

ABH CONCLAVE

PRIVACY POLICY

Effective Date: 23 September 2026

1. Introduction

ABH Conclave Inc., a corporation organized under the laws of the State of Nevada, United States ("ABH", "we", "us", or "our"), respects your privacy. This Privacy Policy describes how we collect, use, share, and protect personal data in connection with ABH Conclave (the "Service"), an AI-powered advisory platform available at abhconclave.com.

This Privacy Policy applies to: (a) visitors to abhconclave.com and related ABH marketing pages; (b) prospective customers who contact us about the Service; (c) administrators and authorized users of the Service ("Service Users"); and (d) recipients of our transactional and marketing communications.

For the purposes of the European Union General Data Protection Regulation (Regulation (EU) 2016/679, the "GDPR") and the UK General Data Protection Regulation (the "UK GDPR"):

- ABH is the controller of personal data relating to website visitors, prospective customers, account administrators, and marketing recipients.
- This Privacy Policy addresses only ABH's activities as a controller. Where ABH processes personal data contained within Customer Content (for example, third-party names and details that a Service User uploads or types into the Service), ABH acts as a processor on behalf of the customer organization, which is the controller. The terms of that processing are not governed by this Privacy Policy but by our Data Processing Addendum and the Terms of Service, available on request.

2. Controller Details and How to Contact Us

Controller: ABH Conclave Inc.

Principal place of business: 3495 Lakeside Drive # 1064, Reno, Nevada 89509, USA.

Email for privacy enquiries: privacy@abhconclave.com

General contact: hello@abhconclave.com

Website: <https://abhconclave.com>

Representative in the European Union. ABH Conclave Inc. is not established in the European Union. In accordance with Article 27 of the GDPR we have designated a representative in the Union, who acts as a point of contact for data subjects and for supervisory authorities on all matters relating to the processing of personal data.

Our EU representative is appointed through Prighter. The designated entity is Prighter EU Rep GmbH, Schellinggasse 3/10, 1010 Vienna, Austria. It may be contacted at <https://prighter.com/q/13141060749>, quoting reference ID-13141060749.

Representative in the United Kingdom. ABH Conclave Inc. is likewise not established in the United Kingdom. In accordance with Article 27 of the UK GDPR we have designated a representative in the United Kingdom, also appointed through Prighter: Prighter Ltd, 20 Mortlake High Street, London SW14 8JN, United Kingdom, contactable at <https://prighter.com/q/13141060749>, quoting reference ID-13141060749.

Representative in Switzerland. ABH Conclave Inc. is not established in Switzerland. ABH has voluntarily designated a contact in Switzerland and, to the extent Article 14 of the Swiss Federal Act on Data Protection applies to ABH, that entity serves as ABH's representative there. The designated entity, appointed through Prighter, is Prighter CH GmbH, Obergrundstrasse 17, 6002 Luzern, Switzerland, contactable at <https://prighter.com/q/13141060749>, quoting reference ID-13141060749.

You may contact any of these representatives in the language of your choice on any matter relating to your personal data. Doing so does not limit your right to contact us directly at privacy@abhconclave.com, and it does not affect your right to lodge a complaint with a supervisory authority as described in Section 10.

3. Personal Data We Collect

3.1 Information you provide to us

- Account and contact data: name, work email address, organization name, role/title, billing address, and telephone number (optional).
- Authentication data: password hashes (we never store plaintext passwords), single sign-on identifiers (where applicable), and two-factor authentication settings.
- Billing data: payment method details (handled by our payment processor, Stripe — we receive limited metadata such as card brand, last four digits, expiry, and country, but not full card numbers). Where an invoice is paid by bank transfer rather than by card, we receive confirmation that the payment was received and the information your bank includes with the transfer; we do not receive your online banking credentials.
- Communications: messages, support tickets, survey responses, and any other content you send to us by email, in-product chat, or other channels.
- Customer Content: text, files, prompts, and other materials you submit to the Service. Customer Content may contain personal data about you, your colleagues, your customers, or other third parties, depending on what you choose to submit.
- Voice input: if you choose to speak an answer rather than type it, your browser captures the audio of what you say and sends it to ABH's own transcription service. The audio is transcribed and discarded; only the resulting text is kept, as Customer Content. See Section 5.

