Data Processing Agreement

Controller to Processor

RecruitiFi, Inc. as Processor and Service Provider

Effective: September 17, 2026

Data Processing Agreement

This Data Processing Agreement (this "DPA") is entered into as of the date determined under Recital E (the "Effective Date") by and between:

(1) the company or other organization that uses the Services under the MSA, as identified in the MSA or in its account on the Services ("Client"); and

(2) RecruitiFi, Inc., a Delaware corporation with its principal place of business in the United States ("RecruitiFi").

Client and RecruitiFi are each a "Party" and together the "Parties."

Recitals

A. RecruitiFi operates a cloud-based platform through which Client distributes job requisitions to staffing vendors, receives the candidate submissions those vendors make, and manages the resulting hiring workflow and, where Client uses the temporary staffing service, manages the engagement of selected candidates as Resources, including Statements of Services, timesheet submission and approval, and related engagement administration (the "Services"), pursuant to a master services agreement or order form between the Parties or, where none has been executed, Client's acceptance of the RecruitiFi Terms (in either case, the "MSA"). The commercial scope of the Services is set out in the MSA.

B. In the course of providing the Services, RecruitiFi Processes Personal Data on behalf of Client.

C. This DPA sets out the terms on which RecruitiFi Processes such Personal Data and reflects the Parties' agreement with respect to the Processing of Personal Data in accordance with Data Protection Laws.

D. This DPA is incorporated into and forms part of the MSA. In the event of a conflict between this DPA and the MSA (including the RecruitiFi Terms) with respect to the Processing of Personal Data, this DPA prevails as set out in Section 13.

E. This DPA is the RecruitiFi Standard Client Data Processing Agreement published at https://www.recruitifi.com/legal/client-dpa. It is incorporated by reference into the RecruitiFi Terms and forms part of the MSA. Client accepts this DPA by accepting the RecruitiFi Terms, by entering into the MSA, or by continuing to use the Services after being notified of this DPA in accordance with the MSA, and the Parties agree that acceptance in electronic form satisfies Article 28(9) of the EU GDPR. This DPA takes effect on the later of (i) the date Client first accepts the RecruitiFi Terms or enters into the MSA and (ii) the effective date stated at the top of this DPA (the "Effective Date"), and applies to all Processing of Personal Data on behalf of Client under the MSA, including Processing

that commenced before the Effective Date. Where the Parties have executed a separate data processing agreement signed by both Parties that expressly supersedes this DPA (a "Negotiated DPA"), the Negotiated DPA governs in place of this DPA for as long as it remains in force. RecruitiFi may update this DPA from time to time and will give Client at least 30 days' notice of any change that materially reduces Client's rights or RecruitiFi's obligations under it.

NOW, THEREFORE, the Parties agree as follows.

1. Definitions

1.1 Capitalized terms used but not defined in this DPA have the meanings given in the MSA. The following definitions apply to this DPA.

"CCPA" means the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, and its implementing regulations (Cal. Civ. Code section 1798.100 et seq.).

"Controller" means the natural or legal person that, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. For CCPA purposes, "Controller" includes a "Business," and for the purposes of Canadian Data Protection Laws includes an "organization" that is accountable for Personal Data.

"Data Protection Laws" means all laws and regulations applicable to the Processing of Personal Data under this DPA, including, as applicable: (a) the EU General Data Protection Regulation (Regulation (EU) 2016/679) ("EU GDPR"); (b) the EU GDPR as incorporated into the law of the United Kingdom (the "UK GDPR"); (c) the Swiss Federal Act on Data Protection ("Swiss FADP"); (d) the CCPA and other US State Privacy Laws; (e) the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA") and applicable provincial legislation including Quebec's Act respecting the protection of personal information in the private sector as amended by Law 25 ("Quebec Law 25"); and (f) any successor, amendment, or replacement of the foregoing.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

"EU SCCs" means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to the EU GDPR, as set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"Personal Data" means any information relating to a Data Subject that is Processed by RecruitiFi on behalf of Client under the MSA, and includes "personal information" and "personal data" as defined under applicable Data Protection Laws.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

"Process or Processing" means any operation performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.

