PRIVACY POLICY

Effective September 17, 2026

Table of Contents

Introduction....3
Data Protection Officer....3
EU & UK Representatives....3
Identifying the Data Controller and Processor....3
Your Rights Relating to Your Personal Data....4
Your Rights Under US State Privacy Laws....5
How to Exercise Your Rights....5
Personal Data We Collect....6
- Information You Provide to Us....6
- Information Received from Third Parties....7
- Information Collected Automatically....8
- Aggregated Data....8

Cookies and Controlling Their Use....8
- Change Your Cookie Preferences....9
- Third-Party Analytics....9
- Change Your Browser's Cookie Settings....10

How We Use Your Personal Data....10
Agency Performance Scoring....11
How Long We Keep Your Personal Data....11
Information Sharing and Disclosure....12
International Data Transfers....13
Who Processes Your Data, and Where....14
Data Security....15
Platform Security Monitoring....15
Policy on Children's Privacy....16
Links to Third-Party Websites....16
Updates to Our Privacy Policy....16

Introduction

This Privacy Policy describes how RecruitiFi Inc. collects, uses, and discloses information, and what choices you have with respect to the information.

When we refer to "RecruitiFi," "we," or "us," we mean the entity (RecruitiFi Inc.) that operates www.RecruitiFi.com (the "Service") and acts as the processor and controller of your information in different scenarios, as explained in more detail in the "Identifying the Data Controller and Processor" section below. RecruitiFi has many different parties that may use the service in different ways. We may refer to "Employers," "Recruiters," "Candidates," and "Website Visitors" as specific cases that apply only to that party or their relevant business entities, but collectively, they may be referred to as "Users" or "you."

Data Protection Officer

We are committed to educating users about their rights and resolving complaints regarding your privacy and our collection or use of your personal information. RecruitiFi has appointed a Data Protection Officer, Norm Clausen. To communicate with our Data Protection Officer, please email dpo@recruitifi.com or via post at: RecruitiFi, Inc. 21 West 46th St. New York, NY 10036.

EU & UK Representatives

RecruitiFi, Inc. is established outside the European Economic Area and the United Kingdom and has appointed representatives under Article 27 of the EU GDPR and Article 27 of the UK GDPR. You may contact either representative on all matters relating to the processing of your Personal Data, in addition to or instead of contacting our Data Protection Officer.

EU representative: Instant EU GDPR Representative Ltd (Company No. 665191), Office 2, 12A Lower Main Street, Lucan, Co. Dublin, K78 X5P8, Ireland. Email contact@gdprlocal.com. Telephone +353 (0)1 554 9700.

UK representative: GDPR Local Ltd (Company No. 12969035), 1st Floor Front Suite, 27-29 North Street, Brighton, England, BN1 1EB. Email contact@gdprlocal.com. Telephone +44 (0)1772 217800.

Identifying the Data Controller and Processor

Data protection law in certain jurisdictions differentiates between the "Controller" and "Processor" of information. In general, RecruitiFi, a US company based in New York City, New York, does not own, control, or direct the use of Candidate data. RecruitiFi acts as the Processor of Candidate data in accordance with the Controller's documented instructions. For a Candidate submission, the Controllers are the Recruiter's Agency, which determines the purposes and means of

submitting the Candidate, and the Employer, which is a separate and independent Controller of Candidate data for its own hiring purposes. A Candidate is the data subject of that processing, not its Controller. RecruitiFi asserts no legal basis of its own for this processing, processes it only under an Article 28 data processing agreement with each Controller, and is not a joint controller with either of them.

In circumstances where Users provide personal information via the platform both actively and passively (such as name, e-mail address, IP address, company affiliation, or similar personally identifying data), RecruitiFi is the data Controller of such personal information. Where RecruitiFi is the data controller of such information, it will comply with all associated responsibilities under EU Law or any other applicable data privacy law.

In general, requests to exercise any of your rights regarding Personal Data below should be directed to RecruitiFi. Unless otherwise noted in this Privacy Policy, required by law, or you are otherwise notified by RecruitiFi that additional steps must be taken, RecruitiFi will handle Personal Data requests with any Controllers or Processors affiliated with the platform.

RecruitiFi is the independent Controller of the following activities, which it carries out for its own purposes and not on anyone's instructions: (a) platform account administration for Employer and Agency users; (b) platform security, fraud prevention, and service-integrity monitoring; (c) the handling of data subject requests addressed to RecruitiFi in respect of processing for which it is Controller; (d) the evaluation and scoring of Agency users; (e) payment administration, being the collection of Employer fees and the payment of Agencies for placements; and (f) analytics on our marketing website, subject to your cookie consent. Each is described in this Privacy Policy, and RecruitiFi relies on its own legal basis for each.

