Bexa Privacy Policy

How Bexa collects, uses, and protects personal information.

Effective Date: September 18, 2026
Version: 1.0
Website: https://hirebexa.ai
Privacy Policy: https://hirebexa.ai/privacy-policy

This Privacy Policy explains how Corecentrix Business Solutions LLC, doing business as Corebex ("Bexa," "we," "us," or "our"), collects, uses, discloses, and protects personal information in connection with the Bexa AI calling platform, the hirebexa.ai website, and related services (together, the "Service").

Bexa serves businesses. When a customer configures an AI Agent and runs calling or messaging workflows, that customer decides what information is collected from call recipients and why. In those workflows the customer is the controller or business, and Bexa acts as a processor or service provider on the customer's documented instructions.

For the website, marketing, billing, and account administration, Bexa acts on its own behalf. This Policy covers both roles and says which is which.

If you interacted with an AI Agent operated by one of our customers and want your information corrected or deleted, contact that business directly. We will help them respond.

1. Who This Policy Covers

This Policy applies to:

- Visitors to hirebexa.ai and anyone who submits a form on it;
- Customers and their authorized users who access the platform;
- People who call, or are called by, an AI Agent configured by a customer; and
- Prospective customers, partners, and applicants who contact us.

It does not apply to third-party websites, customer systems, or telecommunications providers that operate under their own privacy practices.

2. Definitions

"Personal information" means information that identifies, relates to, or could reasonably be linked with an identifiable person or household.

"Customer Data" means the contact lists, recordings, transcripts, scripts, consent records, and other content a customer submits to or generates through the Service.

"Processor" means a party that processes personal information on another party's documented instructions rather than for its own purposes.

“Service Provider” has the meaning given under applicable United States state privacy law and describes Bexa’s role when handling Customer Data.

3. Information We Collect

We collect the following categories of information:

1. Contact details — name, business name, business email, phone number, and job role, typically supplied through a demo or contact form;
2. Account information — login credentials, permissions, and administrative settings for authorized users;
3. Call content — audio recordings, transcripts, summaries, and outcomes for calls handled by an AI Agent, where the customer has enabled them;
4. Call metadata — telephone numbers, timestamps, duration, routing path, transfer events, and disposition;
5. Configuration data — scripts, prompts, knowledge-base content, business hours, and escalation rules;
6. Billing information — plan, invoices, usage totals, and payment status, with card details held by our payment processor rather than by us;
7. Support information — messages, attachments, and diagnostic notes exchanged with our team; and
8. Device and usage information — IP address, browser type, pages viewed, and referring URL, collected automatically when you use the website or dashboard.

We do not ask for, and customers must not submit, payment-card security codes, government credentials, protected health information, or other regulated sensitive data unless we have approved that use in writing under a separate addendum.

4. Call Recordings and Transcripts

Recording and transcription are configurable and are controlled by the customer operating the AI Agent.

Where recording is enabled, an AI Agent can be configured to announce at the start of the call that the conversation is handled by an automated voice agent and may be recorded.

The customer is responsible for determining whether a call may be recorded in the relevant jurisdictions and for obtaining and documenting any consent the law requires. Bexa provides the disclosure and consent tooling but does not decide when it is legally sufficient.

Recordings and transcripts are stored against the customer’s account, available to the authorized users the customer designates, and retained for the period the customer configures, subject to the limits in the retention section.

5. How We Use Information

We use personal information to:

1. Provide, configure, and support the Service;
2. Route, transcribe, summarize, and deliver calls and messages a customer has configured;
3. Authenticate users and administer accounts;
4. Bill for subscriptions and usage, and collect amounts due;
5. Monitor performance, capacity, reliability, and quality;
6. Detect, investigate, and prevent fraud, abuse, and security incidents;
7. Respond to enquiries, support requests, and legal or regulatory requests;
8. Send service and administrative notices; and
9. Send marketing about Bexa where you have opted in and not since opted out.

We do not sell personal information, and we do not share it for cross-context behavioral advertising.

6. AI Processing and Model Training

Calls handled by an AI Agent are processed by speech recognition, language, and speech synthesis models in order to understand the caller and respond.

We do not use Customer Data to train general-purpose or shared AI models, and our model providers are contractually restricted from doing so with data processed for Bexa.

A customer's own agent configuration — scripts, prompts, and knowledge-base content — is used only to operate that customer's workflows.

We may use deidentified and aggregated information, which cannot reasonably be linked back to a customer or an individual, to measure quality, plan capacity, and improve the Service.

7. Legal Bases for Processing

Where the GDPR or UK GDPR applies to processing we carry out for our own purposes, we rely on:

- Performance of a contract, to provide and bill for the Service;
- Legitimate interests, to secure the Service, prevent abuse, and communicate with business contacts;
- Consent, for optional marketing messages and non-essential cookies; and
- Legal obligation, where retention or disclosure is required by law.

Where we process personal information on a customer's instructions, that customer is responsible for establishing the legal basis for the underlying calling or messaging.

