Privacy Statement

Visibility HR · visibilityhr.com and the Visibility HR platform

Effective date: January 1, 2027 · Replaces the Privacy Statement effective October 1, 2026 and the Data Security and Privacy Statement dated August 1, 2021

Visibility HR, LLC, 1215 Friend Street, Newberry, South Carolina 29108, provides the Visibility HR website and platform. On January 1, 2027, Visibility Software, L.L.C. merged into Visibility HR, LLC, which continues its business. In this statement, "we" and "us" mean Visibility HR, LLC.

We handle two very different kinds of personal information, and this statement is organized around that difference. Part 1 covers what happens when you visit our website, fill out a form, or talk to us about working together. Part 2 covers the Visibility HR platform: the recruiting, onboarding, and training management software our clients use to hire and develop their people. In the platform, the information belongs to our client and the people who applied to or work for that client. We process it on the client's instructions and do not use it for our own purposes.

If you applied for a job or completed onboarding or training through a careers page or portal that one of our clients runs on our platform, that client is responsible for your information. Their privacy notice governs, and requests about your information should go to them. Part 2 explains what we do on their behalf and how we can help you reach them.

Part 1 — Our website and our business relationship with you

1.1 What we collect

When you visit visibilityhr.com we receive the technical information any website receives: IP address, browser and device type, pages viewed, the page that referred you, and the date and time of your visit. We use cookies and similar technologies for the site to function, to remember your preferences, and to understand how the site is used. At launch, the site uses Webflow site analytics and Google Analytics 4. We also use the LinkedIn Insight Tag for conversion measurement only, to learn whether a visit from a LinkedIn ad led to a form submission; we do not use it to build advertising audiences or to retarget visitors.

When you fill out a form, request a Talent Improvement Session, register for a webinar, download a resource, or subscribe to updates, we collect what you give us: typically your name, work email, phone number, company, title, and the area you want to talk about. When you become a client, we also hold the contact and billing information needed to run the account.

1.2 How we use it

We use this information to respond to you, to deliver the session or resource you asked for, to run and improve the website, to send updates you have asked for or that relate to a service you use, and to keep records of our business relationship. We keep contact and account information in our customer relationship system (EngageBay) and our email and calendar systems (Microsoft 365).

We do not sell personal information. We do not share it with third parties for their own marketing. We do not buy or rent contact lists.

1.3 Marketing choices

Every marketing email we send includes an unsubscribe link, and we honor requests within ten days. You can also write to us at the address in Section 3.5. Unsubscribing from marketing does not stop service messages about an account you hold with us.

1.4 Who else sees it

Service providers that run our website, hosting, analytics, email, CRM, scheduling, and webinar tools see personal information only as needed to provide those services to us, under contracts that restrict their use of it. We disclose information when the law requires it, to protect our rights or safety or those of others, and to a successor in a merger or reorganization of our business, who takes it subject to this statement.

1.5 How long we keep it

We keep website form and contact information for as long as we have an active conversation or business relationship with you and for a reasonable period afterward for our records, then delete or anonymize it. You can ask us to delete it sooner (Section 3.2).

Part 2 — The Visibility HR platform

2.1 Our role

Our clients use the platform to publish jobs, receive applications, screen and communicate with candidates, complete new-hire paperwork, and assign and track training. The people whose information is in the platform are the client's applicants, candidates, employees, contractors, and volunteers. The client decides what information to collect, why, how long to keep it, and who at the client can see it. In privacy-law terms, the client is the controller or business and we are the processor or service provider. We act only on the client's documented instructions, which are set out in our Subscription Agreement and this statement.

2.2 What the platform holds

What is collected depends entirely on how the client configures its careers page, application, onboarding forms, and training records. It can include contact details, work and education history, resumes and cover letters, answers to application questions, references, interview recordings or notes, eligibility and identification documents used for onboarding (such as I-9 supporting documents), tax and payroll setup forms, emergency contacts, and training assignments, completions, scores, and certifications. Some clients collect information that is sensitive, such as Social Security numbers, dates of birth, self-identification for equal-opportunity reporting, or accommodation requests. We tell clients to collect only what they need and to review the legal requirements for anything sensitive, and we provide field-level controls to limit it.

2.3 Screening questions and knockout rules

The platform lets a client write its own application questions, assign points to answers, and choose whether a particular answer removes an applicant from the active process for that position. We want to be plain about how this works. The client writes the questions, chooses the answers, sets the points, and

decides which answers, if any, end the process. The platform applies those rules exactly as written. It does not score, rank, or reject applicants using artificial intelligence, machine learning, or any model we built or trained. An applicant removed by a client's rule receives a status the client selects, stays in the system attached to the position, and remains visible to the client, which can review and reverse the result at any time. Whether a client's screening questions comply with employment and anti-discrimination law, and whether any notice is owed to applicants where the client hires, is the client's responsibility; we provide the controls and the audit history to support it.

2.4 Resume parsing and other automated features

When a candidate uploads a resume, the platform may use a parsing service to read it and fill in application fields so the candidate does not have to retype them. Parsing extracts text; it does not evaluate the candidate. Candidates can review and correct what was filled in. The platform also automates routine steps a client configures, such as acknowledgment emails, interview scheduling messages, onboarding task reminders, and training due-date notices. None of these makes a hiring, employment, or training decision. Some features use an artificial-intelligence service to help a client's users draft or summarize content, such as job description summaries, requisitions, interview questions, and applicant summaries. These produce drafts for a person to review. They do not score, rank, classify, or recommend any applicant, and the client decides whether and how to use them.