Your Rights Relating to Your Personal Data

Individuals in certain countries have statutory rights regarding data that enables personal identification ("Personal Data"). In many cases, hiring data must be kept on file in accordance with various international regulations. Except where RecruitiFi is legally obligated to retain certain data, you have the right under this Privacy Policy, and by law if you are within a jurisdiction that mandates the following, to:

- **Request access to your Personal Data.** If you are in the EU, you can request a copy of the Personal Data we hold about you and verify that we are lawfully processing it.
- **Request correction of the Personal Data that we hold about you.** This enables you to have any incomplete or inaccurate information we hold about you corrected.
- **Request erasure of your Personal Data.** This enables you to ask us to delete or remove Personal Data where there is no good reason for us to continue processing it. You also have the right, if you are within the EU, to ask us to delete or remove your Personal Data where you have exercised your right to object to processing (see below). When we process an

© 2026 RecruitiFi, Inc.

erasure request, your Personal Data is immediately removed from active use. Backup copies are held in immutable, encrypted, access-restricted storage that cannot be altered before their retention period expires, so those copies persist until their retention period expires and are then destroyed; a record deleted at your request is re-suppressed if a backup is ever restored. We will tell you what was deleted, what is retained, and why.

- **Object to processing of your Personal Data.** This right applies when we rely on a legitimate interest as the legal basis for our processing, and there is something about your situation that makes you want to object to the processing of your Personal Data on this ground.
- **Request the restriction of processing of your Personal Data.** This enables you to ask us to suspend the processing of your Personal Data, for example, if you want us to verify its accuracy or the reason for processing it.
- **Request the transfer of your Personal Data.** If you are within the EU, we will provide your Personal Data, or that of a third party you have chosen, to you or to a third party you have chosen in a structured, commonly used, machine-readable format.
- **Withdraw consent.** This right only applies where we rely on your consent to process your Personal Data ("Consent Withdrawal"). If you withdraw your consent, we may not be able to provide you with access to certain specific functionalities of our platform. We will advise you if this is the case when you withdraw your consent.

Exceptions to the data rights above apply to areas where RecruitiFi is required to retain data under a separate legal statute, and that statute takes precedence over the data rights mentioned above. For example, anti-discrimination laws in many countries require retaining data for a minimum period equal to the statute of limitations for any potential discrimination claim. Data may not be deleted before the conclusion of this period, regardless of the data subject's requests.

If you have questions about specific retention and deletion rights as they pertain to your situation and jurisdiction, you can contact us as outlined in "How to Exercise Your Rights" below.

Your Rights Under US State Privacy Laws

If you are a resident of California or of another US state with a comprehensive privacy law, you may have the right to know what Personal Data we have collected about you and the categories of sources, purposes and recipients; to obtain a copy of it; to correct inaccurate Personal Data; to request deletion; to opt out of the sale or sharing of Personal Data for cross-context behavioral advertising; to limit our use and disclosure of sensitive personal information; and, in some states, to appeal a decision we make on your request.

We do not sell Personal Data, and we do not share Personal Data for cross-context behavioral advertising. We do not use or disclose sensitive personal information for any purpose other than those permitted without a right to limit.

© 2026 RecruitiFi, Inc.

Where we process Personal Data on behalf of an Employer or an Agency, we act as that party's service provider or contractor. We process it only to perform the services and for the business purposes set out in our agreement with them, and we do not retain, use or disclose it for any other purpose, combine it with data from other sources except as the CCPA permits, or sell or share it.

We will not discriminate against you for exercising any of these rights. To exercise them, use the contact routes in "How to Exercise Your Rights" above. You may use an authorized agent, and we may ask the agent for proof of your authorization. If we decline a request, we will tell you why and, where applicable law provides an appeal, how to appeal.

How to Exercise Your Rights

If you want to exercise any of the rights described above or lodge a complaint regarding this Privacy Policy, please use our data subject request form or email our Data Protection Officer directly at: dpo@recruitifi.com. We respond to requests within one month of receipt. Where a request is complex or where we have received several requests from you, we may extend that period by up to two further months, and we will tell you of the extension and the reasons for it within one month of receipt. Where the Personal Data in question is processed by us as a Processor on the instructions of an Employer or an Agency, we do not respond to the request ourselves, other than to acknowledge receipt and to tell you who the Controller is; we forward the request to that Controller promptly and assist them in answering it. You may use an authorized agent to submit a request on your behalf where permitted by applicable law, and we may ask the agent for proof of your authorization. We may need to request specific information from you to help us confirm your identity and ensure your right to access your Personal Data (or to exercise any of your other rights). This is a security measure to ensure that Personal Data is not disclosed to anyone who does not have the right to receive it. We may also contact you to request further information regarding your request to expedite our response.

If you feel that a complaint has not been adequately resolved, you have the right to contact a data protection supervisory authority. If you are in the EU or EEA, you may contact your local supervisory authority; a list is available here. For transfers under our Standard Contractual Clauses, the competent authority is the one designated in the applicable data processing agreement or, in the absence of such a designation, the Irish Data Protection Commission. If you are in the United Kingdom, you may contact the Information Commissioner's Office. If you are in Switzerland, you may contact the Federal Data Protection and Information Commissioner here. You may also contact our EU or UK representative named above.