"Processor" means the entity that Processes Personal Data on behalf of the Controller. For CCPA purposes, "Processor" includes a "Service Provider" or "Contractor," and for Canadian Data Protection Laws includes a "service provider" or "third party" engaged to Process Personal Data.

"RecruitiFi Terms" means RecruitiFi's online terms of service governing Client's use of the Services, being the RecruitiFi Temp Terms and the RecruitiFi Permanent Placement Terms as accepted by or on behalf of Client through the Services, as updated from time to time in accordance with their terms.

"Restricted Transfer" means a transfer of Personal Data to, or access to Personal Data from, a country or recipient not benefiting from an adequacy decision or equivalent recognition under the applicable Data Protection Law, where such transfer would be prohibited absent an appropriate safeguard.

"Negotiated DPA" has the meaning given in Recital E.

"Sub-processor" means any third party engaged by RecruitiFi (or by a RecruitiFi affiliate) to Process Personal Data on behalf of Client.

"UK Addendum" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018, in force since 21 March 2022.

"US State Privacy Laws" means all US state comprehensive consumer privacy laws applicable to the Processing, including the CCPA, the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act, the Texas Data Privacy and Security Act, the Oregon Consumer Privacy Act, the Montana Consumer Data Privacy Act, the Florida Digital Bill of Rights, the Delaware Personal Data Privacy Act, and comparable laws of other states as and when they take effect.

1.2 The terms "Business," "Service Provider," "Contractor," "Sell," "Share," "Sale," and "Sharing" have the meanings given in the CCPA.

2. Scope and roles

2.1 This DPA applies to the Processing of Personal Data by RecruitiFi on behalf of Client in connection with the Services.

2.2 As between the Parties, Client is the Controller (and, where applicable, the Business) and RecruitiFi is the Processor (and, where applicable, the Service Provider or Contractor) with respect to the Personal Data. Where RecruitiFi engages a Sub-processor under Module 3 conditions, RecruitiFi acts as Processor and the Sub-processor as sub-processor.

2.3 Client is responsible for the lawfulness of its collection of Personal Data and its instructions to RecruitiFi, and for the accuracy, quality, and legality of the Personal Data provided to RecruitiFi.

2.4 The details of the Processing, being the subject matter, duration, nature and purpose, types of Personal Data, and categories of Data Subjects, are set out in Annex I.

2.5 RecruitiFi acts as an independent Controller, and not as a Processor on Client's instructions, in respect of: (a) platform security, fraud prevention, and service-integrity monitoring; (b) administration of platform user accounts; (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 staffing vendor users of the platform; (e) payment administration, including RecruitiFi's processing of Client billing contact details for fee collection and its records of the amounts owed and paid to staffing vendors for placements and Resource engagements; and (f) analytics on RecruitiFi's marketing website. RecruitiFi determines the purposes and means of those activities independently of Client, relies on its own lawful basis for them, and describes them in the RecruitiFi Privacy Policy. This DPA does not apply to that Processing, and nothing in it makes Client a Controller of it. The Parties are not joint controllers in respect of any Processing under this DPA.

2.6 Where the same personal data is Processed both on Client's instructions under this DPA and by RecruitiFi as independent Controller under Section 2.5, RecruitiFi applies the technical and organizational measures in Annex II to it in either case.

3. Processing instructions

3.1 RecruitiFi shall Process Personal Data only on documented instructions from Client, including with regard to Restricted Transfers, unless required to do so by applicable law to which RecruitiFi is subject. Where such a legal requirement applies, RecruitiFi shall inform Client of that legal requirement before Processing, unless the law prohibits such notice on important grounds of public interest.

3.2 The MSA, this DPA (including Annex I), and Client's documented use and configuration of the Services constitute Client's complete and final documented instructions for Processing. Additional or alternative instructions must be agreed in writing and may be subject to fees where they require changes to the Services.

3.3 RecruitiFi shall immediately inform Client if, in its opinion, an instruction infringes Data Protection Laws. RecruitiFi is not obligated to conduct a legal review of the lawfulness of Client's instructions.

