

Privacy Policy (v3.20)

Effective Date: August 1, 2026 | Last Updated: August 1, 2026

This Privacy Policy describes how **GZYN Inc.**, together with its affiliates, subsidiaries, officers, employees, contractors, and representatives, collectively referred to as “**Company**,” “**we**,” “**us**,” or “**our**”, collects, uses, discloses, stores, and protects personal information in connection with our websites, applications, cloud-based software-as-a-service (SaaS) products, AI-enabled features, subscription services, job portal, APIs, communications, and related services collectively referred to as the “**Services**.”

This Privacy Policy applies to:

- a. Visitors to our websites;
- b. Customers who register for, trial, purchase, or use our Services;
- c. Authorized users of our customers;
- d. Candidates, applicants, contractors, employees, or other individuals whose information is uploaded to or processed through our Services;
- e. Users of our job portal or publicly accessible pages; and
- f. Individuals who communicate with us or otherwise interact with our Services.

By accessing or using the Services, you acknowledge that you have read and understood this Privacy Policy.

If you are using the Services on behalf of an organization, you represent that you are authorized to accept this Privacy Policy on behalf of that organization.

1. Definitions

For purposes of this Privacy Policy:

- 1.1. “**Customer**” means an organization or individual that subscribes to, trials, purchases, or uses our Services.
- 1.2. “**Customer Data**” means data, files, text, documents, resumes, job descriptions, contracts, candidate profiles, summaries, messages, metadata, and other content that a Customer or its authorized users upload, submit, transmit, store, or process through the Services.
- 1.3. “**Personal Information**” or “**Personal Data**” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to an identified or identifiable individual.
- 1.4. “**Candidate Data**” means information relating to job candidates, applicants, employees, contractors, or other individuals, including resumes, CVs, employment history, education, skills, contact information, job preferences, assessments, summaries, ratings, notes, interview feedback, and similar information.
- 1.5. “**AI Features**” means artificial intelligence, machine learning, generative AI, natural language processing, ranking, matching, summarization, extraction, scoring, classification, or similar features made available through the Services.
- 1.6. “**Third-Party AI Providers**” means third-party providers of AI models or AI-related infrastructure, including providers such as OpenAI, Google Gemini, Anthropic, and other providers that we may use from time to time.
- 1.7. “**Cloud Providers**” means third-party providers of Cloud infrastructure, Cloud APIs, Cloud Storage or related technology used by Company to provide Product Features, which may include Google Cloud Platform, Amazon Web Services (AWS), MicroSoft Azure and other providers.
- 1.8. “**Process**” or “**Processing**” means any operation performed on Personal Information, including collection, storage, use, disclosure, transfer, analysis, deletion, or modification.

2. Our Role as Controller and Processor

Depending on the context, we may act as either a **data controller/business** or a **data processor/service provider**.

2.1. When We Act as a Processor or Service Provider

For most Customer Data processed through our SaaS products, we process Personal Information on behalf of our Customers. In such cases:

- a. The Customer determines the purposes and means of Processing;
- b. We process Customer Data according to the Customer’s instructions, our agreement with the Customer, this Privacy Policy, and applicable law;
- c. The Customer is responsible for providing required notices, obtaining required consents, establishing lawful bases for Processing, and responding to data subject requests where applicable.

For example, if a Customer uploads a Candidate's resume and asks our Services to match that resume against a job description using AI Features, the Customer is generally the controller/business of that Candidate Data, and we act as the processor/service provider.

2.2. When We Act as a Controller or Business

We may act as a controller/business when we process Personal Information for our own purposes, such as:

- a. Managing accounts and subscriptions;
- b. Operating our website;
- c. Processing payments through third-party payment processors;
- d. Conducting analytics and improving our Services;
- e. Marketing our Services;
- f. Detecting fraud and ensuring security;
- g. Managing customer support;
- h. Complying with legal obligations;
- i. Publishing or hosting publicly accessible content where we determine the relevant purposes and means.

3. Information We Collect

We may collect the following categories of information.

3.1. Account and Customer Profile Information

When you create an account, start a trial, subscribe to a product, or interact with us, we may collect:

- a. Name;
- b. Business email address;
- c. Phone number;
- d. Company name;
- e. Job title;
- f. Billing address;
- g. Account username;
- h. Password or authentication credentials;
- i. Subscription plan information;
- j. Customer profile information;
- k. Communications preferences;
- l. Support requests and correspondence.