3.2 Information we collect automatically

- Usage data: information about how you interact with the Service, including pages visited, features used, queries made, session duration, and timestamps. This is used to operate, secure, and improve the Service.
- Device and connection data: IP address, browser type and version, operating system, device identifiers, language preference, and referring URL.
- Log data: server logs, including request paths, response codes, and error events. Logs are retained for a limited period for security, debugging, and audit purposes.
- Cookies and similar technologies: see Section 9.

3.3 Information we receive from third parties

- If you register or sign in using a third-party identity provider, we receive the profile attributes you authorize that provider to share with us.
- We may receive limited information from our payment processor about payment status (success, failure, dispute).
- Our marketing platform (GoHighLevel) may attribute visits to marketing campaigns and provide aggregated engagement data.

3.4 Special categories of personal data

We do not request, and the Service is not designed to receive, special categories of personal data within the meaning of Article 9 of the GDPR (such as data revealing racial or ethnic origin, political opinions, religious beliefs, trade-union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation). If you choose to include such data within Customer Content, you are responsible for ensuring you have a lawful basis to do so, and you should consider whether the Service is appropriate for that use. We also do not use voice recordings, or any measurement derived from them, to identify or authenticate any individual. We do not create voiceprints or other biometric templates, we do not run speaker-identification, emotion-detection or sentiment-analysis on voice, and we do not process biometric data within the meaning of Article 9 of the GDPR or of applicable United States biometric-privacy laws.

4. How We Use Personal Data and Our Legal Bases

We process personal data for the following purposes, on the legal bases identified:

4.1 Operating the Service

We process account, authentication, billing, usage, and Customer Content data to deliver the Service, including generating AI Output, maintaining accounts, processing payments, providing support, and securing the Service.

Legal basis: performance of a contract (GDPR Article 6(1)(b)); legitimate interests in operating and securing our business (Article 6(1)(f)).

4.2 Communications about the Service

We send transactional communications about your account, billing, security, and service status. These communications are not promotional and you cannot opt out of essential service communications while maintaining an active account.

Legal basis: performance of a contract (Article 6(1)(b)); legitimate interests (Article 6(1)(f)).

4.3 Marketing communications

Where permitted by applicable law, we may send marketing communications about the Service or related ABH offerings. You may opt out of marketing communications at any time using the unsubscribe link in the email or by contacting us.

Legal basis: consent (Article 6(1)(a)) for opt-in jurisdictions; legitimate interests for soft-opt-in to existing customers consistent with applicable law (Article 6(1)(f)).

4.4 Product improvement, analytics, and AI evaluation

We analyze usage data and aggregated performance metrics to understand how the Service is used, diagnose problems, and improve features. We do not use Customer Content to train, fine-tune, or otherwise improve any AI foundation model, whether ours or our subprocessors'.

Legal basis: legitimate interests in improving our products (Article 6(1)(f)).

4.5 Security, fraud prevention, and abuse detection

We process usage and log data to detect, investigate, and prevent unauthorized access, abuse, security incidents, and violations of our Terms or Acceptable Use Policy.

Legal basis: legitimate interests (Article 6(1)(f)); legal obligation (Article 6(1)(c)) where applicable.

4.6 Legal, regulatory, and contractual compliance

We process personal data as needed to comply with laws and regulations applicable to us (including tax, accounting, and consumer-protection rules), to respond to lawful requests from public authorities, and to establish, exercise, or defend legal claims.

Legal basis: legal obligation (Article 6(1)(c)); legitimate interests (Article 6(1)(f)).

4.7 Corporate transactions

If ABH is involved in a merger, acquisition, financing, reorganization, or sale of assets, personal data may be transferred as part of that transaction, subject to appropriate confidentiality protections.

Legal basis: legitimate interests (Article 6(1)(f)).