3.4 Client instructs RecruitiFi not to collect or Process Special Categories of Personal Data (as described in Article 9 of the EU GDPR) or criminal offence data (as described in Article 10

of the EU GDPR) through the Services, except through fields the Services expressly provide for that purpose, and Client shall not otherwise submit such data. For roles based in the United States, the Services present optional equal opportunity fields (racial and ethnic background, disability status, and veteran status) so that Client can meet EEOC and OFCCP recordkeeping obligations. Completion is optional, these fields are keyed to the location of the role and are not presented for roles based in the EEA, the UK, or Switzerland, and RecruitiFi Processes the responses solely for that recordkeeping purpose on Client's behalf.

3.5 Client acknowledges that RecruitiFi creates anonymized aggregate data, industry reports, and statistics as described in the MSA. Such data is created and used only in a form that does not identify, and cannot reasonably be used to identify or be linked to, any Data Subject, Client, or staffing vendor, and does not constitute Personal Data. Where Personal Data subject to US State Privacy Laws is used to create de-identified data, RecruitiFi maintains technical safeguards and business processes that prohibit reidentification, publicly commits to maintain and use the data only in de-identified form, and does not attempt to reidentify it except as permitted to test the effectiveness of de-identification. Nothing in this DPA restricts RecruitiFi's creation or use of that data, and nothing in the MSA authorizes RecruitiFi to use Personal Data in identifiable form for its own purposes.

3.6 Where RecruitiFi receives instructions from Client and from a staffing vendor in respect of the same Candidate record that cannot both be complied with, RecruitiFi shall notify both controllers without undue delay and shall give effect to the instruction that RecruitiFi reasonably determines is required to comply with applicable law, including recordkeeping obligations applicable to Client as a federal contractor under 41 CFR 60-1.12. Where neither instruction is required by law, RecruitiFi shall give effect to the instruction of the controller on whose behalf the record was created, being the staffing vendor in respect of a Candidate submission.

4. Confidentiality

4.1 RecruitiFi shall ensure that persons authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. RecruitiFi personnel execute confidentiality agreements as part of onboarding through the TriNet human resources information system.

4.2 RecruitiFi shall ensure that access to Personal Data is limited to those personnel who require access to perform the Services, in accordance with the least-privilege access controls described in Annex II.

4.3 The confidentiality obligations in this Section 4 survive termination of the MSA and this DPA.

5. Security measures

5.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risk to Data Subjects, RecruitiFi shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 of the EU GDPR and comparable requirements of the other Data Protection Laws.

5.2 The technical and organizational measures maintained by RecruitiFi as of the Effective Date are described in Annex II. RecruitiFi may update or modify the measures from time to time provided that such updates do not materially reduce the overall level of security of the Personal Data.

5.3 RecruitiFi shall ensure that its personnel receive appropriate data protection and security awareness training.

6. Sub-processing

6.1 Client grants RecruitiFi general written authorization to engage Sub-processors to Process Personal Data, subject to this Section 6. The Sub-processors authorized as of the Effective Date are those identified in Annex III, which incorporates the RecruitiFi Sub-Processor List.

6.2 RecruitiFi shall inform Client of any intended addition or replacement of a Sub-processor at least 30 days in advance, giving Client the opportunity to object to such changes. RecruitiFi shall provide notice by publishing an updated RecruitiFi Sub-Processor List with a revised effective date and notifying Client through the Services, by email to Client's designated contact, or by another reasonable means. Client may subscribe to notifications of changes to the list at the address in Annex III.

6.3 If Client has a reasonable, data-protection-based objection to a new Sub-processor, Client shall notify RecruitiFi in writing within the notice period. The Parties shall work in good faith to resolve the objection. If the Parties cannot resolve the objection, Client may, as its sole and exclusive remedy, terminate the affected portion of the Services that cannot be provided without the objected-to Sub-processor.

6.4 Where RecruitiFi engages a Sub-processor, it shall do so by way of a written contract that imposes on the Sub-processor data protection obligations that are substantially the same as, and in any event no less protective than, those set out in this DPA, in particular providing sufficient guarantees to implement appropriate technical and organizational measures. RecruitiFi shall ensure that each Sub-processor is bound by the data protection obligations required under Article 28(4) of the EU GDPR and the equivalent provisions of the EU SCCs.