Personal Data We Collect

RecruitiFi uses Personal Data we collect to provide our service, personalize content, remember information to help you efficiently access your account, make or receive payment for services

obtained through the RecruitiFi platform, administer temporary staffing engagements, including timesheets and assignment-duration notifications requested by Employers, analyze how our services are used, diagnose service or technical problems, maintain security, monitor aggregate metrics such as total number of visitors, traffic, and demographic patterns, and track User content and Users as necessary to comply with the OFCCP and EEOC regulations in addition to other applicable laws.

You do not have a legal obligation to provide us with any information, but you may have a contractual obligation to do so, and if we do not receive certain information from you, then we will not be able to provide our Service to you. If you have any questions regarding whether provision of information is mandatory and the consequences for withholding such information, please contact our Data Protection Officer.

This Personal Data and other information may be collected in a variety of manners, as listed below.

Information You Provide to Us

There are many occasions when you provide information directly to us as part of our services. The following types of information may be provided by you.

- **Contact Information:** In the course of using the Service, we may require or otherwise collect information that identifies you as a specific individual and can be used to contact or identify you. Examples include your name, email address, company address, phone number, a photo, or links to online profiles. Some of this information may be made viewable by other RecruitiFi users.
- **Payment Information:** If you use the Service to make or receive payments, we collect the information we need to administer those payments. If you are an Employer, that is the billing contact details and billing address we use to invoice you and to record your fee payments; Employers pay us by bank transfer, and we do not collect or hold Employer card or bank account details. If you are an Agency user we pay, your bank account details and tax information are collected by our payment provider directly from you through its own onboarding process, and we do not receive them; we hold only the account reference that provider assigns to you, the amounts we owe and pay you, and the record of those transactions.
- **Temporary Engagement Data:** If a Candidate is engaged as a Resource under our temporary staffing service, we process the Statement of Services terms for that engagement (start date, anticipated length of engagement, bill rates, and description of work), the weekly timesheet records of hours worked that the Resource's staffing firm submits and the Employer approves, assignment status, and assignment-duration data we derive from those records, including the Resource's cumulative time on assignment with an Employer measured from the first assignment recorded on the platform. We process this data as a Processor on the documented instructions of the Employer and the staffing firm: to

© 2026 RecruitiFi, Inc.

administer the engagement, to invoice and pay for hours worked, and, where an Employer uses the feature, to notify the Employer when a Resource's cumulative assignment duration approaches a threshold set under the Employer's own policies. RecruitiFi does not set tenure limits and makes no decisions about a Resource's engagement.

- **Identity Verification:** Identity verification for payouts, including any identity document, date of birth or taxpayer identification number required for know-your-customer, anti-money-laundering or tax reporting purposes, is carried out by our payment provider directly with you, under its own privacy notice. We do not collect, receive or hold that information.
- **Non-Identifying Information:** We also may collect other information, such as zip codes, demographic data, information regarding your use of the Service, and general JobCast-related data ("Non-Identifying Information"). We may aggregate Non-Identifying Information collected from RecruitiFi Users.
- **Content Data:** Any content you post to the Services not already included in another category, including without limitation, your profiles, questions, answers, messages, comments, ratings, feedback, and other contributions on the Services, and metadata about them (such as when you posted them) ("Content").
- **Marketing and Communications Data:** Your preferences in receiving marketing from us and our third parties and your communication preferences. If you correspond with us by email or messaging through the Services, we may retain the content of such messages and our responses.
- **Special Categories of Personal Data:** You may be asked to provide certain categories of data that are considered special under statutes such as the GDPR in the EU or the CCPA in California. These fields are presented only for roles based in the United States, so that an Employer can meet its EEOC and OFCCP recordkeeping obligations. They are keyed to the role's location and are not presented for roles based in the EEA, the United Kingdom, or Switzerland. Completion is entirely optional and has no effect on how your submission is considered. Where you do complete them, the responses are processed solely for that recordkeeping purpose. Where data of this kind is collected through these fields from an individual to whom the GDPR applies, we rely on explicit consent under Article 9(2)(a) as the condition that lifts the prohibition on processing. The fields cover racial and ethnic background, disability status, and veteran status. We do not collect any other special category or criminal offense data by design, and Employers and Agencies are instructed not to submit such data through any other field; incidental mentions in a resume or a free-text answer are not solicited.
- **Hashed Information:** In some cases, we may render Personal Data into a form of Non-Identifying Information referred to in this Privacy Policy as "Hashed Information." This is typically accomplished using a mathematical process (commonly known as a hash function)

© 2026 RecruitiFi, Inc.

to convert information into a code. The code does not identify you directly, but it may be used to connect your activity and interests.

Information Received from Third Parties

As RecruitiFi engages in the submission of Candidates to Employers by Recruiters, some elements of Personal Data are presented to RecruitiFi and other Users by third parties as a designed part of the Service. We may also integrate with or receive information from third-party services that may constitute Personal Data.