8. Cookies and Similar Technologies

The website uses a small number of cookies and similar technologies:

- Strictly necessary cookies, which keep sessions secure and remember form state;
- Preference cookies, which remember choices such as a selected plan view; and
- Analytics cookies, which tell us in aggregate which pages are used and where visitors drop off.

Non-essential cookies are set only where local law permits or after consent, and browser controls can block or clear cookies at any time. Blocking strictly necessary cookies may break sign-in and form submission.

9. How We Share Information

We disclose personal information only as follows:

1. To service providers and subprocessors that host, transmit, secure, analyze, or support the Service, under written data-protection terms;
2. To telecommunications carriers, as required to originate, terminate, and label calls and messages;
3. To the customer whose AI Agent handled a call, together with the authorized users that customer designates;
4. To professional advisers, auditors, and insurers, where confidentiality obligations apply;
5. To an acquirer or successor in a merger, financing, or sale of assets, with notice where required;
6. To law enforcement, regulators, or courts, where disclosure is legally required or necessary to establish or defend legal claims; and
7. With your consent, or at your direction.

10. Subprocessors and International Transfers

We use affiliates and subprocessors for hosting, telecommunications, speech and language processing, analytics, payment, and support. We impose data-protection obligations appropriate to each one’s role, and we remain responsible for their performance of those obligations.

Personal information is processed in the United States and in other locations where we or our service providers operate.

Where personal information is transferred out of the EEA, the United Kingdom, or Switzerland, we rely on the European Commission’s standard contractual clauses, the UK addendum, or another lawful transfer mechanism, together with technical and organizational safeguards.

A current subprocessor list is available on request through the contact details below.

11. Data Retention

We keep personal information only as long as it is needed for the purpose it was collected for, or as long as law requires.

Typical periods:

- Call recordings and transcripts — for the retention window the customer configures;
- Account and configuration data — for the subscription term and a short wind-down period after it;
- Billing and tax records — for the period tax and accounting law requires;
- Security and audit logs — for a rolling period appropriate to their purpose; and
- Marketing contact details — until you opt out, or until the record goes stale.

After expiration or termination, and on written request within thirty days, we will delete or return reasonably accessible Customer Data, except where retention is legally required, needed to establish or defend legal claims, or held in backups that are deleted in the ordinary course. Bexa is not a customer's sole records-retention system.

12. Security

We maintain administrative, technical, and physical safeguards appropriate to the nature of the information we hold, including access controls, authentication, encryption in transit, monitoring and logging, vulnerability management, backups, personnel confidentiality obligations, and incident-response procedures.

No system is completely secure, and we cannot guarantee that unauthorized access, cyberattack, or data loss will never occur.

Customers are responsible for protecting their credentials, setting appropriate permissions, removing former users promptly, and reporting suspected unauthorized access to us without delay.

Where we confirm unauthorized acquisition of personal information within our control, we will notify affected customers without undue delay and provide the information reasonably needed for their own assessment and response.

13. Your Privacy Rights

Depending on where you live, you may have the right to:

1. Access the personal information we hold about you;
2. Correct inaccurate or incomplete information;
3. Delete information, subject to legal exceptions;
4. Receive a portable copy of information you provided;
5. Object to or restrict certain processing;
6. Withdraw consent you previously gave; and
7. Be free from discrimination for exercising these rights.

To exercise a right, use the contact details in the final section. We will verify the request before acting on it, and we will respond within the period applicable law allows.

If your information was collected by an AI Agent operated by one of our customers, we will forward your request to that customer and assist them in responding, because they decide what happens to that information.

14. Regional Disclosures

California

We do not sell personal information and do not share it for cross-context behavioral advertising, including that of anyone under sixteen. When handling Customer Data we act as a service provider and use it only for the purposes set out in our contract with the customer. California residents may exercise access, deletion, correction, and opt-out rights as described above, and may use an authorized agent.

EEA, United Kingdom, and Switzerland

You may lodge a complaint with your local supervisory authority. Where we act as a processor for a customer, please direct requests to that customer in the first instance.

Other United States states

Residents of states with comprehensive privacy laws have equivalent rights of access, correction, deletion, portability, and appeal. If we decline a request, our response will explain how to appeal that decision.

15. Children’s Privacy

The Service is built for business use and is not directed to children. We do not knowingly collect personal information from anyone under sixteen.

Customers must not configure AI Agents to call or message minors. If we learn that a child’s information has been collected through the Service, we will delete it and notify the relevant customer.

16. Changes to This Policy

We may update this Policy to reflect changes in our practices, technology, or legal requirements.

The version and effective date at the top of this page identify the current Policy. Material changes will be announced through the Service or by email before they take effect, and prior versions are archived and available on request.

Continuing to use the Service after a change takes effect means the updated Policy applies.

17. Contact Us

Questions, requests, and complaints about this Policy can be sent to our privacy team:

Corecentrix Business Solutions LLC d/b/a Corebex?80 Orville Drive, Suite 100?Bohemia, New York 11716

You can also reach us through the contact form at https://hirebexa.ai/contact, and we will route your message to the right team.