6.5 RecruitiFi remains fully liable to Client for the performance of each Sub-processor's data protection obligations.

7. Data subject rights assistance

7.1 Taking into account the nature of the Processing, RecruitiFi shall assist Client by appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Client's obligation to respond to requests from Data Subjects exercising their rights under Data Protection Laws, including rights of access, rectification, erasure, restriction, portability, and objection.

7.2 If RecruitiFi receives a request from a Data Subject in relation to Personal Data Processed on behalf of Client, RecruitiFi shall not respond to the request directly, other than to acknowledge receipt or to direct the Data Subject to Client where permitted, and shall promptly forward the request to Client, unless legally required to respond.

8. Data protection impact assessment and consultation assistance

8.1 RecruitiFi shall assist Client in ensuring compliance with Client's obligations under Articles 32 to 36 of the EU GDPR, and comparable provisions of other Data Protection Laws, taking into account the nature of Processing and the information available to RecruitiFi.

8.2 This assistance includes reasonable cooperation with data protection impact assessments and prior consultations with a supervisory authority where required.

9. CCPA and US state privacy law addendum

9.1 This Section 9 applies to Processing of Personal Data subject to the CCPA or other US State Privacy Laws. In this Section, Client is the "Business" and RecruitiFi is the "Service Provider" or "Contractor."

9.2 RecruitiFi shall Process Personal Data solely for the purpose of performing the Services under the MSA and for the business purposes specified in Annex I, and shall not retain, use, or disclose Personal Data for any purpose other than those business purposes, or as otherwise permitted by the CCPA.

9.3 RecruitiFi shall not:

(a) Sell or Share Personal Data;

(b) retain, use, or disclose Personal Data outside the direct business relationship between the Parties;

(c) retain, use, or disclose Personal Data for any purpose other than the business purposes specified in the MSA and Annex I; or

(d) combine Personal Data received from or on behalf of Client with Personal Data it receives from or on behalf of another person, or collects from its own interaction with a Data Subject, except as permitted under the CCPA.

9.4 RecruitiFi certifies that it understands the restrictions in this Section 9 and will comply with them.

9.5 RecruitiFi shall notify Client if it determines that it can no longer meet its obligations under applicable US State Privacy Laws. Upon such notice, or where Client reasonably believes RecruitiFi is engaged in unauthorized Processing, Client may take reasonable and appropriate steps to stop and remediate the unauthorized Processing.

9.6 Client may take reasonable and appropriate steps to help ensure that RecruitiFi uses Personal Data in a manner consistent with Client's obligations under US State Privacy Laws.

9.7 The Parties acknowledge that RecruitiFi's Processing of Personal Data does not constitute consideration paid for the Personal Data, and that no Sale or Share of Personal Data occurs under this DPA.

10. Personal data breach notification

10.1 RecruitiFi shall implement and maintain the incident response plan and documented playbooks described in Annex II.

10.2 RecruitiFi shall notify Client of a Personal Data Breach affecting Client's Personal Data without undue delay and in any event no later than 24 hours after RecruitiFi becomes aware of the Personal Data Breach.

10.3 Such notification shall, to the extent then known and available, describe the nature of the Personal Data Breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, the measures taken or proposed to address the breach, and a contact point for further information. Where the information is not all available at once, it may be provided in phases without undue further delay.

10.4 RecruitiFi shall take reasonable steps to mitigate the effects of, and to minimize any damage resulting from, the Personal Data Breach, and shall reasonably cooperate with Client in relation to Client's own breach notification obligations to supervisory authorities, regulators, and Data Subjects.

11. International transfers

11.1 RecruitiFi shall not make a Restricted Transfer of Personal Data except in compliance with this Section 11 and applicable Data Protection Laws.