- **Professional Information:** Your name, email, phone number, professional history, resume/CV, work references, and other professional information (typically provided by a Candidate) may be provided to RecruitiFi by a third party (typically a Recruiter). Using the available contact information, you will be notified that this information has been provided to RecruitiFi and by whom. Your professional information can be updated by you and deleted where legally allowed. It is not disclosed to an Employer until you have reviewed the submission and confirmed it for that specific job, and you may withdraw from consideration at any time. Once you have confirmed a submission, that Employer receives your information as an independent Controller and may disclose it to its own service providers and vendors in connection with filling the role, including for background checks.
- **Analytics Platforms:** We use Google Analytics on our marketing website to understand how visitors use it. Google Analytics sets cookies and receives your IP address, device and browser metadata, and page interaction and referral data. For visitors from the European Economic Area and the United Kingdom, this information is not collected unless and until you consent through our cookie consent tool; for visitors from the United States, it is collected on an opt-out basis as described under “Change Your Cookie Preferences” below. It is not joined to your platform account data, and it is not shared with any additional third parties.
- **Miscellaneous Third-Party Info:** We may also receive information about you from third parties if you choose to sign in with a third-party service or link to an outside service. If we combine the information we receive from third parties with information we collect through the Service, we will treat the combined information as described in this Privacy Policy.

Information Collected Automatically

Like other online companies, we receive technical information when you use our Services. We use these technologies to analyze how people use our Services, to improve how our platform functions, and to save your log-in information for future sessions.

- **Browsing Information:** We and our third-party service providers, including analytics and third-party content providers, may automatically collect certain information from you whenever you access or interact with the Service. This information may include, among other information, the browser and operating system you are using, the URL or

© 2026 RecruitiFi, Inc.

advertisement that referred you to the Service, the search terms you entered into a search engine that led you to the Service, areas within the Service that you visited, and other information commonly shared when browsers communicate with websites. We may automatically combine this log information with other information we collect about you. We do this to improve the services we offer you and to enhance marketing, analytics, and site functionality.

- **Device Identifiers:** The information we collect also includes the Internet Protocol ("IP") address or other unique device identifier ("Device Identifier") for any device (computer, mobile phone, tablet, etc.) used to access the Service. A Device Identifier is a number that is automatically assigned or connected to the device you use to access the Service, and our servers identify your device by its Device Identifier. Some mobile service providers may also provide our third-party service providers or us with information regarding the physical location of the device used to access the Service.
- **Cookies:** Covered in more depth below in the "Cookies and Controlling Their Use" section.

Aggregated Data

We may also collect, use, and share "Aggregated Data" such as statistical or demographic data for any purpose. Aggregated Data may be derived from your Personal Data, but once in aggregated form it will not constitute Personal Data for the purposes of the GDPR or CCPA as this data does not directly or indirectly reveal your identity. However, if we combine or connect Aggregated Data with your Personal Data so that it can directly or indirectly identify you, we treat the combined data as Personal Data and will use it in accordance with this Privacy Policy.

Cookies and Controlling Their Use

RecruitiFi uses cookies and similar technologies (small data files, browser local storage, and embedded scripts) to operate the Service, remember your choices, measure how our marketing website is used, and support visitors through our website chat. We do not use cookies for targeted advertising, and we do not permit third parties to advertise to you through the Service. On www.recruitifi.com, cookies and similar technologies fall into four categories:

- **Essential:** required for the website and the consent tool itself to function — for example, the cookie that records your consent choices (fs-consent, 180 days) and the cookie used to determine which consent options to show you (country). These are always active. The logged-in platform also sets cookies that are strictly necessary to authenticate you and keep your session secure; those are governed by the Terms of Service.
- **Analytics:** measure how visitors use our marketing website so we can improve it. We use Google Analytics 4 for this purpose (cookies _ga and _ga_6KCTRNWEM7, duration 2 years).
- **Personalization:** power the support chat on our website (Intercom) and remember your preferences (cookies intercom-id-gkaz0pgq, intercom-session-gkaz0pgq and

intercom-device-id-gkaz0pgq, and equivalent browser storage, durations 1 week to 9 months).

- **Marketing:** attribute visits that reach us from third-party review sites (G2). This uses an embedded script only; it sets no cookie on your device. We do not use targeted-advertising cookies.

The complete, current list of the cookies and similar technologies in each category — the name, type, provider, purpose, and duration of each — is published in our Cookie Notice, which is published at https://www.recruitifi.com/legal/cookie-notice and available from the cookie preference center on our website. We update the Cookie Notice as our tooling changes, without amending this Privacy Policy.

Change Your Cookie Preferences

How we ask for your permission depends on where you are visiting from. If you are in the European Economic Area or the United Kingdom, no cookies other than essential cookies are set unless and until you allow them through the consent banner; you can accept all categories, reject all, or make a per-category choice, and each option is equally available. If you are visiting from the United States, non-essential categories are active by default and you can opt out at any time, in full or per category. We also honor the Global Privacy Control (GPC) browser signal: if your browser sends GPC, we automatically treat it as an opt-out of non-essential cookies and, for the purposes of US state privacy laws, as a request to opt out of the "sale" or "sharing" of Personal Data (although, as stated above, we do not sell or share Personal Data).

You can review or change your choices at any time using the Preferences button in the bottom-left corner of every page of our website. Your choice is stored for 180 days, after which we ask again. Withdrawing consent stops the affected cookies from being set or read from that point onward; it does not remove cookies already on your device, which you can delete through your browser settings as described below.