5. How We Handle Customer Content for AI Processing and Voice

5.1 AI inference

Because the Service relies on AI inference, only the query-relevant excerpts of Customer Content needed to answer a given request — together with the active session's messages — are transmitted to our AI subprocessor to generate Output. We do not transmit your full stored dossier. We have structured this pipeline to limit risk:

- No training. Our agreements with our AI subprocessors prohibit them from using Customer Content to train, fine-tune, or otherwise improve their foundation models.
- Limited retention by inference providers. A zero- or short-retention (ZDR) arrangement is not currently available to ABH. Under our current API terms, our AI subprocessor may retain the transient excerpts and Output transmitted for a given request for up to thirty (30) days for security and abuse-prevention before deleting them; we do not control this provider-side retention window. If a shorter-retention arrangement becomes available, the window will be reduced and this Policy updated.
- Embeddings stored under ABH's control. Vector embeddings generated from Customer Content for retrieval purposes are stored in our own MongoDB Atlas database in Frankfurt, scoped to your tenant, and not shared with the embedding provider beyond the inference call that produced them.
- Tenant isolation. Customer Content and Output are logically segregated by tenant identifier. Authorized Users only see content belonging to their own organization.
- Output is probabilistic. We do not have a record-of-truth for Output; running the same prompt twice can produce different responses. Customer is responsible for verifying any Output before relying on it. Please see our Terms of Service for the full disclaimer regarding AI Output.
- Provenance marking. Our AI subprocessor embeds provenance information in the content it generates: an imperceptible statistical watermark within generated text and, for file types that support it, signed provenance metadata following the C2PA standard. The PDF reports you download from the Service are rendered by ABH's own systems and carry ABH's own machine-readable provenance mark: document metadata identifying the content as AI-generated (using the IPTC digital-source-type vocabulary), the generator and the time of generation. ABH does not represent that those PDFs carry C2PA metadata, and the provider's statistical text watermark may persist in their text. This marking identifies the content as machine-generated by that provider's model. It does not identify you, your organization, your account, or the contents of your dossier, and it is not a means by which the provider can associate Output with you. It is applied by the provider under its own terms, is not something ABH can disable, and ABH does not add, alter, or remove it. Marking may persist where Output is copied or lightly edited.

5.2 Voice input (speech to text)

The Service offers optional voice input. Where a field supports it, you may speak your answer instead of typing it. Voice input is never required: every field that accepts speech also accepts typed text, and the Service is fully usable without a microphone.

When you use voice input, your browser records audio while you speak and transmits it, encrypted in transit, to a transcription service that ABH operates on its own infrastructure in Frankfurt, Germany. The audio is transcribed there and discarded as soon as the text exists. No third-party speech-recognition provider receives your audio at any point. We do not send it to your browser vendor's speech service, to a hosted transcription API, or to any other outside processor — transcription is

performed by software we run ourselves, which is why it takes a few seconds rather than being instant. The audio is held in memory only for as long as transcription takes. It is never written to disk, never written to our logs, never stored, and never backed up, and neither the audio nor the text derived from it is used to train, fine-tune or otherwise improve any model.

Transcription is automatic and is not guaranteed to be accurate. The transcribed text is placed in the field you were completing so that you can read it, correct it, and decide whether to submit it. Once you submit it, that text is Customer Content and is handled exactly as text you had typed, including the AI-processing arrangements described in Section 5.1 and the transfers described in Section 7.2.

Your browser asks for your permission before it can use your microphone, and the Service records only while you have started a recording and not yet stopped it. That permission is granted to, and can be withdrawn from, your browser at any time in its own settings, independently of your ABH account.

5.3 Voice output (text to speech)

The Service can also read certain text aloud — for example, a clarifying question put to you during a session. Where this is offered, the audio is generated by a speech-synthesis service that ABH operates on the same infrastructure in Frankfurt. The text is synthesized to audio there and streamed to your browser for playback. No third-party speech-synthesis provider receives the text, and the generated audio is not stored by us and is not retained after playback.

The voices are synthetic. They are produced by a general-purpose open-source speech model and are not recordings, imitations or clones of any identified or identifiable individual.

6. Who We Share Personal Data With

We share personal data only as needed to operate the Service and only with the categories of recipients described below for our internal business purposes.

6.1 Subprocessors

The subprocessors that process personal data on our behalf to deliver the Service — including our AI inference and embedding providers, our database host and our application host — are set forth in our Data Processing Addendum, together with the transfer mechanism relied on for each. Customers will be notified of our current and updated subprocessor list in accordance with that addendum.

6.2 Service providers

The following providers support ABH's own business operations. They do not process Customer Content on your behalf, and they are not subprocessors for the purposes of Article 28(2). ABH is the controller of the personal data they handle, with one exception: our representative acts as a controller in its own right when advising and supporting ABH on representative matters, and as a processor when operating the tool through which data subject requests are received and structured.