2.5 Service providers we use (subprocessors) and services a client turns on

We use a small number of service providers to operate the platform for every client. Each is bound by a written contract to use client data only to provide its service to us and to protect it. As of the effective date they are:

Provider	What it does	Where data is processed
Amazon Web Services (AWS)	Hosting, storage, and backups for the platform	United States (primary east-coast region; backups in a west-coast region)
Amazon Simple Email Service (SES)	Delivery of platform email to candidates, employees, and client users	United States
Affinda	Resume parsing: reads an uploaded resume and fills application fields	North America
Hireflix	One-way video interviews, when a client enables them	Spain (European Union)
OpenAI	AI-assisted drafting and summaries described in Section 2.4, when a client uses those features	United States

This list is also published at https://visibilityhr.com/terms. We will post changes there and notify clients through the update subscription on that page at least 30 days before a new subprocessor handles client data, so a client can raise an objection under its agreement with us.

Clients can also choose to connect the platform to other services. These providers are not our subprocessors: the client chooses them and works with them under its own agreement, and data goes

to them only for that client and only when the client turns the service on. We list them here so clients have one place to see where platform data can go.

Service	What it does	Whose agreement
Indeed	Job distribution and Indeed Apply, when a client enables it	The client's own agreement with Indeed
Screening partners (for example, Verified First)	Background and exclusion-list screening the client orders through the platform; the report stays in the partner's system	The client's own agreement with the partner
Other job boards	Posting jobs to boards the client selects	The client's own agreement with each board
Client-specific integrations	A connection we build for one client to that client's chosen system, such as its HR or payroll system, named in that client's Order Form or statement of work	The client's own agreement with that provider

2.6 What we do and do not do with client data

We use client data only to provide, support, secure, and improve the platform for that client, and as the client's agreement with us permits. We do not sell it, use it to market to candidates or employees, combine it across clients to build profiles, or use it to train artificial-intelligence models, and our AI provider does not use client data sent through its API to train its models. We may produce aggregated, de-identified statistics (for example, average time-to-fill across all clients) that cannot reasonably be used to identify a client, a candidate, or an employee.

2.7 Security

We maintain administrative, physical, and technical safeguards designed to protect client data, including encryption in transit, encrypted password storage, multi-factor authentication for administrative access, network firewalls and intrusion detection, role-based access within the platform, logging, and rolling fourteen-day backups stored in a separate west-coast region. A short Security Overview is published at visibilityhr.com/security. A more detailed description of our controls is available to clients on request. No system is perfectly secure; clients control their own users' access and are responsible for keeping credentials confidential.

2.8 If something goes wrong

If we confirm a security incident that has resulted in unauthorized access to, disclosure of, or loss of client data, we will notify the affected client without undue delay and in any event within 48 hours of confirming it, with what we know, what we have done, and what we recommend. The client is responsible for any notice owed to its applicants or employees or to regulators; we will support the client with the information it needs to make those notices.

2.9 How long client data stays in the platform

During the subscription, the client controls retention and can delete records at any time using the platform's tools. Within ten days after a subscription ends, a client may request an export of its data,

which we deliver in a standard format. We delete the client's database, including all applicant and employee records, from our production environment within 30 days after the subscription ends, and from backups within 180 days after that, except where the law requires us to keep something longer.

2.10 Requests from applicants and employees

If you want to access, correct, or delete information about you in a client's system, or to ask how it has been used, please contact the employer you applied to or work for. Their notice tells you how. If you contact us instead, we will tell you which client holds your information and pass your request to them; we cannot act on it ourselves without the client's instruction, because the information is theirs. We support clients' responses to these requests with the platform's export, correction, and deletion tools.

Part 3 — Terms that apply to everyone

3.1 Your state privacy rights

Depending on where you live, state law may give you rights to know what personal information a business holds about you, to correct or delete it, to obtain a copy, and to opt out of its sale or sharing. We do not sell or share personal information for cross-context behavioral advertising. If you are a California resident, the California Consumer Privacy Act applies to job applicant and employee information; for information in a client's platform account we act as the client's service provider, and your request should go to the client, which is the business responsible for it. For information we hold as a business in Part 1, contact us as described in Section 3.5 and we will respond within the time the law allows, after verifying your identity. We do not discriminate against anyone for exercising privacy rights.

3.2 Making a request to us

For information we hold under Part 1, you may ask us to tell you what we have, correct it, delete it, or stop sending you marketing. Write to the address in Section 3.5. We will confirm your identity using the email address on file and respond within 45 days, or tell you if we need longer and why.

3.3 Outside the United States

Our platform and our business operate in the United States, and client data is stored and processed here, with one exception: one-way video interviews, when a client enables them, are processed by our provider in Spain (see Section 2.5). Clients may not submit personal data that is subject to the EU General Data Protection Regulation, the UK GDPR, or Swiss data protection law unless we have signed a separate data processing addendum covering it. Individuals in those regions should direct requests to the client as described in Section 2.10.

3.4 Children

Our website and platform are for adults. Clients may not use the platform to knowingly collect personal information from anyone under 16 without a parent's or guardian's consent, and we do not knowingly collect it through our website. If we learn we have collected information from a child without appropriate consent, we will delete it.

3.5 How to reach us

Visibility HR, Attn: Privacy, 1215 Friend Street, Newberry, SC 29108 · privacy@visibilityhr.com · 1-800-914-9594.

3.6 Changes to this statement

When we change this statement, we will post the new version here with a new effective date and, for changes that affect how we handle client data in the platform, notify clients through the update subscription at https://visibilityhr.com/terms at least 30 days in advance. We will not make a change that materially reduces the protections for client data described in Part 2.