3.2. Customer Data Uploaded to the Services

Customers and authorized users may upload, submit, generate, or store Customer Data, including:

- a. Candidate resumes and CVs;
- b. Candidate names, email addresses, phone numbers, addresses, and professional profiles;
- c. Employment history;
- d. Education history;
- e. Skills, certifications, licenses, and qualifications;
- f. Compensation expectations;
- g. Job preferences;
- h. Immigration or work authorization information, where included by the Customer;
- i. Job descriptions;
- j. Contracts and contract metadata;
- k. Candidate summaries;
- l. Candidate ratings or matching scores;
- m. Interview notes;
- n. Hiring workflow information;
- o. Customer-created notes and comments;
- p. Other documents, files, or information submitted by Customers.

Customer Data may contain Personal Information and, depending on the content uploaded by the Customer, may include sensitive Personal Information.

3.3. AI Inputs and Outputs

When Customers use AI Features, we may process:

- a. Prompts;
- b. Uploaded documents;

- c. Candidate resumes;
- d. Job descriptions;
- e. Contracts;
- f. Customer instructions;
- g. AI-generated summaries;
- h. Candidate-job matching scores;
- i. Suggested classifications;
- j. Generated text;
- k. Model responses;
- l. AI-generated analytics or recommendations;
- m. Metadata associated with AI requests and responses.

For example, a Customer may submit a Candidate resume and a job description to the Services, and the Services may transmit that information to a Third-Party AI Provider via API to produce a candidate-job fit analysis, skills match, rating, or summary.

3.4. Payment and Subscription Information

We offer monthly subscription billing. In the future we may offer Annual subscription billing. Payments are processed by third-party payment processors.

We may collect and store limited billing-related information, such as:

- a. Billing name;
- b. Billing address;
- c. Subscription plan;
- d. Transaction status;
- e. Invoice information;
- f. Last four digits of payment card, where available;
- g. Payment processor customer ID;
- h. Tax information where required.

We generally do not directly store full credit card numbers or complete payment credentials. Payment information is processed by our third-party payment processor in accordance with its own privacy policy and security practices.

3.5. Website, Device, Usage, and Analytics Information

When you access our websites or Services, we may automatically collect:

- a. IP address;
- b. Device identifiers;
- c. Browser type;
- d. Operating system;
- e. Referring URLs;
- f. Pages viewed;
- g. Features used;
- h. Clickstream data;
- i. Date and time of access;
- j. Session duration;
- k. Log files;
- l. Error reports;
- m. Approximate location derived from IP address;
- n. Cookie identifiers;
- o. Advertising identifiers;
- p. Usage analytics.

3.6. Cookies and Similar Technologies

We and third parties may use cookies, pixels, tags, SDKs, local storage, and similar technologies to:

- a. Enable essential functionality;
- b. Remember user preferences;
- c. Authenticate users;
- d. Improve product performance;
- e. Track usage of App features;
- f. Analyze website and Service traffic;
- g. Personalize content;
- h. Deliver and measure advertisements;
- i. Prevent fraud and abuse.

More information is provided in the Cookies and Tracking Technologies section below.

3.7. Publicly Available Information

We may collect information from publicly available sources, including:

- a. Public professional profiles;
- b. Company websites;
- c. Public job boards;
- d. Public social media pages;
- e. Public databases;
- f. Other publicly accessible sources.

3.8. Communications

If you contact us, we may collect:

- a. Name;
- b. Email address;
- c. Phone number;
- d. Company information;
- e. Message contents;
- f. Attachments;
- g. Support tickets;
- h. Call recordings or transcripts, where permitted by law;
- i. Feedback and survey responses.

4. How We Use Information

We may use Personal Information and Customer Data for the following purposes.

4.1. To Provide and Operate the Services

We use information to:

- a. Create and manage accounts;
- b. Provide SaaS products;
- c. Enable trials and subscriptions;
- d. Authenticate users;
- e. Store and retrieve Customer Data;
- f. Process resumes, job descriptions, contracts, and other documents;
- g. Provide search, matching, ranking, summarization, analysis, and workflow features;
- h. Generate AI outputs;
- i. Provide customer-to-customer sharing features where enabled;
- j. Host public job portal pages;
- k. Provide technical support;
- l. Maintain service availability.