Service provider	Purpose	Location	Transfer mechanism
Jotform Inc.	Hosted forms used for prospective-customer intake and for existing-customer plan-change and cancellation requests. Form-supplied data only; no Customer	European Union (EU data region).	Data remains in EEA; Adequacy Decision / Adequacy

	Content.		Regulation for UK to EU transfers.
Stripe, LLC / Stripe Payments Europe Ltd.	Payment processing, subscription billing and tax calculation.	Ireland (EEA) and United States.	EU-U.S. Data Privacy Framework and UK Extension (where available); Adequacy Decision / Adequacy Regulation for UK to EU transfers; SCCs and UK Addendum where applicable.
HighLevel Inc. (GoHighLevel)	Marketing site hosting, CRM and contact management for ABH's own prospect and customer records. No Customer Content.	United States	EU-U.S. Data Privacy Framework and UK Extension (where available); Adequacy Decision / Adequacy Regulation for UK to EU transfers; SCCs and UK Addendum where applicable.
MongoDB, Inc. (Atlas)	Hosting of our operations database: account, authentication and billing records, for which ABH is the controller. (Atlas also hosts Customer Content, for which ABH is a processor — see our Data Processing Addendum.)	Frankfurt, Germany (EEA). Provider domiciled in the United States.	Data remains in the EEA. SCCs and UK Addendum cover any remote administrative access from the United States; Adequacy Decision / Adequacy Regulation for UK to EU transfers.
Fly.io	Application hosting and runtime, including the speech services ABH operates itself. Processes account and session data in transit and in memory.	Frankfurt, Germany (EEA). Provider domiciled in the United States.	Data remains in the EEA. SCCs and UK Addendum cover any remote administrative

			access from the United States; Adequacy Decision / Adequacy Regulation for UK to EU transfers.
Service provider	Purpose	Location	Transfer mechanism
Zoho Corporation	Business email and support ticketing for correspondence with ABH. No Customer Content.	EU data centre; United States for some services.	EU data region; where a service runs in the United States: SCCs and UK Addendum. Adequacy Decision / Adequacy Regulation for UK to EU transfers.
Better Stack, Inc. (United States)	Uptime monitoring, public status page and operational application logs. Logs contain pseudonymous account and request identifiers only; Customer Content, credentials and IP addresses are removed before logs leave the application. Logs are retained for 30 days.	Ingested to and stored in Better Stack's EU data region; the provider's terms reserve processing in the United States.	Adequacy Decision / Adequacy Regulation for UK to EU transfers; SCCs and UK Addendum where applicable.
Prighter (Prighter Group)	EU representative under GDPR Article 27, UK representative under UK GDPR, and Swiss representative under Article 14 FADP. Receives correspondence from data subjects and supervisory authorities and holds a copy of our record of processing activities. No Customer Content.	Austria (European Union), the United Kingdom and Switzerland.	Data remains in the EEA, the UK and Switzerland; Adequacy Decision / Adequacy Regulation for UK to EU transfers.

6.3 Affiliates

ABH Conclave Inc. is a single legal entity. We do not share personal data with corporate affiliates for their own purposes.

6.4 Professional advisors

We may share personal data with our lawyers, accountants, auditors, and other professional advisors where reasonably necessary and subject to confidentiality obligations.

6.5 Public authorities

We may disclose personal data to public authorities (including tax authorities, the competent data-protection supervisory authority, courts, and law-enforcement agencies) where required by law or to protect our rights or the rights of others.

6.6 No sale of personal data

We do not sell personal data, and we do not "share" personal data for cross-context behavioral advertising within the meaning of California or other state privacy laws.

7. International Data Transfers

ABH Conclave Inc. is established outside the EU and the UK, in the United States.

As a result, personal data for which we are the controller may be processed in the United States, both by ABH Conclave and by the processors and service providers identified in Section 6. Where such data is transferred outside the EEA or the UK, we rely on the safeguards described in this Section.

This Section 7 addresses therefore only transfers of personal data for which ABH acts as a controller. Where ABH processes Customer Content as a processor on behalf of a customer organization, the locations at which that Customer Content is stored and processed are governed by our Data Processing Addendum and the Terms of Service, not by this Privacy Policy.