11.2 **EU transfers.** To the extent Processing involves a Restricted Transfer of Personal Data subject to the EU GDPR from Client, or a Client affiliate in the European Economic Area, to RecruitiFi or a Sub-processor in a country without an adequacy decision, the EU SCCs are hereby incorporated by reference and deemed executed by the Parties, as follows:

(a) Module Two (controller to processor) applies where Client is a Controller and RecruitiFi is a Processor;

(b) Module Three (processor to processor) applies where Client acts as a Processor on behalf of a third-party controller and RecruitiFi acts as a sub-processor;

(c) in Clause 7 (docking clause), the optional docking clause applies;

(d) in Clause 9, Option 2 (general written authorization) applies, with the notice period specified in Section 6.2;

(e) in Clause 11, the optional independent dispute resolution language does not apply;

(f) in Clause 17, the EU SCCs are governed by the law of the EU Member State in which Client is established, or where Client is not established in the EU, the law of Ireland;

(g) in Clause 18, disputes are resolved before the courts of that EU Member State; and

(h) Annex I, Annex II, and Annex III of the EU SCCs are populated by Annex I, Annex II, and Annex III of this DPA respectively, and the sub-processor list required by Annex III of the EU SCCs is the RecruitiFi Sub-Processor List as published at the relevant time.

11.3 UK transfers. To the extent Processing involves a Restricted Transfer subject to the UK GDPR, the UK Addendum is incorporated by reference, appended to and amending the EU SCCs. The information required by Tables 1 to 3 of the UK Addendum is populated by this DPA and its Annexes.

11.4 Swiss transfers. To the extent Processing involves a Restricted Transfer subject to the Swiss FADP, the EU SCCs apply with the following amendments: references to the EU GDPR are read as references to the Swiss FADP to the extent the Processing is subject to it; the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner; the term "Member State" is interpreted to allow Data Subjects in Switzerland to enforce their rights in their place of habitual residence; and the EU SCCs also protect the data of legal entities to the extent required by the Swiss FADP.

11.5 Alternative mechanisms. If RecruitiFi adopts an alternative lawful transfer mechanism recognized under the applicable Data Protection Law, including reliance on an adequacy decision such as the EU-US Data Privacy Framework and its UK and Swiss extensions, that mechanism applies to the relevant transfer in place of, or in addition to, the mechanisms above, to the extent the mechanism is valid and applicable. Where a recipient holds an active certification under the EU-US Data Privacy Framework (including its UK Extension and the Swiss-US Data Privacy Framework), the transfer takes place under the corresponding adequacy decision while that certification and decision remain valid, with the SCC-based mechanisms in this Section 11 standing behind the transfer and engaging automatically if either ceases to be valid.

11.6 Canadian transfers for processing. Where RecruitiFi Processes Personal Data of Data Subjects in Canada on behalf of Client, RecruitiFi shall provide a comparable level of protection to that required under PIPEDA and applicable provincial law while the Personal

Data is being Processed by RecruitiFi, through the contractual and security measures set out in this DPA and Annex II. RecruitiFi shall maintain transparency as to the location of Processing as set out in Annex III.

12. Audits and inspections

12.1 RecruitiFi shall make available to Client all information reasonably necessary to demonstrate compliance with the obligations set out in Article 28 of the EU GDPR, and equivalent obligations under other Data Protection Laws, and shall allow for and contribute to audits, including inspections, conducted by Client or an auditor mandated by Client, subject to this Section 12.

12.2 **Attestation first.** Client agrees that RecruitiFi's compliance and security assurance documentation, including its most recent SOC 2 report where available, independent penetration test summary reports, and responses to reasonable security questionnaires, shall in the first instance be used to satisfy Client's audit and inspection rights. RecruitiFi shall provide such documentation on reasonable request under confidentiality obligations.

12.3 **Escalation to audit.** Where the documentation in Section 12.2 is insufficient to address a specific, reasonable, and documented concern, or where an audit is required by a supervisory authority or regulator with jurisdiction over Client, Client or its mandated auditor may conduct an audit, subject to the following:

(a) Client provides reasonable prior written notice of at least 30 days, except where a shorter period is required by a regulator or follows a Personal Data Breach;

(b) audits occur during normal business hours and are conducted so as to minimize disruption;

(c) audits are limited to once per 12-month period, except where required by a regulator or following a Personal Data Breach;

(d) the auditor is bound by appropriate confidentiality obligations and is not a competitor of RecruitiFi; and

(e) the scope is limited to systems, facilities, records, and processing activities relevant to the Processing of Client's Personal Data.