Please note that some cookies are essential to certain parts of the Service and blocking them may limit your ability to use your account. For example, you may not be able to log in to private areas of the site or access your account.

Third-Party Analytics

We use Google Analytics 4 to understand how visitors use our marketing website. It loads only where permitted under the consent model described above. We configure it through Google Consent Mode, with all advertising signals denied: it is used for measurement only, is not used for advertising, and is not linked to your platform account data. We have set data retention in Google Analytics to the shortest period Google offers (currently two months). Google's use of the information is governed by its own privacy policy.

Change Your Browser's Cookie Settings

Most web browsers allow some control over most cookies through their settings. Many of the cookies set by RecruitiFi can be deleted or blocked in your web browser, but some of them are necessary for the Services to function properly. To find information relating to other browsers, visit the browser developer's website.

How We Use Your Personal Data

RecruitiFi uses Personal Data to deliver and improve our Services; to manage your account and provide you with customer support; to analyze Users' use of the Services; website and marketing site analytics, subject to your cookie consent; to diagnose or fix technology problems; to automatically update the Services on your device; to verify your identify and prevent fraud or other unauthorized or illegal activity; to enforce or exercise any rights in our Terms.

For each purpose for which we use your Personal Data, the GDPR, CCPA, and other similar local privacy acts require us to have a legal basis for that use. The legal bases depend on the Services you use and how you use them. This means we collect and use your Personal Data only where:

- You have consented for us to do so for a specific purpose;
- We need it to provide you the Services, including to operate the Services, provide customer support and personalized features, and to protect the safety and security of the Services;
- It satisfies a legitimate interest (which is not overridden by your data protection interests); or
- We need to process your data to comply with a legal or regulatory obligation.

We may also rely on your consent as a legal basis for using your Personal Data where we have expressly sought it for a specific purpose. You do have the right to revoke consent at any time; however, this will not affect any processing that has already taken place, and, depending on the situation, we may be required to retain data that has already been processed in accordance with local laws. The purposes for which we use Personal Data, and the legal basis for each, are as follows:

- **Platform security, fraud prevention and service-integrity monitoring**: to detect, prevent, investigate and respond to security threats, fraud and abuse, and to preserve the availability, integrity and confidentiality of the Service. Legal basis: our legitimate interests, Article 6(1)(f). See "Platform Security Monitoring" below.
- **Platform account administration**: to create and manage user accounts, authenticate users, provide support and administer the contractual service relationship with Employers and Agencies. Legal basis: performance of a contract, Article 6(1)(b).
- **Candidate submission and hiring workflow**: to distribute an Employer's requisitions to Agencies, receive Candidate submissions, obtain each Candidate's per-job confirmation, present confirmed Candidates to the Employer and support the resulting evaluation and

© 2026 RecruitiFi, Inc.

hiring workflow. For this purpose, we act as Processor on the instructions of the Agency and the Employer, who determine the legal basis.

- **Agency performance scoring**: to compute a performance score for each Agency user from records of their platform activity, so that Employers can make informed invitation decisions. Legal basis: our legitimate interests, Article 6(1)(f). See "Agency Performance Scoring" below.
- **Handling data subject requests**: to receive, verify, action and log requests to exercise data protection rights. Legal basis: compliance with a legal obligation, Article 6(1)(c).
- **Payment administration**: to invoice and collect Employer fees, to instruct our payment provider to pay Agencies for placements, and to keep our own financial records of those transactions. Legal basis: performance of a contract, Article 6(1)(b), and compliance with a legal obligation, Article 6(1)(c), for our own tax and financial records.
- **Marketing website analytics**: to measure and improve the performance of our marketing website. Legal basis: your consent, Article 6(1)(a), collected through our cookie consent tool.

Agency Performance Scoring

If you are a Recruiter or Agency user, the platform computes a performance score for you based on your activity records. Each Agency user is scored individually, so your score is Personal Data about you. Computing this score constitutes profiling within the meaning of Article 4(4) of the GDPR, and this section provides meaningful information about the logic involved and about the significance and the envisaged consequences of that profiling for you. Our legal basis is our legitimate interest in maintaining an efficient and trustworthy marketplace, under Article 6(1)(f) of the GDPR. We have carried out and documented a balancing assessment for this processing.

The inputs to the score are records of activity on the platform only: your submission activity, including submission speed and how far the Candidates you submit advance, as well as ratings provided by Employer users and by Candidates. We do not use external datasets, data enrichment, or inferred data. The formula is deterministic and documented, and changes to it are managed under our change control process. No artificial intelligence or machine learning is involved, and Candidates are not scored.

Scores and the rankings derived from them are advisory. They inform which Agencies an Employer considers inviting to a role, but a role is only ever shared with an Agency when an Employer user explicitly invites it. There is therefore no decision based solely on automated processing that produces legal or similarly significant effects for you within the meaning of Article 22 of the GDPR. The effect of scoring can be economic: a lower-scoring user may receive fewer invitations.