4.2. To Provide AI Features

We may use Customer Data, including Candidate Data, job descriptions, contracts, and prompts, to provide AI Features, such as:

- a. Resume parsing;
- b. Candidate summarization;
- c. Job description analysis;
- d. Candidate-job matching;
- e. Skills extraction;
- f. Contract summarization;
- g. Document classification;
- h. Content generation;
- i. Ranking, scoring, or recommendations;
- j. Similar AI-enabled functionality.

To provide these features, we may transmit relevant data to Third-Party AI Providers via APIs. Responses from those providers may be returned to us and stored in our cloud-hosted databases.

4.3. To Manage Subscriptions and Payments

We use billing-related information to:

- a. Provide free trials;
- b. Manage monthly subscriptions;
- c. Process payments through third-party payment processors;
- d. Send invoices and receipts;
- e. Detect failed payments;
- f. Administer renewals and cancellations;
- g. Comply with tax and accounting obligations.

4.4. To Communicate with Customers and Users

We use information to:

- a. Send account notifications;
- b. Provide service updates;
- c. Respond to inquiries;
- d. Provide customer support;
- e. Send administrative messages;
- f. Send billing notices;
- g. Send security alerts;
- h. Provide marketing communications, where permitted by law.

4.5. To Improve, Secure, and Develop the Services

We may use information to:

- a. Monitor performance;
- b. Debug errors;
- c. Analyze usage trends;
- d. Improve user experience;
- e. Develop new features;
- f. Train personnel;
- g. Protect against unauthorized access;
- h. Detect fraud, abuse, security incidents, and unlawful activity;
- i. Enforce our agreements and policies.

4.6. To Provide Public Pages and Sharing Features

Certain information, including anonymized or pseudonymized candidate summaries, job descriptions, Customer profile information, and related content, may be displayed on publicly accessible web pages or made available through our job portal, depending on Customer settings, product configuration, consent, or publication choices.

We may also provide opt-in Customer-to-Customer sharing features that allow Customers to make selected candidate summaries, job descriptions, or other permitted information searchable and viewable by other Customers.

Customers are responsible for ensuring that they have appropriate rights, notices, consents, and lawful bases before making any Personal Information available publicly or to other Customers.

4.7. To Comply with Law and Protect Rights

We may process and disclose information as necessary to:

- a. Comply with applicable laws, regulations, legal processes, or governmental requests;
- b. Protect our rights, privacy, safety, or property;
- c. Protect Customers, users, candidates, or the public;
- d. Enforce our Terms of Service or other agreements;
- e. Investigate fraud, abuse, security incidents, or unlawful activity;
- f. Establish, exercise, or defend legal claims.

5. Legal Bases for Processing under GDPR and Similar Laws

Where the GDPR, UK GDPR, or similar laws apply, we rely on one or more of the following legal bases.

5.1. Contract

We process information as necessary to provide the Services, manage accounts, administer subscriptions, process payments, and fulfill our contractual obligations.

5.2. Legitimate Interests

We may process information based on our legitimate interests, including:

- a. Operating and improving the Services;
- b. Securing our systems;
- c. Preventing fraud and abuse;
- d. Providing customer support;
- e. Conducting analytics;
- f. Marketing to business contacts;
- g. Enforcing legal rights.

We rely on legitimate interests only where such interests are not overridden by the rights and freedoms of individuals.

5.3. Consent

We may rely on consent where required, including for:

- a. Certain cookies and tracking technologies;
- b. Certain marketing communications;
- c. Certain public disclosures;
- d. Processing of certain sensitive Personal Information where required by law.

Consent may be withdrawn at any time, subject to legal or contractual limitations.

5.4. Legal Obligation

We may process information as necessary to comply with legal obligations, including tax, accounting, regulatory, sanctions, anti-fraud, and law enforcement obligations.

5.5. Customer Instructions

Where we act as a processor, we process Customer Data according to the Customer's documented instructions, including instructions provided through use and configuration of the Services.

6. AI Processing and Third-Party AI Providers

Our Services use AI Features that may involve sending Customer Data to Third-Party AI Providers through APIs. These providers may include, without limitation:

- a. OpenAI;
- b. Google Gemini;
- c. Anthropic;
- d. Other AI model, infrastructure, analytics, or machine learning providers.

