architecture, and infrastructure practices, are described in the Security Policy.

Organisationally, all staff with access to personal data are trained in data protection and security, access to personal data is granted on a need-to-know basis and reviewed regularly, all third-party sub-processors are vetted and bound by DPAs, a data breach response procedure is in place (see Section 13), and internal security policies are reviewed at least annually.

You also play a role in keeping your data secure: choose a strong, unique password and do not share it with others; log out of AhaPlay when using shared or public devices; and notify us immediately at privacy@ahaplay.com if you suspect unauthorised access to your User Account.

9. Consent — When and How We Ask

When you create an AhaPlay User Account, we ask you to read and accept our Terms of Service, read and acknowledge this Privacy Policy, and optionally opt in to marketing communications via a separate, optional checkbox. We record the date and version of the

Privacy Policy you accepted at registration. If we make material changes to this Policy, we will ask for your acknowledgement again. AhaPlay does not use tracking cookies and does not display a cookie consent banner. The tracking technologies requiring your consent are heatmap and session replay analytics (see Section 3.11) and optional Session recording (see Section 3.9), each of which operates on an explicit opt-in basis as described.

Where processing is based on your consent, you have the right to withdraw consent at any time without affecting the lawfulness of processing before withdrawal. To withdraw consent: for marketing emails, click 'Unsubscribe' in any email or update your communication preferences in your account settings; for heatmap and session replay analytics, opt out via your privacy settings; for calendar integration, disconnect via your integrations settings; for profile photo, delete your photo via your profile settings; and for any other consent, contact privacy@ahaplay.com and we will process your withdrawal within 5 business days.

10. Special Categories of Data and High-Risk Processing

Profile photos are uploaded voluntarily and used solely for display purposes (identifying you to team members). AhaPlay does not use facial recognition, biometric identification, or any processing that extracts biometric templates from photos. Profile photos are NOT processed for identification purposes. Legal basis: consent (Art. 6(1)(a) GDPR); you may delete your photo at any time.

AhaPlay has conducted a Data Protection Impact Assessment (DPIA) for its AI and large language model (LLM) processing features in compliance with Article 35 GDPR. The DPIA assessed risks associated with user-generated content processed by external AI providers, AI trace logging, and AI-generated programme content. Mitigations in place include 7-day TTL for AI checkpoints, exclusion of PII identifiers from AI model inputs, 90-day trace retention limit, and Data Processing Agreements with all AI providers.

AhaPlay has conducted a DPIA for heatmap and session replay analytics functionality in compliance with Article 35 GDPR. The DPIA assessed risks including inadvertent capture of sensitive form inputs and keystroke data. Mitigations in place include explicit opt-in consent required before activation, automatic masking of password fields and sensitive inputs, IP anonymisation, maximum retention period of 1 year, and the ability to withdraw consent at any time.

The AhaPlay platform collects engagement and behavioural data to measure team alignment and Programme effectiveness, including login frequency, activity completion rates, device type, engagement metrics, Programme participation, and alignment score trends. This data is used to provide the alignment measurement features that are core to the AhaPlay service. This data is NOT used to make automated decisions about individual employees, infer sensitive characteristics, or build profiles used for purposes beyond service delivery. Legal basis: contract performance (Art. 6(1)(b) GDPR) for service delivery metrics; legitimate interest (Art. 6(1)(f) GDPR) for aggregate product improvement.

11. Your Rights as a Data Subject

Under the GDPR, you have the following rights, which can be exercised free of charge. We will respond within one calendar month (extendable to three months for complex requests, with notice).