If you believe an input to your score is inaccurate, you may have it corrected through the data subject request process; we action corrections within 30 calendar days and recompute the affected score. You may also object to this processing under Article 21 of the GDPR by contacting

© 2026 RecruitiFi, Inc.

our Data Protection Officer. Each objection is assessed individually on your situation, and the outcome may include correcting inputs, recomputing your score, or restricting the processing while we assess the objection. We do not assume that our legitimate interests will override your objection.

How Long We Keep Your Personal Data

We keep Personal Data only for as long as we have a business need for it or to meet a regulatory or contractual requirement and then dispose of it securely. The periods below apply as at the effective date of this Privacy Policy.

Candidate and Employer data processed on the platform: retained for the duration of the relevant Employer's contract, then hard deleted from production systems within 60 days of the end of that contract, unless a legal hold applies. Deletion is performed programmatically in accordance with NIST SP 800-88 and is restricted to named authorized operators.

Records relating to a hiring decision: retained for two years where retention is required by law, for example recordkeeping obligations applicable to federal contractors under 41 CFR 60-1.12, or where needed to establish, exercise or defend legal claims.

Temporary engagement records, being Statements of Services, timesheet records, and derived assignment-duration data: retained for the duration of the relevant Employer’s contract as platform data, then hard deleted from production systems within 60 days of the end of that contract on the same basis as other platform data. The record of amounts invoiced and paid for those engagements is retained as a payment administration record as described below.

Account data for Employer and Agency users: retained for the duration of the contract, then placed in a programmatic deletion queue on termination unless a legal hold applies.

Agency performance scoring records, being each Agency user's computed score and the records of platform activity used as inputs to it: input records older than 24 months from the date of the underlying activity are no longer used to compute the score and are deleted from the scoring dataset; the current computed score is retained for the duration of the Agency user's account and is deleted with the account on closure.

General security event logs: one year from ingestion. Logs and evidence relating to a security incident: three years from the close of that incident.

Data subject request records: three years, reviewed quarterly by our Data Protection Officer.

Payment administration records include Employer billing contact details and billing addresses, the account reference our payment provider holds for each Agency we pay, and the record of amounts invoiced and paid for the duration of the relationship, plus the statutory tax and financial recordkeeping period that applies to us. We hold no bank account details, card details or tax identification data for any user.

© 2026 RecruitiFi, Inc.

Marketing website analytics data: for the retention period configured in our analytics tooling and the cookie lifetimes published in our cookie notice.

Backup copies: backups are immutable and encrypted and expire according to their assigned retention periods. A record deleted at your request is re-suppressed if a backup is restored.

Where we are required by law to retain Personal Data for longer than the periods above, we protect its confidentiality and process it only to the extent and for the period required by law.

Information Sharing and Disclosure

We may share information about you to provide the Services, for legal and investigative purposes, or in the event of a merger or acquisition. We may also share non-identifying information with third parties. You have a choice about whether we share your personal information with third parties for their own marketing purposes.

We may share aggregated Non-Identifying Information, and we may otherwise disclose Non-Identifying Information (including Hashed Information) to third parties. We may also share the information we have collected about you, including Personal Information, as disclosed at the time you provide your information, with your consent, as otherwise described in this Privacy Policy, or in the following circumstances:

- **Information Shared with Other Users:** Recruiters, Employers, and Candidates may have some of their Personal Data and any User Content shared with other Users to provide the Services. This may include Contact Information, Content Data, Special Categories of Personal Data, and Professional Information as covered in the section above, "Personal Data We Collect."
- **Service Providers:** We may employ third-party companies and individuals to facilitate our Service, to provide the Service on our behalf, to perform Service-related services (e.g., without limitation, maintenance services, database management, web analytics, payment processing, fraud detection and improvement of RecruitiFi features) or to assist us in analyzing how our Service is used. These third parties may have access to your Personal Information to perform these tasks on our behalf. They are identified individually in "Who Processes Your Data, and Where" below.
- **Legal and Investigative Purposes:** RecruitiFi will share information with government agencies as required by law in response to lawful requests by public authorities, including to meet national security or law enforcement requirements and, including without limitation, in connection with reporting earnings. We cooperate with government and law enforcement officials and private parties to enforce and comply with the law. We assess every legal demand we receive for its validity and its scope, and we notify our Data Protection Officer and Legal counsel on receipt. We disclose only the information specifically requested that we can reasonably locate, and we do not process overly broad or vague demands. On that

basis we will disclose information about you to government or law enforcement officials, or to private parties, where disclosure is required to respond to valid legal process (including but not limited to subpoenas), or where a governmental authority or other third party conducting an investigation makes a valid request and disclosure is necessary to (a) protect the property and rights of RecruitiFi or a third party, (b) protect the safety of the public or any person, or (c) prevent or stop activity that is, or poses a risk of being, illegal, fraudulent, unethical or legally actionable. We notify affected Employers and Agencies of a demand unless we are legally prohibited from doing so. We may use Device Identifiers to identify RecruitiFi Users where necessary for the purposes described in this section. We do not provide raw security telemetry to any external party; where disclosure is required, only redacted excerpts or summaries reviewed by our Security Officers are released.