6.1. Data Sent to AI Providers

Depending on the feature used, we may send the following to Third-Party AI Providers:

- a. Candidate resumes;
- b. Candidate summaries;
- c. Job descriptions;
- d. Contracts;
- e. Customer prompts;
- f. User instructions;
- g. Relevant metadata;
- h. Other Customer Data necessary to provide the requested AI Feature.

6.2. AI Outputs

AI Providers may return outputs such as:

- a. Candidate summaries;
- b. Skills assessments;
- c. Candidate-job matching analysis;
- d. Ratings or scores;
- e. Suggested interview questions;
- f. Contract summaries;

- g. Extracted fields;
- h. Generated text;
- i. Recommendations.

These outputs may be stored in our cloud-hosted databases and made available to Customers through the Services.

6.3. Limitations of AI Features

AI-generated outputs may be inaccurate, incomplete, biased, misleading, or unsuitable for a particular purpose. Customers are responsible for independently reviewing, validating, and exercising human judgment before relying on AI outputs, especially for employment, hiring, contracting, legal, financial, or similarly significant decisions.

Unless expressly agreed otherwise in writing, our AI Features are intended to assist human decision-making and are not intended to be the sole basis for employment, hiring, termination, compensation, contracting, legal, or other decisions that may significantly affect individuals.

6.4. Customer Responsibilities for AI Use

Customers are responsible for:

- a. Ensuring they have a lawful basis to submit Personal Information to the Services and AI Providers;
- b. Providing required notices to candidates and other individuals;
- c. Obtaining required consents where applicable;
- d. Complying with employment, anti-discrimination, consumer protection, AI governance, privacy, and data protection laws;
- e. Reviewing AI outputs before use;
- f. Avoiding unlawful discrimination or unfair treatment;
- g. Not uploading information that they are not authorized to process.

6.5. Third-Party AI Provider Practices

Third-Party AI Providers process data according to their own agreements, data processing terms, technical controls, and privacy practices. We take commercially reasonable steps to select reputable providers and configure available privacy and security settings appropriately. However, we do not control all aspects of third-party provider systems and are not responsible for their independent acts or omissions except as required by applicable law or applicable agreements.

7. Public Pages, Job Portal, and Customer-to-Customer Sharing

7.1. Publicly Accessible Pages

Certain information may be displayed on publicly accessible web pages, including:

- a. Job descriptions;
- b. Customer profile information;
- c. Company descriptions;
- d. Public job postings;
- e. Anonymized or pseudonymized candidate summaries;
- f. Other content selected, configured, submitted, approved, or authorized for publication.

Publicly accessible information may be indexed by search engines, viewed by third parties, copied, stored, or redistributed by others. We cannot control how third parties use information once it has been made publicly available.

7.2. Anonymized and Pseudonymized Candidate Summaries

We may make anonymized, aggregated, or pseudonymized Candidate summaries available through public pages or sharing features. However, anonymization may not be perfect, and in some circumstances individuals may be re-identified when information is combined with other data.

Customers must not publish Candidate Data unless they have the right and lawful basis to do so.

7.3. Opt-In Customer-to-Customer Sharing

The Services may include an opt-in sharing capability that allows Customers to make selected information searchable or viewable by other Customers, such as:

- a. Candidate summaries;
- b. Candidate skill profiles;
- c. Job descriptions;
- d. Hiring needs;
- e. Customer profile information;
- f. Other Customer-approved content.

Customers control whether to enable such sharing features, subject to product settings. If a Customer enables sharing, other Customers may be able to search, view, copy, contact, or otherwise use the shared information.

Customers are solely responsible for ensuring that shared information does not violate privacy rights, contractual obligations, employment laws, confidentiality obligations, intellectual property rights, or other legal requirements.

8. How We Disclose Information

We may disclose information as described below.

8.1. Service Providers and Subprocessors

We may disclose information to vendors, service providers, contractors, and subprocessors who perform services on our behalf, such as:

- a. Cloud hosting providers, including Google Cloud Platform;
- b. AI model providers;
- c. Payment processors;
- d. Email service providers;
- e. Customer support platforms;
- f. Analytics providers;
- g. Security vendors;
- h. Logging and monitoring providers;
- i. Data storage providers;
- j. Marketing and advertising partners;
- k. Professional advisors.