You have the right of access (Art. 15 GDPR) to obtain a copy of all personal data we hold about you, including purposes, categories, recipients, retention periods, and your other rights — submit a Data Subject Access Request (DSAR) via privacy@ahaplay.com or through your account privacy settings. You have the right to rectification (Art. 16 GDPR) to correct inaccurate personal data or complete incomplete data — update directly in your account profile or contact privacy@ahaplay.com (this right does not extend to audit logs, which are integrity-protected records). You have the right to erasure (Art. 17 GDPR), the 'right to be forgotten', to request deletion of your personal data — contact privacy@ahaplay.com with subject 'Erasure Request', subject to exceptions for legal obligation, public interest, and legal claims; residual data in backups is deleted within 90 days. Where your User Account is associated with one or more active Customer Organisation Workspaces, AhaPlay will erase data for which it acts as independent controller (such as User Account profile, authentication records, marketing preferences, and product analytics tied to your identity) on request; data processed by AhaPlay on behalf of a Customer Organisation (such as Session contributions, Programme participation records, and Workspace-specific content) is governed by the Customer Organisation's instructions and you may also exercise your erasure rights directly with the applicable Customer Organisation as the controller of that processing. If a Customer Organisation does not respond or refuses to act on your request, you may contact privacy@ahaplay.com for assistance and may lodge a complaint with your supervisory authority under Section 15. You have the right to restriction (Art. 18 GDPR) to request that we restrict (pause) processing of your data — contact privacy@ahaplay.com with subject 'Restriction Request', and we will confirm restriction within 5 business days. You have the right to data portability (Art. 20 GDPR) to receive your personal data in a structured, machine-readable format (JSON or CSV) — via your account privacy settings or by contacting privacy@ahaplay.com, applicable to data you provided that is processed by automated means on the basis of contract or consent. You have the right to object (Art. 21 GDPR) to processing based on legitimate interests or for direct marketing — contact privacy@ahaplay.com with subject 'Objection to Processing', or for marketing click 'Unsubscribe' (for marketing, this is an absolute right; for legitimate interests, we must cease unless we demonstrate compelling legitimate grounds). You have rights regarding automated decision-making (Art. 22 GDPR) not to be subject to solely automated decisions with significant legal or similar effect — AhaPlay does not make solely automated decisions with significant legal effects; see Section 12. You have the right to lodge a complaint (Art. 77 GDPR) with your local data protection supervisory authority — see Section 15.

11.1 Data Subject Access Request (DSAR) Process

To submit a DSAR or exercise any of the above rights: submit your request by email to privacy@ahaplay.com with subject line 'Data Subject Rights Request' or via the in-platform privacy settings. We may ask you to verify your identity (for example, confirm your registered email) to protect your data from unauthorised requests. We will acknowledge receipt within 3 business days and provide a full response within 1 calendar month, or notify you of any extension. For access requests, we provide a data export in JSON and/or CSV format covering all personal data described in Section 3. We do not charge for DSAR responses unless the request is manifestly unfounded, repetitive, or excessive.

12. Automated Decision-Making and Profiling

We use automated processing for the following functions, in each case as a support to human-led activities rather than as a replacement for human judgement:

Team alignment scores and divergence metrics — calculated by aggregating participant responses within an activity and computing statistical measures of convergence and variance across the group. These scores describe the group as a whole rather than individuals and are not used to evaluate individual performance.

AI-assisted Programme generation — large language models are prompted with the team goals, work context, and uploaded materials provided by the requesting user, and generate suggested Programme structures, Session outlines, and activity sequences. Outputs are recommendations, not directives, and require human review before deployment.

Group formation, participant distribution, and participation balancing — within a Session, AhaPlay may assign or rebalance participants across breakout groups or activity rounds based on signals such as participation count, role distribution, prior group composition, and Session design parameters. The signals used do not include sensitive characteristics, performance assessments, or behavioural profiles.

Workflow sequencing and orchestration — the order and pacing of activities within Programmes and Sessions is determined by Programme structure (configured by facilitators or Programme leads) and dynamic signals such as activity completion status and participant readiness. Facilitators can override sequencing at any point.

Moderation support — the Platform may flag content or interactions for facilitator or administrator review based on pattern-matching signals (such as keyword filters, length thresholds, or response anomalies). Flagging triggers human review; no automated action is taken on flagged content without human confirmation.

Scheduling, reminders, and notifications — recurring check-in Sessions, email reminders, and participation notifications are generated based on Programme schedules, participant status, and rules configured by Workspace Administrators.

We do NOT make solely automated decisions with significant legal effects on individuals. All meaningful decisions (for example, performance assessments, employment consequences) remain human-driven within your organisation. We do not use alignment scores to make hiring, firing, or promotion decisions. We do not infer sensitive characteristics (health, political views, religion) from your responses. AI-generated Programmes are recommendations rather than authoritative determinations, and a human (your facilitator or Programme lead) reviews and approves them before deployment. AI-generated outputs and recommendations produced by the Platform may contain inaccuracies, biases, omissions, or inappropriate content, and Customer Organisations and facilitators are responsible for reviewing such outputs before relying on them in any decision-making context affecting you. Customer Organisations are contractually prohibited under the Terms of Service from using the Platform, AI-generated outputs, analytics, or behavioural indicators as the sole or primary basis for hiring, termination, disciplinary, compensation, promotion, psychological assessment, health assessment, automated profiling, or other legally significant employment or regulatory determinations.

If you believe an automated process has produced an outcome that significantly affects you, please contact privacy@ahaplay.com and we will provide human review.

13. Data Breaches — Our Obligations and Your Rights

We take data security seriously. In the event of a personal data breach, we follow the procedures mandated by Articles 33 and 34 GDPR. Internally, all staff are trained to identify and immediately report suspected breaches to our Privacy Contact; upon confirming a breach, we conduct a risk assessment within 24 hours; and our incident response procedure documents the nature, data affected, likely consequences, and mitigation measures.