- **Business Transfers:** Personal Data may be transferred as part of a merger, acquisition, reorganization, sale of all or substantially all of our assets, or bankruptcy, and may be disclosed under confidentiality obligations during due diligence with a potential acquirer. Any recipient remains bound by this Privacy Policy in respect of that data, or will give you notice and a choice before using it for a materially different purpose. We do not sell or rent Personal Data, and we do not sell or share Personal Data as those terms are defined in the CCPA. Personal Data that we process as a Processor on behalf of an Employer or an Agency may only be transferred in accordance with our data processing agreement with that Controller.

International Data Transfers

RecruitiFi is a U.S. company. If you are located outside the United States and choose to provide information to us, RecruitiFi transfers Personal Information to the United States for processing, and our service providers may process Personal Information in the United States and elsewhere. These countries may not have the same data protection laws as the country in which you initially provided the information. When we transfer your information to the United States, we will protect it as described in this Privacy Policy.

If we transfer Personal Data originating from the European Union, United Kingdom, or Switzerland to other countries not deemed adequate under applicable data protection law:

- Transfer safeguards: Every processor and sub-processor that processes Personal Data for us is engaged under a written data processing agreement that imposes data protection obligations no less protective than our own, and RecruitiFi remains fully liable for each sub-processor's performance of those obligations. For transfers of Personal Data from the European Economic Area, we rely on the 2021 Standard Contractual Clauses: Module Two where we act as Processor, Module Three where we act as sub-processor, and Module One where the transfer is between another Controller and us, as it is with the providers that pay Agency users in respect of the information they collect directly from those users, and Module Two where such a provider acts on our instruction to execute a payment. For

transfers from the United Kingdom, the 2021 Standard Contractual Clauses apply as amended by the UK International Data Transfer Addendum. For transfers from Switzerland, the 2021 Standard Contractual Clauses apply with the amendments required by the Swiss Federal Act on Data Protection, with the Federal Data Protection and Information Commissioner as the competent authority. Where a processor also holds a certification under the EU-US Data Privacy Framework, its UK Extension, or the Swiss-US Data Privacy Framework, the transfer to that processor is covered by the corresponding adequacy decision, or for United Kingdom transfers, the data bridge, for as long as that certification remains active, and our processor agreements are written on that basis. The Standard Contractual Clauses are incorporated in each of those agreements and stand behind the certification, taking effect if a certification lapses or an adequacy decision ceases to apply. Adequacy coverage extends to Personal Data within the scope of the processor's certification. We verify each certification against the published participant list to confirm the correct legal entity, and we maintain a transfer risk assessment for each recipient so we can rely on the Clauses if needed. To request more information about our transfer safeguards, contact our Data Protection Officer.

Who Processes Your Data, and Where

All platform processing takes place in the United States. The application and its managed databases are hosted in the United States (Virginia), with disaster recovery in the United States (Oregon). Our edge security and content delivery provider operates on a global network, so requests to our site may be inspected at an edge location outside the United States before reaching the platform.

We publish the full list of authorized sub-processors, stating for each one its legal entity name, the service it provides, the location of processing and the transfer safeguard relied on, at https://www.recruitifi.com/legal/sub-processors. The list carries a version number, an effective date and a change log, and superseded versions are retained and provided on request. As at the effective date of this Privacy Policy the authorized sub-processors are Salesforce, Inc. (Heroku) for application hosting and managed data stores; Amazon Web Services, Inc. for object storage, content delivery, key management and security monitoring; Cloudflare, Inc. for edge security, web application firewall and content delivery; Datadog, Inc. for centralized logging, security monitoring, in-application web application firewall, account-takeover monitoring, and intrusion detection and prevention; Stytch, Inc. for end-user authentication; and Intercom, Inc. for the in-platform support messenger and support communications.

We give at least 30 days' notice before a new sub-processor begins processing Personal Data, by publishing an updated list with a revised effective date and notifying Employers and Agencies through the platform or by email. An Employer or Agency with a reasonable, data-protection-based objection to a new sub-processor may object within the notice period. To subscribe to change notifications, contact dpo@recruitifi.com.

© 2026 RecruitiFi, Inc.

Separately, we engage the following providers for our own purposes as a Controller. They do not process Candidate data or data processed on the instructions of an Employer or an Agency, and they are not sub-processors: Stripe, LLC and Airwallex US, LLC, to which we send the instruction to pay an Agency, being the provider's account reference for that Agency and the amount, so that we can meet our own payment obligations under the platform terms. The bank account details and tax information of Agency users we pay are collected by those providers directly from the Agency user under their own privacy notices, and we do not receive or hold them; Google LLC (Google Analytics), for marketing website analytics subject to your cookie consent; and Google LLC (Google Workspace), which is our corporate identity provider and internal collaboration suite.