These parties may access information only as necessary to provide services to us or as otherwise permitted by applicable law and agreements.

8.2. Google Cloud Platform

We store Customer Data and other data in cloud infrastructure provided by Google Cloud Platform. Data may be stored, backed up, replicated, or processed in data centers located in various regions depending on our configuration, Customer settings, availability, redundancy, and operational needs.

Third-Party AI Providers

As described above, we may disclose Customer Data to Third-Party AI Providers to provide AI Features requested or enabled by Customers.

8.3. Payment Processors

Payment information is processed by third-party payment processors. We may share billing-related information with payment processors to administer subscriptions, collect monthly payments, process refunds, detect fraud, and comply with financial regulations.

8.4. Other Customers and Public Users

Where enabled, configured, or authorized, information may be shared with:

- a. Other Customers through opt-in sharing features;
- b. Visitors to public job portal pages;
- c. Search engines;
- d. Other public internet users.

8.5. Business Transfers

We may disclose or transfer information in connection with:

- a. A merger;
- b. Acquisition;
- c. Financing;
- d. Reorganization;
- e. Bankruptcy;
- f. Sale of assets;
- g. Due diligence;
- h. Change of control;
- i. Similar corporate transaction.

Information may be transferred as part of such transactions, subject to applicable law.

8.6. Legal Compliance and Protection

We may disclose information if we believe in good faith that disclosure is necessary or appropriate to:

- a. Comply with law;
- b. Respond to subpoenas, court orders, or legal processes;
- c. Cooperate with regulators or law enforcement;
- d. Protect our rights, safety, or property;
- e. Protect Customers, users, candidates, or others;
- f. Investigate fraud, security incidents, or abuse;
- g. Enforce our agreements.

8.7. Affiliates

We may disclose information to our affiliates and related entities for purposes consistent with this Privacy Policy.

9. Cookies, Advertising, and Tracking Technologies

We use cookies and similar technologies for several purposes.

9.1. Types of Cookies We Use

- a. Essential Cookies: Required for login, authentication, security, account management, and core functionality.
- b. Functional Cookies: Remember preferences and improve user experience.
- c. Analytics Cookies: Help us understand how users interact with our websites and Services.
- d. Advertising Cookies: Help deliver, personalize, and measure advertisements.
- e. Performance Cookies: Help us monitor performance and troubleshoot issues.

9.2. Third-Party Cookies and Advertising

We may allow third-party analytics and advertising partners to use cookies, pixels, or similar technologies on our websites and Services. These third parties may collect information about your activities over time and across different websites and services.

Where required by law, we will obtain consent before placing non-essential cookies or using advertising trackers.

9.3. Managing Cookies

You can manage cookies through:

- a. Browser settings;
- b. Cookie consent banners or preference centers, where available;
- c. Device settings;
- d. Industry opt-out tools;
- e. Advertising network opt-out mechanisms.

If you disable cookies, some features of the Services may not function properly.

9.4. Do Not Track and Global Privacy Control

Some browsers send "Do Not Track" signals. Because there is no uniform standard for such signals, we may not respond to all Do Not Track signals.

Where required by applicable law, including certain U.S. state privacy laws, we will honor recognized opt-out preference signals such as Global Privacy Control for applicable browsers and contexts.

10. Data Retention

We retain Personal Information and Customer Data for as long as reasonably necessary to fulfill the purposes described in this Privacy Policy, including:

- a. Providing the Services;
- b. Maintaining accounts;
- c. Complying with contractual obligations;
- d. Providing customer support;
- e. Maintaining business records;
- f. Complying with legal, tax, accounting, and regulatory obligations;
- g. Resolving disputes;
- h. Enforcing agreements;

- i. Maintaining backups and security logs.

Customer Data is generally retained for the duration of the Customer's subscription or as otherwise configured by the Customer or required by agreement. After account termination, we may delete or anonymize Customer Data after a reasonable period, subject to backup retention, legal obligations, dispute resolution, and legitimate business needs.

Publicly posted or shared information may remain accessible until removed, but copies may persist in search engines, caches, archives, backups, or third-party systems beyond our control.

11. Data Security

We use commercially reasonable administrative, technical, and physical safeguards designed to protect Personal Information and Customer Data from unauthorized access, loss, misuse, alteration, or disclosure.