7.1 Where your data is stored

Your account, authentication and billing data — the data for which ABH is the controller — is stored within the European Economic Area (EEA), on infrastructure located in Frankfurt, Germany. Customer Content (your dossier, your sessions and the vector embeddings generated from them) is stored on the same infrastructure; its handling as processor data is governed by our Data Processing Addendum, and we describe it here for transparency. We do not store Customer Content outside the EEA, and we do not create any copy of it outside the EEA.

7.2 Where AI processing takes place

Storage in the EEA does not mean that every processing operation takes place there, and we want to be plain about that. Generating Output requires us to transmit the query-relevant excerpts described in Section 5, together with the messages of the active session, to our AI subprocessor. That subprocessor is established in the United States. It processes those excerpts on its own infrastructure and does not offer a European processing region, so we cannot direct these requests to the EEA; they are routed across that provider's global infrastructure. Each request therefore involves a transfer of the transmitted excerpts, and of the Output returned, outside the EEA, and that provider may retain them for up to thirty (30) days as described in Section 5. This transfer is inherent to an AI service of this kind and cannot be disabled while the Service is in use.

Three limits apply to it, and they are the reason the Service is built the way it is. Only the excerpts a given request needs are transmitted — never your full dossier. Nothing transmitted is used to train, fine-tune, or otherwise improve any model. And no copy of your dossier is created outside our own EEA infrastructure: what leaves is transient, and what remains stored is in Frankfurt. Our embedding provider, which converts passages of Customer Content into the numerical vectors that make your dossier searchable, is also established in the United States; the vectors it returns are stored by us in Frankfurt.

7.3 Safeguards for transfers outside the EEA

Some of our processors are located outside the EEA, including in the United States, as further described in the table at Section 6 above. When personal data is transferred outside the EEA or the United Kingdom to a country that has not been deemed adequate by the European Commission or the UK government, we rely on appropriate safeguards, principally the European Commission's Standard Contractual Clauses (SCCs) and, for transfers from the UK, the UK International Data Transfer Addendum. Where a recipient is certified under the EU-U.S. Data Privacy Framework (and, for UK transfers, its UK Extension), we may rely on that certification. For transfers that rely on the SCCs or the UK Addendum, we carry out and document a transfer impact assessment (for EU transfers) or transfer risk assessment (for UK transfers) for each such transfer, and we apply supplementary measures where the assessment calls for them, such as encryption in transit and at rest, transmitting only the excerpts a request needs, pseudonymous identifiers in operational logs, and data minimisation.

7.4 More information

You may request a summary of the transfer mechanisms applicable to a specific transfer or processor by contacting us at privacy@abhconclave.com.

8. How Long We Keep Personal Data

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected, including legal, accounting, or reporting requirements.

- Account data: for the duration of the account, plus a wind-down period of up to twelve (12) months after account closure.
- Customer Content: retained while the Subscription is active. You may delete any Customer Content at any time; deletion is immediate, complete and irreversible, and we hold no backup from which it could be restored. Customer Content is held on a database cluster with backups permanently disabled, so no copy survives deletion. On termination or cancellation, Customer Content is deleted from our systems immediately and irreversibly. We do not retain a copy for any grace, wind-down or export period, and we hold no backup from which it could be restored. While your Subscription is active you can download a PDF of any Board Session verdict and of any 1:1 session transcript; please download anything you wish to keep before you cancel. Separately, and outside our control, our AI subprocessor may retain the transient per-request excerpts and Output described in Section 5 for up to thirty (30) days under its own terms.
- Voice audio: not retained. Audio captured for voice input exists only in memory for the duration of transcription and is then discarded. It is never written to persistent storage, never written to our logs, and never backed up. The transcribed text is retained as Customer Content, as described above.
- Usage and log data: typically retained for up to twelve (12) months for security and analytics purposes; security-relevant logs may be retained longer where needed for incident investigation.

- Billing and tax records: retained for seven (7) years following the end of the tax year, as required by applicable tax law, or longer if required by other applicable law.
- Marketing data: retained until you unsubscribe or otherwise object, after which we retain only the minimum necessary to honor your opt-out.
- Backups: Customer Content (your dossier) is stored on database infrastructure that is not backed up; when you delete it, it is permanently removed and cannot be recovered (see Section 5 and our Terms of Service). Account and billing records, which are not Customer Content, are kept on separate, backed-up infrastructure and may persist in encrypted backups for a limited period after deletion from production before being overwritten.