If a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the competent supervisory authority within 72 hours of becoming aware of the breach, including the nature of the breach and categories of data affected, the number of individuals likely to be affected, the likely consequences, and the measures taken or proposed to address it. If a breach is likely to result in a high risk to your rights and freedoms, we will notify you directly without undue delay in plain language, describing what happened and what data was involved, what we are doing about it, what you can do to protect yourself, and contact details for further information. We maintain a register of all data breaches (whether or not they meet the notification threshold) as required by Art. 33(5) GDPR.

14. Children's Privacy

AhaPlay is intended for use by individuals at or above the digital consent age applicable in their country of residence, which under GDPR Article 8 may range from 13 to 16 depending on the relevant EU member state (for example, the digital consent age is 16 in Germany and the Netherlands and 13 in some other member states). We do not knowingly collect personal data from children under the applicable digital consent age without verified parental consent. If your

organisation deploys AhaPlay for participants under the applicable digital consent age, the organisation is responsible for obtaining appropriate parental consent and must notify us in advance at privacy@ahaplay.com. If we discover we have inadvertently collected data from a child without appropriate consent, we will delete it promptly. Parents or guardians who believe their child's data has been collected without consent should contact us at privacy@ahaplay.com.

15. Your Right to Complain to a Supervisory Authority

Without prejudice to any other administrative or judicial remedy, you have the right to lodge a complaint with a data protection supervisory authority if you believe that our processing of your personal data infringes the GDPR (Article 77 GDPR). You can lodge a complaint with the supervisory authority of the EU member state where you habitually reside, where you work, or where the alleged infringement took place. You do not need to contact us first, but we encourage you to reach out at privacy@ahaplay.com as we would like the opportunity to address your concerns directly. For contract-related disputes between AhaPlay and a Customer Organisation, the escalation procedure set out in Section 18.2 of the Terms of Service applies in addition to (and without prejudice to) your non-waivable right to lodge a regulatory complaint.

The principal supervisory authority for AhaPlay is the Commission for Personal Data Protection (CPDP), Bulgaria — cpdp.bg, kzld@cpdp.bg. For UK data subjects, the UK Information Commissioner's Office (ICO) — ico.org.uk, 0303 123 1113. For other EU data subjects, you may locate your local data protection authority at edpb.europa.eu/about-edpb/about-edpb/members_en.

16. Records of Processing Activities (RoPA)

AhaPlay maintains an internal Record of Processing Activities (RoPA) as required by Article 30 GDPR. The RoPA documents all processing activities, purposes, lawful bases, data categories, recipients, transfers, and retention periods. This document is available to the supervisory authority on request. A summary of our processing activities is set out in this Privacy Policy; for the full internal RoPA, authorised parties (including supervisory authorities) should contact privacy@ahaplay.com.

17. Data Processing Agreements

We have executed Data Processing Agreements (DPAs) with all third-party sub-processors identified in Section 5.4, in compliance with Article 28 GDPR. These DPAs include specification of the subject matter, duration, nature, and purpose of processing; the type of personal data processed and categories of data subjects; processor obligations (to process only on our instructions, implement security measures, notify us of breaches, assist with data subject rights, and delete or return data on contract termination); and restrictions on sub-processing (sub-processors must obtain our authorisation before engaging further sub-processors). A list of our sub-processors and their DPA status is maintained internally and on our sub-processor

page; Customer Organisations and data subjects may request confirmation of DPA coverage for specific sub-processors by writing to privacy@ahaplay.com.

18. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technology, legal requirements, or for other operational reasons. We will post the updated Policy on our website with a revised 'Last Updated' date; notify Customer Organisations of material changes through reasonable communication channels in accordance with Section 17.2 of the Terms of Service; for changes that require renewed consent, present you with a new consent prompt at next login; and maintain an archive of previous versions of this Policy, available on request. Your continued use of AhaPlay after the effective date of a revised Policy constitutes your acknowledgement of non-material changes. For material changes requiring consent, we will seek your explicit agreement.

19. How to Contact Us

For any questions, concerns, or requests relating to this Privacy Policy or our data processing practices, contact us via privacy contact email at privacy@ahaplay.com, for data subject rights requests at privacy@ahaplay.com with subject 'Data Subject Rights Request', by postal address at AhaPlay Bulgaria VCC, Attn: Privacy Contact, 5 Rozova Dolina Street, Floor 4, Lozenets District, Sofia 1421, Bulgaria, via in-platform requests through your account privacy settings, or via our website at ahaplay.com/privacy-policy. We aim to respond to all privacy requests within 5 business days and provide full DSAR responses within 1 calendar month.