These safeguards may include:

- a. Encryption in transit;
- b. Access controls;
- c. Authentication mechanisms;
- d. Monitoring and logging;
- e. Segregation of duties;
- f. Secure cloud infrastructure;
- g. Vendor security reviews;
- h. Backup and recovery procedures;
- i. Security policies and training.

However, no method of transmission, storage, or processing is completely secure. We cannot guarantee absolute security. Customers and users are responsible for maintaining the confidentiality of account credentials and for all activity occurring under their accounts.

12. International Data Transfers

The Services are available globally. Your information may be processed in countries other than the country where you are located, including countries that may not provide the same level of data protection as your jurisdiction.

Where required by law, we use appropriate safeguards for international transfers, such as:

- a. Standard Contractual Clauses approved by the European Commission;
- b. UK International Data Transfer Addendum;
- c. Adequacy decisions;
- d. Data processing agreements;
- e. Other lawful transfer mechanisms.

By using the Services, you understand that information may be transferred to and processed in countries outside your jurisdiction, subject to applicable legal safeguards.

13. GDPR, UK GDPR, and EEA/UK/Swiss Privacy Rights

If you are located in the European Economic Area, United Kingdom, or Switzerland, you may have certain rights under applicable data protection laws.

Depending on the circumstances, these rights may include:

- a. Right of access;
- b. Right to rectification;
- c. Right to erasure;
- d. Right to restriction of processing;
- e. Right to data portability;
- f. Right to object to processing;
- g. Right to withdraw consent;
- h. Right not to be subject to certain automated decision-making;
- i. Right to lodge a complaint with a supervisory authority.

Where we act as a processor, requests relating to Customer Data should generally be directed to the relevant Customer. If we receive such a request directly, we may forward it to the Customer or instruct the requester to contact the Customer.

To exercise rights where we act as controller, contact us at: contact.us@4everi.com.

14. Automated Decision-Making and AI-Assisted Processing

Our AI Features may assist Customers in analyzing resumes, job descriptions, contracts, candidate-job matches, and related information.

Unless expressly stated otherwise, our Services are not intended to make fully automated decisions that produce legal or similarly significant effects without human involvement. Customers are responsible for ensuring appropriate human review of AI outputs and for complying with applicable laws governing automated decision-making, employment decisions, hiring tools, profiling, and AI systems.

If you believe an AI Feature has been used to make a decision about you, you should contact the Customer responsible for that decision.

15. California Privacy Notice

This section applies to California residents and is intended to comply with the California Consumer Privacy Act as amended by the California Privacy Rights Act, collectively the "CCPA."

15.1. Categories of Personal Information We May Collect

Depending on your relationship with us, we may collect the following categories of Personal Information:

CCPA Category	Examples
Identifiers	Name, email address, phone number, IP address, account ID
Customer records information	Billing address, subscription details, payment-related information
Commercial information	Products purchased, subscription status, invoices, transaction records
Internet or network activity	Usage logs, pages viewed, feature usage, cookies, analytics data
Geolocation data	Approximate location derived from IP address
Professional or employment-related information	Resumes, job history, education, skills, job descriptions
Education information	Education history included in resumes or profiles
Inferences	Candidate summaries, matching scores, preferences, profiles
Sensitive Personal Information	Information included in resumes or documents, such as government identifiers, immigration status, demographic data, or other sensitive information if uploaded by Customers

We collect these categories from Customers, users, candidates, public sources, service providers, cookies, and automated technologies.

15.2. Purposes for Collection and Use

We may collect and use Personal Information for the purposes described in this Privacy Policy, including:

- Providing the Services;
- Processing Customer Data;
- Providing AI Features and Customer to Customer Sharing Features;
- Managing subscriptions and payments;
- Customer support;
- Analytics;
- Advertising and marketing;
- Security and fraud prevention;
- Legal compliance.

15.3. Disclosure of Personal Information

We may disclose Personal Information to the categories of third parties described in this Privacy Policy, including:

- Cloud hosting providers;
- AI providers;
- Payment processors;
- Analytics providers;
- Advertising partners;
- Customer support providers;

- g. Professional advisors;
- h. Affiliates;
- i. Other Customers or public users where sharing or public posting is enabled;
- j. Government authorities where required by law.

15.4. Sale or Sharing of Personal Information

We do not sell Personal Information for money.