9. Cookies and Similar Technologies

Our website and Service use a limited set of cookies and similar technologies, broadly falling into three categories:

- **Strictly necessary:** cookies required to operate the Service (for example, authentication and session cookies, security cookies, load-balancing cookies). These cannot be disabled without breaking the Service.
- **Functional:** cookies that remember your preferences (for example, language, currency selection). These improve your experience but are not strictly necessary.
- **Analytics:** cookies (or equivalent technologies) that help us understand how the website and Service are used. We use first-party analytics with IP anonymization where feasible.

We do not use cookies for cross-site advertising or third-party behavioral targeting. Where required by applicable law (including the EU ePrivacy Directive and its national implementations), we obtain consent for non-essential cookies via a banner on first visit.

10. Your Rights

Subject to applicable law, you have the following rights regarding your personal data:

- **Access (GDPR Article 15):** request a copy of the personal data we hold about you.
- **Rectification (Article 16):** request correction of inaccurate or incomplete data.
- **Erasure (Article 17, the "right to be forgotten"):** request deletion of personal data, subject to limited exceptions.
- **Restriction of processing (Article 18):** request that we limit how we use personal data in certain circumstances.
- **Data portability (Article 20):** request a machine-readable copy of certain personal data and ask that we transmit it to another controller where technically feasible.
- **Objection (Article 21):** object to processing based on legitimate interests, including direct marketing.
- **Withdraw consent (Article 7(3)):** where processing is based on consent, withdraw consent at any time, without affecting the lawfulness of prior processing.

- **Automated decision-making (Article 22):** we do not make decisions that produce legal or similarly significant effects about you based solely on automated processing. Output from the Service is informational and is not a substitute for a human decision-maker.

To exercise any of these rights, please contact us at privacy@abhconclave.com. We may need to verify your identity before responding. We will respond within the time limits set by applicable law (normally one month under the GDPR, extendable in complex cases).

If our customer organization is the controller of personal data we process (for example, third-party data within Customer Content), please direct your request to that customer organization in the first instance. We will support the customer organization in responding to your request.

You also have the right to lodge a complaint with a data-protection supervisory authority, including in the country of your habitual residence, place of work, or place of the alleged infringement.

11. Security

We implement technical and organizational measures designed to protect personal data against unauthorized access, alteration, disclosure, or destruction. These measures include:

- Encryption of personal data in transit using TLS 1.2 or higher.
- Encryption of personal data at rest in our primary database.
- Logical tenant isolation so Authorized Users only access data belonging to their organization.
- Access controls and the principle of least privilege for ABH personnel.
- Regular review of subprocessor security postures.
- Audit logging of administrative actions.
- Voice audio processed for transcription is held in memory only, for the duration of transcription, and is never written to disk, to logs, or to backup.
- Backup and disaster-recovery procedures apply only to our operations database — account records, authentication data, and billing and accounting records — and to our source code. Customer Content is never backed up. It is held on a separate database cluster with backups permanently disabled, so deletion is immediate, complete and irreversible: no snapshots, no copies, nowhere.

No system is fully secure. If we become aware of a personal data breach that is likely to result in a risk to your rights and freedoms, we will notify you and the relevant supervisory authority as required by applicable law.

12. Children

The Service is intended for business and professional use by individuals aged 18 or over. We do not knowingly collect personal data from children. If you believe that we have inadvertently collected personal data from a child, please contact us at privacy@abhconclave.com and we will take steps to delete the information.

13. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The "Effective Date" at the top of this Privacy Policy indicates when it was last revised. If we make material changes, we will provide notice through the Service or by email to the Administrator on the account before the changes take effect. Continued use of the Service after the effective date of the updated Privacy Policy constitutes acceptance of the changes.

14. How to Contact Us

Privacy enquiries: privacy@abhconclave.com

General support: hello@abhconclave.com

Postal address: ABH Conclave Inc., 3495 Lakeside Drive # 1064, Reno, Nevada 89509, USA.

Version 2 · ABH Conclave Inc. (Nevada, USA). This Privacy Policy is published by ABH Conclave Inc.
Questions may be directed to privacy@abhconclave.com.