12.4 RecruitiFi shall provide Client with information and assistance reasonably necessary to enable Client to respond to inquiries from a regulator with jurisdiction over Client. Nothing in this Section 12 grants any regulator a direct right of audit of, or direct access to, RecruitiFi's systems, facilities, or records.

13. Liability, order of precedence, and term

13.1 Each Party's liability arising out of or related to this DPA, whether in contract, tort, or otherwise, is subject to the limitations and exclusions of liability set out in the MSA or the

applicable Statement of Work ("SOW"), depending on which governs the relevant Services, or, where neither specifies a limitation of liability, the RecruitiFi Terms. Any reference to the liability of a Party in the applicable agreement means the aggregate liability of that Party under that agreement and this DPA together.

13.2 In the event of a conflict between this DPA and the MSA (including the RecruitiFi Terms) regarding the Processing of Personal Data, this DPA prevails. Where a Negotiated DPA is in force between the Parties, the Negotiated DPA prevails over this DPA to the extent of any conflict. In the event of a conflict between this DPA and the EU SCCs, or the UK Addendum, the EU SCCs, or the UK Addendum, prevail with respect to the relevant Restricted Transfer.

13.3 This DPA takes effect on the Effective Date, applies to all Processing of Personal Data on behalf of Client under the MSA whether commenced before or after the Effective Date, and remains in force for as long as RecruitiFi Processes Personal Data on behalf of Client under the MSA, except for any period during which a Negotiated DPA is in force between the Parties. If a Negotiated DPA is terminated or expires while RecruitiFi continues to Process Personal Data on behalf of Client under the MSA, this DPA governs that Processing from the date of termination or expiry.

13.4 The obligations in this DPA that by their nature should survive termination, including confidentiality, deletion and return, and liability, survive termination or expiry of the MSA and this DPA.

13.5 This DPA is governed by the laws of the State of New York, without regard to its conflict of laws principles, and the Parties submit to the exclusive jurisdiction of the state and federal courts located in New York, New York, except that the EU SCCs, the UK Addendum, and the Swiss amendments are governed by the laws and subject to the jurisdictions specified within those instruments.

14. Deletion and return of data

14.1 At the choice of Client, RecruitiFi shall delete or return all Personal Data to Client after the end of the provision of the Services relating to Processing, and shall delete existing copies unless applicable law requires storage of the Personal Data. Deletion of backup copies is subject to Section 14.3.

14.2 Deletion and return are performed in accordance with RecruitiFi's Data Deletion Policy and Client's documented instructions, subject to Section 3.6 where a conflicting controller instruction or legal retention obligation applies to the same record. Where Personal Data is retained because required by applicable law, RecruitiFi shall protect the confidentiality of such Personal Data and shall Process it only to the extent and for the period required by that law.

14.3 Backup copies remain encrypted and access-restricted and expire under their assigned retention periods. Backups are held in immutable storage, so a backup copy cannot be altered or deleted before its assigned retention period expires; on expiry it is deleted in the ordinary course. Personal Data deleted under Section 14.1 is removed from active use immediately, and a record deleted on Client's instruction is re-suppressed if a backup is ever restored. Records relating to hiring decisions that are retained on a legal basis, and Personal Data subject to a legal hold, remain retained for the required period notwithstanding this Section 14.

15. Records of processing

15.1 RecruitiFi shall maintain records of the categories of Processing carried out on behalf of Client as required by Article 30(2) of the EU GDPR, and shall make such records available to Client or a supervisory authority on reasonable request.

Annex I: Description of processing

A. List of parties

Data exporter (Controller or Business): the Client under the MSA, as identified in the MSA or in its account on the Services. Contact: the data protection contact in Client's account profile or, absent one, Client's notice contact under the MSA. Role: Controller, or Processor where Client acts on behalf of a third-party controller.