However, our use of certain advertising cookies, pixels, or similar technologies may be considered a “sale” or “sharing” of Personal Information under the CCPA or other U.S. state privacy laws.

California residents may opt out of such sale or sharing by:

- a. Using our cookie preference tool, if available;
- b. Clicking “Do Not Sell or Share My Personal Information” where provided;
- c. Enabling Global Privacy Control in a supported browser;
- d. Contacting us at contact.us@4everi.com

15.5. Sensitive Personal Information

We do not use or disclose Sensitive Personal Information for purposes that require a right to limit under the CCPA, unless otherwise disclosed at the time of collection or permitted by law.

Customers should avoid uploading Sensitive Personal Information unless necessary and lawful.

15.6. California Privacy Rights

California residents may have the right to:

- a. Know what Personal Information we collect, use, disclose, sell, or share;
- b. Access Personal Information;
- c. Delete Personal Information;
- d. Correct inaccurate Personal Information;
- e. Opt out of sale or sharing;
- f. Limit certain uses of Sensitive Personal Information;
- g. Not be discriminated against for exercising privacy rights.

To exercise these rights, contact us at contact.us@4ever.com

We may need to verify your identity before responding. If your request relates to Customer Data, we may direct you to the Customer that controls that data.

15.7. Authorized Agents

California residents may designate an authorized agent to submit requests on their behalf. We may require proof of authorization and identity verification.

16. Other U.S. State Privacy Rights

Residents of certain U.S. states, such as Colorado, Connecticut, Virginia, Utah, Texas, Oregon, Montana, Delaware, Iowa, Tennessee, Indiana, and others, may have additional privacy rights under applicable laws.

Depending on your state, these rights may include:

- a. Right to access;
- b. Right to correct;
- c. Right to delete;
- d. Right to data portability;
- e. Right to opt out of targeted advertising;
- f. Right to opt out of sale of Personal Information;
- g. Right to opt out of certain profiling;
- h. Right to appeal a privacy rights decision.

To exercise applicable rights, contact us at contact.us@4everi.com

17. Candidate and Applicant Privacy

Our Customers may use the Services to process Candidate Data. If you are a Candidate whose resume, profile, or other information has been uploaded to the Services by one of our Customers, that Customer is generally responsible for determining how your information is used.

You should contact the relevant Customer directly to:

- a. Access your Candidate Data;
- b. Correct inaccurate information;
- c. Request deletion;
- d. Object to processing;
- e. Ask about hiring decisions;
- f. Request information about AI-assisted analysis;
- g. Withdraw consent, where applicable.

If you contact us directly about Customer Data, we may refer your request to the relevant Customer or assist the Customer in responding, as required by applicable law and our agreements.

18. Customer Responsibilities

Customers are responsible for:

- 18.1.** Providing all required privacy notices to candidates, employees, contractors, job applicants, and other individuals;
- 18.2.** Obtaining all required consents and authorizations;
- 18.3.** Establishing lawful bases for Processing;
- 18.4.** Ensuring that uploaded data is accurate, lawful, and not excessive;
- 18.5.** Complying with employment, recruitment, anti-discrimination, privacy, AI, data protection, consumer protection, and other applicable laws;
- 18.6.** Reviewing AI outputs before relying on them;
- 18.7.** Configuring public pages and sharing settings appropriately;
- 18.8.** Ensuring they have rights to publish or share Customer Data;
- 18.9.** Responding to data subject and consumer rights requests;
- 18.10.** Maintaining confidentiality of account credentials;
- 18.11.** Ensuring that authorized users comply with applicable terms and laws.

Customers agree not to upload or process information through the Services unless they have all necessary rights, permissions, consents, and lawful bases.

19. Children's Privacy

The Services are not intended for children under the age of 16, and we do not knowingly collect Personal Information from children under 16.

Customers must not upload information about children unless they have all necessary legal rights and consents and the use is permitted under applicable law.

If we learn that we have collected Personal Information from a child in violation of applicable law, we will take appropriate steps to delete it.

20. Marketing Communications

We may send marketing communications to Customers, prospective customers, and business contacts where permitted by law.