Our payment providers act on our instructions only to execute the payment we ask them to make. They do not act on our instructions in respect of the information they collect from you: each decides for itself how to carry out payment execution, sanctions screening, anti-money-laundering and know-your-customer checks, fraud monitoring, and tax and regulatory reporting, and each is an independent Controller of the Personal Data it processes for those purposes, under its own privacy notice. Where you are an Agency user, we pay; we recommend reading the privacy notice of the provider that pays you.

Fees paid to us by Employers are a separate matter. Employers pay us by bank transfer into an account held in our name, in the same way as a payment into any other company bank account. We do not disclose Personal Data to the provider of that account to receive those payments.

Data Security

We take several steps to protect your data, but no security is guaranteed.

RecruitiFi takes commercially reasonable steps to help protect and secure the information it collects and stores about RecruitiFi Users. Personal Data is encrypted in transit using Transport Layer Security ("TLS") version 1.2 or higher and encrypted at rest using AES-256. RecruitiFi's payment processors are PCI Service Provider Level 1-certified. We also use HTTP Strict Transport Security to add an additional layer of protection for our RecruitiFi Users. But remember that no method of transmission over the Internet or of electronic storage is 100% secure. Thus, while we strive to protect your Personal Information, RecruitiFi cannot ensure and does not warrant the security of any information you transmit to us.

Our other technical and organizational measures include: access to production systems and Personal Data restricted on a least-privilege basis; single sign-on with multi-factor authentication enforced for staff access; multi-factor authentication available to platform users and required for administrative roles; centralized logging and security monitoring with tamper alerting; a web application firewall configured with the OWASP Core Rule Set, distributed denial of service protection and bot management at the edge; centrally managed and encrypted endpoints with endpoint detection and response; static application security testing, dependency vulnerability management and secret scanning in our development pipeline; vulnerability remediation targets

© 2026 RecruitiFi, Inc.

of 7 days for critical, 30 days for high, 90 days for medium and 180 days for low severity findings; annual independent penetration testing; security awareness training for all personnel; and background checks and confidentiality agreements administered at onboarding.

If a personal data breach affects Personal Data we hold, we notify the affected Employer or Agency without undue delay and in any event no later than 24 hours after we become aware of it, and we notify supervisory authorities and affected individuals where and as applicable law requires, which under the GDPR means notification to the supervisory authority within 72 hours of becoming aware.

Platform Security Monitoring

We monitor the platform to detect, prevent, investigate, and respond to security threats, fraud, and abuse, and to preserve the availability, integrity, and confidentiality of the service. Our legal basis is our legitimate interest in protecting the platform and the people whose data it holds, under Article 6(1)(f) of the GDPR.

What we process for this purpose is only security-relevant metadata: authentication events, IP addresses, request metadata, device and browser metadata, and account and configuration changes. Sensitive patterns are scrubbed at source before logs are indexed. Detection and blocking are rule-based and maintained by our Security Officers; no artificial intelligence or machine learning is used. We apply geographic blocking aligned to jurisdictions sanctioned by the U.S. Office of Foreign Assets Control. An automated block of a request or session does not produce legal or similarly significant effects for you: it is a remediable denial of access, high-severity detections are triaged by a person, and false positives are corrected.

General security event logs are retained for one year from ingestion. Logs and evidence related to an incident are retained for 3 years from the close of the incident. Access to these logs is restricted to Security Officer administrator accounts, and any modification or deletion is alerted.

You may object to this processing under Article 21 of the GDPR by contacting our Data Protection Officer. We assess each objection individually and answer within 30 calendar days. For security processing, we expect in most cases to be able to demonstrate compelling legitimate grounds that override the objection, because the processing protects the platform and other data subjects, but we do not assume that outcome and each assessment is documented.

Policy on Children's Privacy

Protecting the privacy of children is especially important. The Service is for a general audience and is intended for users 18 and older. We do not knowingly collect Personal Information from anyone younger than age 18. If we become aware that a child younger than 18 has provided us with Personal Information, we will use commercially reasonable efforts to delete such information from our files. If you are the parent or legal guardian of a child younger than age 18 and believe

© 2026 RecruitiFi, Inc.

that RecruitiFi has collected Personal Information from your child, please contact our Data Protection Officer at: dpo@RecruitiFi.com.

Links to Third-Party Websites

This Privacy Policy applies only to RecruitiFi and our Services. Our Service contains links to other websites. If you choose to click on a third-party link, you will be directed to that third party's website. The fact that we link to a website is not an endorsement, authorization or representation of our affiliation with that third party, nor is it an endorsement of their privacy or information security policies or practices. We do not exercise control over third-party websites. These other websites may place their own cookies or other files on your computer, collect data or solicit Personal Information from you. We encourage you to read the privacy policies or statements of the other websites you visit.

Updates to Our Privacy Policy

We may change this Privacy Policy from time to time. Where a change is material, we will give notice at least 30 days before it takes effect, by email to Employer and Agency account holders at the address on file or by notice within the platform, and we will post the updated Privacy Policy with a revised Effective Date. Non-material changes take effect on posting. You can determine whether changes have been made by checking the Effective Date above. Where we rely on your consent for a particular processing activity, we will ask for your consent again rather than treating continued use of the Services as consent to the change.

© 2026 RecruitiFi, Inc.