Data importer (Processor or Service Provider): RecruitiFi, Inc., a Delaware corporation. Contact: RecruitiFi Privacy and Security team. Role: Processor, or sub-processor under Module 3 where applicable.

B. Categories of data subjects

- Client hiring managers and other authorized Client users of the Services, to the extent their actions appear in submission and workflow records Processed on Client's behalf. Their account data itself is addressed in Section 2.5(b).
- Job candidates submitted to the Services by staffing vendors.
- Resources, being candidates selected by Client and engaged on assignment under a Statement of Services, whose engagement and timesheet records are Processed on Client's behalf for the duration of the assignment.
- Staffing vendor recruiters and users who access the Services.

C. Categories of personal data

- Candidate data: name, contact details (email, telephone, address), employment history, education history, and other resume or curriculum vitae content submitted through the Services; responses to screening questions defined by Client, where Client requires them; per-job candidate confirmation records; and candidate submission and hiring workflow status.
- Temporary engagement data: Statement of Services terms (start date, anticipated length of engagement, bill rates, description of work), weekly timesheet records of hours worked as submitted by the staffing vendor and approved by Client, assignment status, and assignment-duration data derived from those records, including cumulative time on assignment measured from the Resource's first platform-recorded assignment with Client.
- User account data, being the name, business email address, and role or job function of Client users, is Processed by RecruitiFi as independent Controller for platform account administration and is not Processed on Client's behalf; it is addressed in Section 2.5(b) and listed here for transparency only.
- Usage and log data: platform activity records generated through Client's use of the Services and made available to Client through the Services, including submission and

workflow audit trails. Security event telemetry, being authentication events, IP addresses, request metadata, and device and browser metadata processed for security, fraud prevention, and service-integrity monitoring, is not Processed on Client's behalf and is addressed in Section 2.5.

D. Special categories of personal data

For roles based in the United States, the Services present optional equal opportunity fields (racial and ethnic background, disability status, and veteran status) so that Client can meet EEOC and OFCCP recordkeeping obligations. Completion is optional. These fields are keyed to the location of the role and are not presented for roles based in the EEA, the UK, or Switzerland. No other special category or criminal offence data is collected by design, and Client is instructed not to submit such data except through those fields (Section 3.4). Where Special Categories of Personal Data are nonetheless submitted by Client or its staffing vendors outside those fields, RecruitiFi applies the technical and organizational measures in Annex II uniformly to all Personal Data.

E. Frequency of the transfer

Continuous, for the duration of the Services.

F. Nature and purpose of the processing

Provision, operation, support, and maintenance of the RecruitiFi platform for the candidate submission and hiring workflow, being the distribution of Client's job requisitions to staffing vendors, the receipt of candidate submissions from those vendors, candidate confirmation of each submission, presentation of confirmed candidates to Client, and management of the resulting evaluation and hiring workflow, together with the hosting, storage, transmission, and display of Personal Data necessary for those purposes, in accordance with the MSA. Where Client uses the temporary staffing service, the processing additionally comprises the administration of Resource engagements, being the recording of Statements of Services, the submission, approval, and invoicing of timesheets, and the computation of each Resource’s cumulative assignment duration from platform records in order to generate tenure alerts to Client in support of Client’s own workforce tenure policies. Tenure alerts are informational; the definition of, and compliance with, any tenure limit remains Client’s responsibility. The candidate submission and hiring workflow is the processing described under that name in RecruitiFi’s Data Protection Impact Assessment and Record of Processing Activities; the temporary staffing service is currently offered for roles based in the United States and its processing falls outside the territorial scope of that register.

G. Duration of processing and retention

For the term of the MSA, and thereafter Personal Data is deleted or returned in accordance with Section 14 of this DPA, RecruitiFi's Data Deletion Policy, and Client's documented instructions.

H. Competent supervisory authority

For EU SCC purposes, the competent supervisory authority is that of the EU Member State in which Client is established, or where Client is not established in the EU, the Irish Data Protection Commission. For UK transfers, the Information Commissioner's Office. For Swiss transfers, the Federal Data Protection and Information Commissioner.