You may opt out of marketing emails by using the unsubscribe link in the email or contacting us at contact.us@4everi.com

Even if you opt out of marketing communications, we may still send non-marketing messages, such as:

- a. Account notices;
- b. Subscription notices;
- c. Security alerts;
- d. Legal updates;
- e. Support communications;

- f. Transactional messages;

21. Third-Party Links and Services

The Services may contain links to third-party websites, integrations, APIs, platforms, or services. This Privacy Policy does not apply to third-party services that we do not control.

We are not responsible for the privacy, security, or content practices of third parties. You should review their privacy policies before using third-party services.

22. Aggregated, De-Identified, and Anonymized Data

We may create, use, disclose, and retain aggregated, de-identified, or anonymized data for purposes such as:

- a. Analytics;
- b. Benchmarking;
- c. Product development;
- d. AI performance evaluation;
- e. Research;
- f. Marketing;
- g. Security;
- h. Business intelligence.

We will not attempt to re-identify de-identified or anonymized data except as permitted by law, such as to test de-identification measures or comply with legal obligations.

23. Data Processing Agreements

Where required by applicable law, we may enter into a Data Processing Agreement or similar agreement with Customers. Such agreements may include provisions addressing:

- a. Processor obligations;
- b. Customer instructions;
- c. Confidentiality;
- d. Subprocessors;
- e. Security measures;
- f. International transfers;
- g. Assistance with data subject requests;
- h. Deletion or return of Customer Data;
- i. Audits or compliance information.

If there is a conflict between this Privacy Policy and a signed Data Processing Agreement, the Data Processing Agreement will control to the extent of the conflict.

24. Subprocessors

We may use subprocessors to provide the Services, including cloud hosting providers, AI providers, analytics providers, communication vendors, and support tools.

We may update our subprocessors from time to time. Where required by law or contract, we will provide notice of new subprocessors and an opportunity to object.

A current list of subprocessors may be available upon request at contact.us@4everi.com

25. Retention and Deletion of AI Inputs and Outputs

AI inputs and outputs may be retained as part of Customer Data, logs, audit records, backups, or system records.

Customers may request deletion of Customer Data according to account settings, applicable agreements, or by contacting support. Deletion from active systems may not immediately delete information from backups, logs, or archival systems, but such information will be deleted or isolated according to our standard retention practices unless retention is required by law.

Third-Party AI Providers may retain data according to their own applicable terms, privacy policies, API data processing terms, or abuse-monitoring policies. We use commercially reasonable efforts to configure AI Provider settings to limit retention and secondary use where available and appropriate.

26. Employment, Recruitment, and Anti-Discrimination Compliance

Our Services may be used in employment, recruitment, staffing, contracting, or workforce-related contexts. Customers are solely responsible for ensuring their use of the Services complies with all applicable laws, including:

- a. Employment laws;
- b. Equal opportunity and anti-discrimination laws;
- c. Background check laws;
- d. AI hiring tool laws;
- e. Notice and consent requirements;
- f. Data protection laws;
- g. Recordkeeping obligations;
- h. Candidate access and correction rights.

We do not guarantee that AI outputs, candidate ratings, matching scores, or recommendations are free from error or bias. Customers must conduct appropriate human review and validation.

27. Limitation Regarding Customer Data

We do not control the content of Customer Data uploaded by Customers. Customers are solely responsible for the legality, accuracy, quality, integrity, and appropriateness of Customer Data.

To the maximum extent permitted by law, Company and its affiliates, officers, directors, employees, contractors, agents, and representatives are not responsible for claims arising from:

- a. A Customer's failure to provide required notices or obtain required consents;
- b. A Customer's unlawful upload, processing, publication, or sharing of Personal Information;
- c. A Customer's use of AI outputs;
- d. A Customer's employment, hiring, or contracting decisions;
- e. Personal Information included in resumes, contracts, documents, or other files uploaded by Customers;
- f. Public disclosure resulting from Customer-enabled sharing or publication settings;
- g. Third-party use of publicly accessible information.

Nothing in this Privacy Policy limits rights that cannot be limited under applicable law.

28. Changes to This Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our Services, technologies, legal requirements, business practices, or other reasons.

When we update this Privacy Policy, we will revise the "Last Updated" date above. Where required by law, we will provide additional notice or obtain consent for material changes.

Your continued use of the Services after an updated Privacy Policy becomes effective means that you acknowledge the updated Privacy Policy.

29. Contact Us

If you have questions, requests, or concerns about this Privacy Policy or our privacy practices, please contact us at: contact.us@4everi.com