Annex II: Technical and organizational measures

This Annex describes the technical and organizational security measures maintained by RecruitiFi as of the Effective Date. RecruitiFi may update these measures provided the overall level of security is not materially reduced.

1. Hosting and infrastructure

- The application is hosted on a platform-as-a-service environment on Heroku, a Salesforce product, with production hosted in the United States (Virginia) and disaster recovery in the United States (Oregon).
- Managed data stores comprise Heroku Postgres and Heroku Redis.
- Amazon Web Services provides object storage (Amazon S3 with cross-region replication), content delivery (CloudFront), key management (KMS), audit logging (CloudTrail), threat detection (GuardDuty), and centralized identity and access management for cloud resources (IAM Identity Center).
- Cloudflare provides edge security, including a web application firewall configured with the OWASP Core Rule Set, distributed denial of service protection, bot management, and geographic blocking aligned to OFAC-sanctioned jurisdictions.

2. Encryption

- Personal Data is encrypted at rest using AES-256.
- Personal Data is encrypted in transit using TLS version 1.2 or higher.

3. Identity and access management

- Corporate access uses Google Workspace single sign-on with multi-factor authentication enforced.
- Access follows least-privilege principles. Access to production systems and Personal Data is restricted to personnel who require it to perform the Services.
- Secrets are managed using 1Password.

4. Endpoint and device security

- The corporate device fleet is macOS-only and centrally managed using Jamf Pro mobile device management.
- Endpoint detection and response is provided by Bitdefender, including Device Control that blocks removable media.

5. Logging and monitoring

- Centralized logging and security monitoring are provided through Datadog, supplemented by AWS CloudTrail and GuardDuty for cloud-layer activity and threat detection.

6. Secure development and vulnerability management

- Source code is managed in GitHub, with static application security testing using CodeQL, dependency vulnerability management using Dependabot, and secret scanning using GitGuardian.
- Vulnerability remediation service levels are: Critical within 7 days, High within 30 days, Medium within 90 days, and Low within 180 days.
- Independent penetration testing: Workstreet, August 2026 (external black-box assessment of the pre-production environment, report v1.0 dated 11 August 2026): no critical or high findings; two medium and one low finding, all remediated 14 August 2026, within the M2 vulnerability remediation service levels; remediation verified against the production host.

7. Business continuity and disaster recovery

- A disaster recovery capability is maintained with production in Virginia and disaster recovery in Oregon.
- The disaster recovery plan was most recently tested on January 10, 2026, achieving a recovery time objective of 2 hours and 47 minutes against a 4-hour target, and a recovery point objective of 9 hours and 57 minutes against a 24-hour target.

8. People security

- Security awareness training is delivered through Wizer.
- Background checks and confidentiality agreements are administered through TriNet human resources information system onboarding.

9. Incident response

- RecruitiFi maintains an incident response plan with documented playbooks governing detection, triage, containment, eradication, recovery, notification, and post-incident review.

Annex III: Authorized Sub-Processors

The Sub-processors authorized as at the effective date of this Agreement are those listed in the RecruitiFi Sub-Processor List published at https://www.recruitifi.com/legal/sub-processors, which is incorporated into this Agreement by reference. The list states, for each Sub-processor, its legal entity name, the service it provides, the location of processing, and the transfer safeguard relied on, and carries a version number, an effective date, and a change log. Superseded versions are retained and provided on request to the RecruitiFi Data Protection Officer at dpo@recruitifi.com, or by post to RecruitiFi, Inc., 21 West 46th St., New York, NY 10036.

Processing locations. All platform processing takes place in the United States. Requests to the platform transit Cloudflare's global edge network and may be inspected at an edge location outside the United States before reaching the platform, as described in the Sub-Processor List's edge-processing note.

Notice of changes. RecruitiFi gives at least 30 days' notice before a new Sub-processor begins Processing Personal Data under this Agreement, by publishing an updated version of the list with a revised effective date and notifying clients through the platform or by email to the designated contact. To subscribe to change notifications, contact dpo@recruitifi.com. Objections are handled in accordance with Section 6 of this Agreement.